

EDICIÓN ANUAL DE LA CONFERENCIA

ACAMS[®] TODAY

La Revista Para los Profesionales del Campo Antilavado de Dinero

LA FANTASÍA
CONTRA LA
REALIDAD

NO ECHE LOS
DADOS

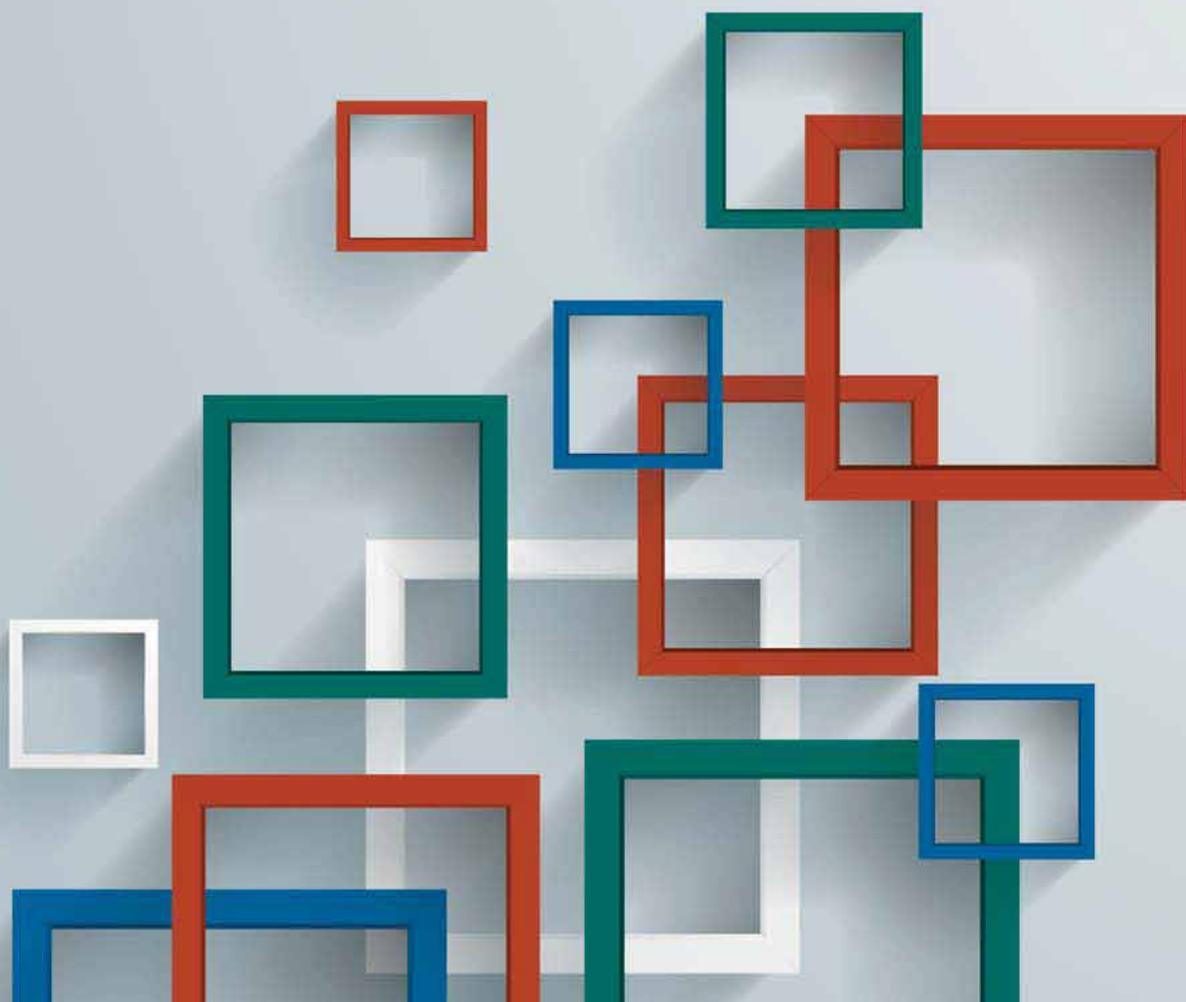
SEPTIEMBRE—
NOVIEMBRE 2016
VOL. 15 NO. 4

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

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

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



**“CLEAR® PUTS
QUALITY
INFORMATION
IN ONE
EASY-TO-USE
LOCATION.”**

– CLEAR customer

Bring the facts into focus.

Designed to address the needs of fraud investigators, CLEAR brings all the important information on a person or business into an easy-to-use dashboard. Quick Analysis Flags uncover a person’s risk from criminal records, vehicle history reports, and medical and OFAC sanctions and allow deeper searching into data if something is revealed. Graphical Display helps to visualize connections between people and businesses.

Investigate confidently with CLEAR. To learn more, visit clear.thomsonreuters.com or call 1-800-262-0602.



THOMSON REUTERS™

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 2300
Miami, FL, 33130

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

Email: info@acams.org
Internet: www.ACAMS.org
www.espanol.acams.org
www.ACAMSToday.org

| EDICIÓN Y DISEÑO |

ASISTENTE EDITORIAL *Alexa Serrano, CAMS*

DISEÑADORA GRÁFICA *Victoria Racine*

| COMITÉ EDITORIAL |

PRESIDENTA *Debbie Hitzeroth, CAMS-FCI*

Kevin Anderson, CAMS

Brian Arrington, CAMS

Edwin (Ed) Beemer, CAMS-FCI

Aaron Fox

Robert Goldfinger, CAMS

Jennifer Hanley-Giersch, CAMS

Carolina Rivas, CAMS

Eric Sohn, CAMS

Joe Soniat, CAMS

Amy Wotapka, CAMS

Elaine Yancey, CAMS

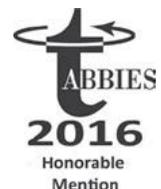
ACAMS Today © 2016 por la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS). Todos los derechos reservados. La reproducción de cualquier material de esta publicación, en todo o en parte, sin permiso expreso por escrito de ACAMS está estrictamente prohibido.

2016 Regional Gold and Silver
Addy Award Winner

AMERICAN
ADVERTISING
AWARDS



2016 Winner of Gold
and Silver Awards



| PERSONAL SENIOR |

OFICIAL EJECUTIVO EN JEFE *Ted Weissberg, CAMS*
 GERENTE DE FINANZAS Y DESARROLLO CORPORATIVO OFICIAL *Ari House, CAMS*
 JEFA DE ASIA *Hue Dang, CAMS-Audit*
 VICEPRESIDENTE DE VENTAS *Geoffrey Fone, CAMS*
 DIRECTORA DE MARKETING *Kourtney McCarty, CAMS*
 JEFA DE EUROPA *Angela Salter*
 DIRECTOR DE OPERACIONES *Tim McClinton*

| REPRESENTANTES REGIONALES Y DE VENTAS |

VICEPRESIDENTE SENIOR DE DESARROLLO DE NEGOCIOS *Geoffrey Chunowitz, CAMS*
 DIRECTORA REGIONAL *Sonia Leon, CAMS*
 JEFE DE ÁFRICA & ORIENTE MEDIO *Jose Victor Lewis*

| CONSEJO DIRECTIVO |

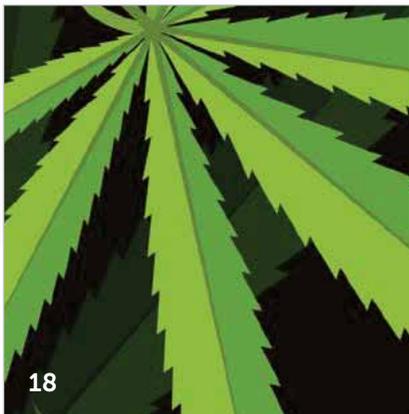
PRESIDENTE *Rick A. Small, CAMS*
Luciano J. Astorga, CAMS
Robert Curry, CAMS
William J. Fox
María de Lourdes Jiménez
Frank Lawrence, CAMS
Dennis M. Lormel, CAMS
William D. Langford, CAMS
Rick McDonell
Karim Rajwani, CAMS
Anna M. Rentschler, CAMS
Anthony Luis Rodriguez, CAMS, CPA
Nancy Saur, CAMS, FICA
Markus E. Schulz
Daniel Soto, CAMS

| ASESORES ESPECIALES PARA EL CONSEJO DIRECTIVO |

Samar Baasiri, CAMS
Vasilios P. Chrisos, CAMS
David Clark, CAMS
Susan J. Galli, CAMS
Peter R. Hazlewood

ACAMS[®] | Capacitando
 Profesionales contra el
 Crimen Financiero Mundial

Contenido



18

De la editora 8

Noticias de los miembros... 10

Carta del vicepresidente ejecutivo 12

Sondeo de la viabilidad práctica de las normas del GAFI para prevenir el movimiento de dinero para el terrorismo..... 14

Una evaluación de las recomendaciones del GAFI sobre la financiación del terrorismo.

Definiendo las empresas relacionadas con la marihuana 18

Un marco global para ordenar las empresas relacionadas con la marihuana en tres niveles basados en el riesgo.



22

Logrando el riesgo de la empresa cuando las leyes de ALD y de privacidad entran en conflicto 22

Las instituciones financieras y otras instituciones reguladas se enfrentan a enormes desafíos al tratar de ver el riesgo en toda la empresa.

Cuando dos mundos chocan 26

El efecto de la tecnología de cadenas de bloques sobre los profesionales de ALD en todo el mundo.

La lucha contra el lavado de dinero en el sector inmobiliario 30

Una mirada a dos debilidades de ALD/CFT que deben ser eliminadas para luchar contra el lavado de dinero en el sector inmobiliario.



50

¿Cuánto puedes bajar? 34

Una revisión de dos medidas de ejecución y las obligaciones y consecuencias de identificar correctamente las participaciones de propiedad.

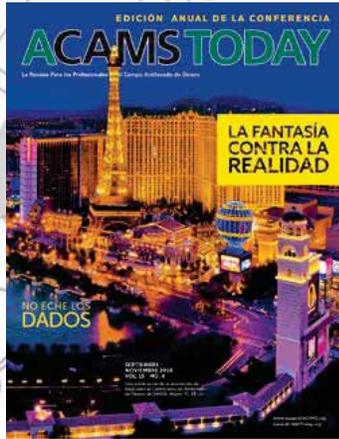
Rick McDonnell: Temas de ALD y GAFI 38

El ex secretario ejecutivo del GAFI habla de desafíos de antilavado de dinero de este año y la importancia del GAFI hoy.

Soluciones de cumplimiento: La combinación de la computación cognitiva con la inteligencia humana 50

Herramientas para mejorar los procesos de toma de decisiones de la institución financiera.

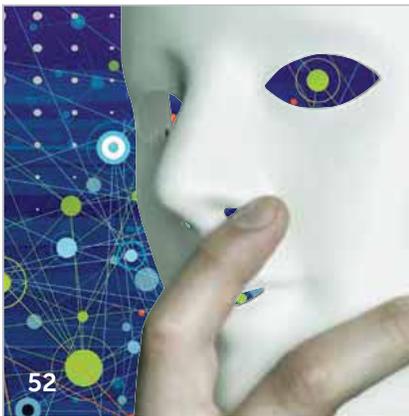




EN LA PORTADA:

La fantasía contra la realidad..... 44

Un enfoque práctico para el programa de ALD de un casino



Desenmascarando el prejuicioso en los algoritmos de ALD..... 52

Medidas que las instituciones financieras pueden tomar para eliminar el prejuicio en la presentación de análisis y reportes de ALD.

El ALD y los préstamos: La construcción de la concientización mediante la asociación 56

Los beneficios de la colaboración de funciones cruzadas entre prestamistas y profesionales de ALD.

No eche los dados 58

Una discusión en profundidad de conozca a su cliente para los casinos.



La comprensión del riesgo del cliente..... 64

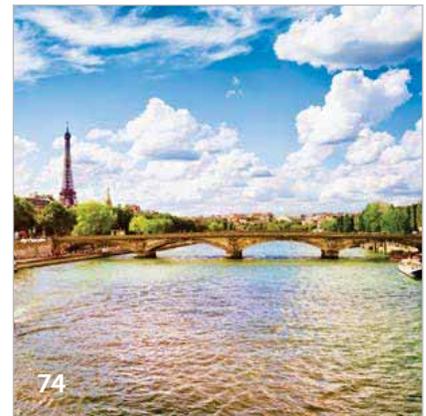
Cómo capturar de manera efectiva el riesgo del cliente y entender el riesgo general planteado por los clientes.

El león al acecho: El impacto del Memo de Yates sobre oficiales de cumplimiento y monitoreo 66

Un modelo de organización sobre la cultura y el control de las instituciones financieras.

Navegando la Recomendación 16 del GAFI 70

Medidas que los bancos deben tomar para hacer frente a los desafíos operativos y de cumplimiento relacionados con las nuevas necesidades de datos y beneficiarios en los mensajes de pago.



Anuncios europeos 74

El primer programa de Certificación Avanzada en Europa y qué se puede esperar de la certificación CAMS y los capítulos en toda Europa.

Mary Bashore, CAMS: El siguiente paso como directora ejecutiva emérita de la junta directiva 76

Mary Bashore habla de su nominación como la primera directora ejecutiva emérita del Capítulo de la Capital de los EE.UU.

Conozca al personal de ACAMS..... 80

Graduados de CAMS y de la Certificación Avanzada..... 81



Lo que pasa en Las Vegas... queda en Las Vegas



¿Pero es así? No siempre. Especialmente si su estadía en Las Vegas implica algún tipo de delito financiero. La mayoría de la gente va a Las Vegas para escapar de la realidad y para entretenerse. Entonces, ¿qué es fantasía y qué es realidad?

Hace un tiempo, pasé el fin de año en Las Vegas. Mis amigos me habían dicho que todo el mundo debería experimentar el fin de año en Las Vegas. Durante mucho tiempo me habían compartido historias de sus aventuras por la avenida principal. Cuando llegué a la ciudad el día antes del fin de año, pensé, “¿Se comparará la realidad con las historias que mis amigos me contaron?” Honestamente puedo decir que el fin de año fue muy memorable y la realidad superó la fantasía. Mientras caminaba por la avenida principal me detuvieron dos trabajadores de los casinos y me regalaron entradas gratuitas para pasar el fin de año con Neil Diamond en el MGM. Después de algunas dudas, acepté las entradas.

Esa experiencia no se quedó en Las Vegas porque les conté la aventura memorable a mis amigos. Sin embargo, los delincuentes de delitos financieros prefieren que sus actividades ilegales permanezcan en Las Vegas y pasen desapercibidas. En el artículo titular *La fan-*

tasía contra la realidad, Paul Camacho esboza un enfoque práctico que los casinos deben tomar en cuanto a su programa de anti-lavado de dinero (ALD). Camacho afirma “que, debido a las muchas transacciones de divisas realizadas por los casinos, existen vulnerabilidades de lavado de dinero, pero no hay excusa para que los casinos no hagan cumplir una prioridad”.

Nuestro segundo artículo titular, *No eche los dados*, analiza la importancia de conocer a su cliente (KYC) para los casinos y muestra lo que los casinos deberían considerar a la hora de construir su programa de KYC. Peter S. Alvarado y Thomas J. Paramo mencionan el impacto de los reportes de operaciones sospechosas (ROS), teniendo un enfoque basado en el riesgo y los muchos escenarios diferentes por considerar en la construcción de un programa de cumplimiento de ALD fuerte y la implementación de una política eficaz de KYC.

La edición de la *Conferencia Anual de ACAMS Today* está llena de artículos informativos. Los temas van desde la definición de las empresas relacionadas con la marihuana, el anti-lavado de dinero en el sector inmobiliario, el sesgo de desenmascaramiento en los algoritmos de ALD hasta el efecto de que la tecno-

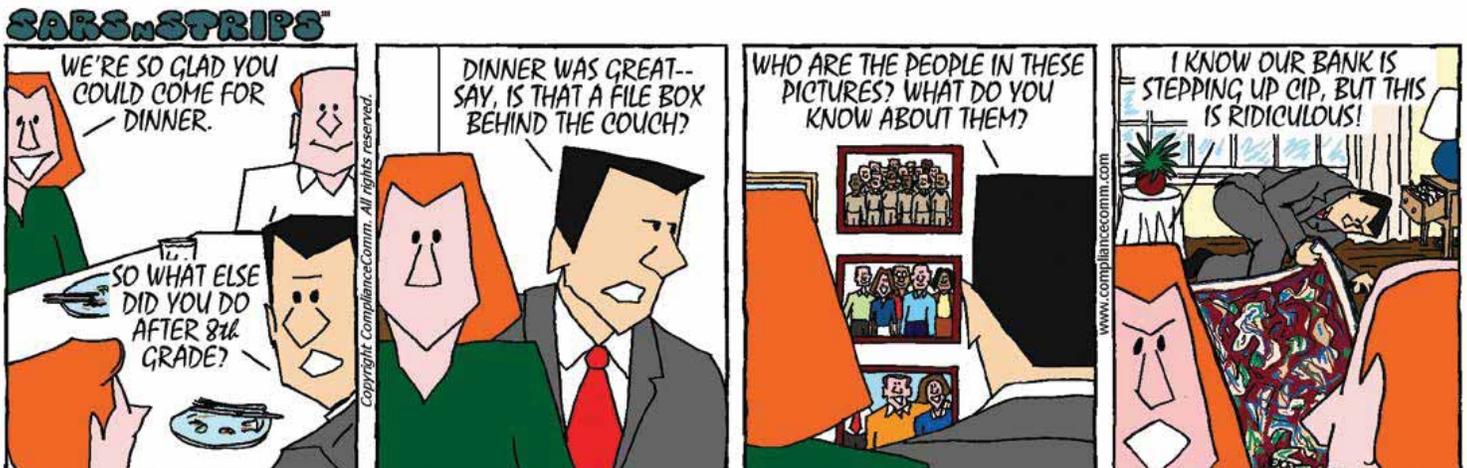
logía global de las cadenas de bloques tienen en los profesionales de prevención de delitos financieros de ALD.

Esta edición también contiene una entrevista con Rick McDonnell, ex secretario ejecutivo del GAFI y actualmente director ejecutivo de ACAMS y miembro de la junta asesora de ACAMS. McDonnell discute desafíos de ALD y evaluaciones mutuas del GAFI. Nuestra siguiente entrevista es con Mary Bashore, CAMS, del Capítulo de la Capital de los EE.UU. Bashore habla de su papel como directora emérita de la junta directiva, sus muchos años de experiencia en la junta directiva del Capítulo de la Capital de los EE.UU. y cómo ve el futuro próximo del capítulo.

Que la fortuna nos sonría a todos este año y espero verlos a muchos de ustedes en la Conferencia Anual de ACAMS. 🎲

Karla Monterrosa-Yancey

Karla Monterrosa-Yancey, CAMS
jefa de redacción



Producido por: ComplianceComm

Ready for FinTech?



Obtain risk, strategy
and compliance insights
from the market leader.

The digital revolution in financial services is here. The question is, will your bank engage with emerging players in FinTech or remain on the sidelines? Stratis Advisory can help you better understand the opportunities, risks and compliance management requirements involved with building a FinTech portfolio.

Stratis Advisory is an objective resource in the FinTech ecosystem, connecting the dots between companies, investors and banks by integrating deep regulatory risk domain expertise into the broad context of business strategy, risk management and compliance operations. Learn more about managing opportunity and risk in the new world of FinTech. Call 917.554.9903 (NY), 415.379.0730 (SF) or visit StratisAdvisory.com



Trish Emerson, CAMS
Charlotte, Carolina del Norte, EE.UU.

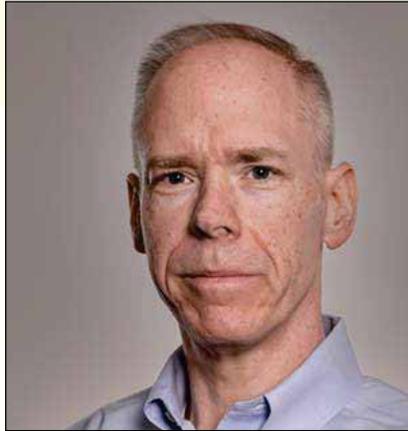
Trish Emerson es directora senior del Equipo de Investigación de ALD de Enterprise de Ally Financial, Inc., donde es responsable de todas las investigaciones de antilavado de dinero (ALD) y financiamiento del terrorismo, así como de otras actividades de cumplimiento.

Antes de unirse a Ally, Emerson fue la gerente de investigaciones de ALD de la unidad de inteligencia financiera de Wachovia/Wells Fargo East Coast que se encuentra en Charlotte, Carolina del Norte. Tiene más de 12 años de experiencia en la industria financiera. Además, tiene extensa experiencia significativa en investigaciones de reportes de operaciones sospechosas y operaciones de integración.

Antes de su carrera en la banca, Emerson fue agente especial de la Oficina Estatal de Investigación de Carolina del Norte en Charlotte, Carolina del Norte. Como agente especial, Emerson se especializaba en investigaciones internacionales de drogas y lavado de dinero, así como de la investigación de homicidios.

Emerson asistió a la Universidad de Carolina del Norte en Charlotte, donde obtuvo una licenciatura en derecho penal con una subespecialización en sociología. En junio de 2008, Emerson recibió su credencial de Especialista Certificado en Antilavado de Dinero de ACAMS. Además, es socia activa del Capítulo de las Carolinas de ACAMS.

Sus premios incluyen el *Premio de Honor* de la Asociación Internacional de Oficiales de Cumplimiento de Narcóticos y el *Premio de Agente del Año* de la Organized Crime Drug Enforcement Task Force de la Región Sudeste.



Michael Slover
Riverwoods, IL, EE.UU.

Michael Slover es vicepresidente, oficial jefe de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) y de sanciones de Discover Financial Services. Desde julio de 2015, ha sido responsable de los programas globales de gestión de BSA/ALD, la financiación del contrterrorismo y las sanciones de cribado de la Oficina de Control de Activos Extranjeros, que incluye el holding bancario, así como la supervisión central y la gobernanza para Discover Bank y las empresas de Servicios de Pago. Desde su incorporación a Discover, Slover se ha centrado en la construcción del equipo de BSA/ALD y de sanciones y procesos de implementación y modernización de la tecnología para permitir la viabilidad a largo plazo del programa y apoyo del crecimiento futuro.

Antes de unirse a Discover, Slover trabajó en American Express como jefe de cumplimiento para varias líneas globales de negocios y estableció su función de Gestión del Riesgo de Cumplimiento. Antes de su estadía en American Express, formó parte del Consejo para la Práctica de normativas en Pricewaterhouse Coopers. Como director en el grupo de banca y mercados de capitales, se centró en el desarrollo y aplicación de las reglamentaciones de las instituciones financieras en todos los EE.UU. y el extranjero. Slover también sirvió en agencias de control legal en su estado natal de Nueva Jersey en los condados de Somerset y de Warren. Además, es licenciado en contabilidad por la Universidad de Rutgers y es Contador Público Certificado.



Tatiana Turculet, CAMS
Munich, Alemania

Tatiana Turculet ha estado trabajando en consultoría desde 2014 después de unirse al Departamento de Asesoría de Riesgos de Deloitte. Ha participado en proyectos de auditoría de alta complejidad, normativos y forenses con bancos de primer nivel en Frankfurt am Main, Alemania. Además, Turculet tiene experiencia en banca y cumplimiento financiero, delitos financieros, antilavado de dinero (ALD) y la lucha contra el financiamiento del terrorismo (CFT), así como la protección de datos.

Antes de trabajar en Deloitte, Turculet trabajó en el Banco Europeo de Inversiones (parte del Grupo BEI) en Ciudad de Luxemburgo y en la Dirección General de la Comisión Europea para el Presupuesto en Bruselas, Bélgica. La experiencia profesional adquirida dentro del Departamento de Cumplimiento del BEI, en asuntos relacionados con ALD/CFT, conozca a su cliente, debida diligencia, junto con sanciones y embargos, fue un factor decisivo en su decisión de proseguir con este campo.

Turculet obtuvo una Maestría en Derecho y Negocios en el año 2013 de dos prominentes universidades alemanas: la Facultad de Derecho de Bucerius y WHU – Otto Beisheim School of Management, con un enfoque en la ley de los mercados de capitales de la UE. Se convirtió en socia de ACAMS en enero de 2016 y obtuvo su certificación CAMS cuatro meses más tarde. Además, es parte del Grupo de Trabajo Europeo y colaboradora para temas relacionados con la UE. 



THE SECRET IS OUT!

Compliance challenges and unforeseen risks are hiding at every turn, but finding an easier way to overcome these obstacles shouldn't be a mystery. With CSI, you get **a technology partner with proven expertise** in compliance, risk management and security. Our innovative solutions and industry experts are the secret combination you've been waiting for.



csiweb.com/Secret

Enterprise Risk Management • WatchDOG® Watch List Screening • Compliance Software & Services • Cyber & Information Security Services

ACAMS® | Affiliate Member *Gold*

ALD en el entorno actual

Si en duda, es difícil creer que nos estamos acercando a la 15ª Conferencia Anual de ALD y Delitos Financieros de ACAMS. Con otra impresionante asistencia de más de 160 ponentes y temas que recorren la gama desde comprender el papel de los medios de comunicación social en la lucha contra el impacto de la financiación del terrorismo hasta los retos actuales de la seguridad cibernética y donde los datos se inscriben en el antilavado de dinero (ALD), los cambios en nuestra comunidad han sido masivos desde la primera conferencia de ACAMS.

Lo hemos mencionado antes, pero para ser un profesional del ALD en 2016, hay que entender una amplia gama de áreas que tocan los delitos financieros, tales como el abuso de los mayores, el tráfico de personas y la corrupción, entre muchos otros desafíos. Cualquier persona involucrada en el ALD y la disuasión de delitos financieros ahora deberá tener personal o información sobre el funcionamiento de la actividad financiera. Por lo tanto, el cumplimiento o los antecedentes legales no son suficientes para hacerles frente a todas las acciones que requieren la presentación de reportes y/o prevención.

Otro aspecto del ALD en el entorno actual es el impacto que las decisiones tienen sobre las personas o entidades que necesitan acceder a relaciones financieras de todo el mundo. El debate de la llamada “eliminación del riesgo” en lo que ha llegado a ser conocido como la inclusión, parece continuar sin ninguna solución real. ACAMS, en conjunto con el Grupo del Banco Mundial, llevó a cabo un “diálogo entre las partes”, en mayo y junio sobre los problemas que han causado mucho daño colateral en todo el mundo. Estamos cerca de un

reporte preliminar con las posibles soluciones, pero el asunto clave es que todos los que están en el ALD quieren claridad, orientación y apoyo para permitir que los participantes legítimos en el sector privado prosperen y apoyen a aquellos que necesitan acceder a la economía global. Les pedimos a todos nuestros socios que vean la “eliminación del riesgo” como un área que necesita enfocarse y tener soluciones.

Un momento para recordar

Ser parte de la comunidad de ALD se distribuye tristemente en pre-y post-9/11. Muchos de nosotros nos hemos estado ocupando de los problemas y desafíos de la forma de abordar el lavado de dinero desde mediados de la década de 1980. Esos primeros “veteranos” se centraron en la estructuración, el narcotráfico y los primeros intentos de colocación de fondos ilícitos. Después del 11 de septiembre del 2001, el sector financiero tuvo que mirar más allá del disfraz financiero básico y empezar a pensar como un terrorista solitario o uno como parte de una banda. También hemos tenido que aceptar, por primera vez, que las instituciones financieras no tradicionales necesitan mejorar su enfoque sobre actividades sospechosas. Curiosamente, todavía hay entidades financieras y los llamados porteros que se oponen a unirse a sus colegas financieros para reportar, detectar y impedir que los grupos transfieran fondos contaminados e ilícitos que pueden disfrazar su fuente original.

Para los de nosotros involucrados en la respuesta financiera a 9/11, parece difícil observar que esos actos horribles ocurrieron hace 15 años. Me sentí personalmente conmovido

por la rápida respuesta del sector privado al rompecabezas financiero que todos necesitábamos resolver. También quedó claro que el gobierno estatal, local y federal estaban todos alineados y se movieron tan rápido y eficientemente—mostrando a los escépticos del gobierno lo bueno que podían ser. En lo personal, me sentí abrumado por la cooperación, la coordinación y la comunicación en toda la comunidad de ALD.

Los que se aferran a la vieja mentira de que el gobierno no funciona, sólo tienen que volver la vista atrás a ese momento difícil para los EE.UU. y observar cómo la respuesta resultó ser lo opuesto a lo que piensan los detractores—el gobierno y los ciudadanos pueden trabajar juntos.

Gracias a todos los que ayudaron después del 9/11 y al nuevo grupo de profesionales de ALD comprometidos que trabajaron juntos para abordar los componentes financieros en San Bernardino, Orlando, París y muchas otras áreas.

Me siento orgulloso de ser parte de la comunidad global de ALD y esperamos que ACAMS le ayude a ser parte de este gran grupo de expertos comprometidos. 



John J. Byrne, Esq., CAMS
vicepresidente ejecutivo





Advising against money laundering

Making an impact that matters

We have a specialist team in providing strategies and solutions for operations with illegal resources.

For more information.

<http://www.deloitte.com/mx/asesoriafinanciera>
<http://www.deloitte.com/mx/investigacionforense>

Sondeo de la **viabilidad práctica** de

LAS NORMAS DEL GAFI

para prevenir el movimiento de **dinero para el terrorismo**

Después del 9/11 y el crecimiento de los estudios sobre terrorismo, ha habido un mayor enfoque de las prácticas relacionadas con la financiación del terrorismo. Del mismo modo, en reconocimiento de los métodos casi indistinguibles en el que las actividades financieras pueden apoyar la financiación del terrorismo, el interés ha crecido en torno a la utilización de actividades legítimas y semilegítimas. El fenómeno creciente del Estado Islámico de Irak y el Levante (ISIL por sus siglas en inglés) presenta un nuevo tipo de organización terrorista—uno que explota vías particulares de financiación para apoyar sus actividades. Exista o no un nexo entre el delito organizado y el terrorismo, parece que el antilavado de dinero (ALD) y la lucha contra la financiación del terrorismo (CFT) se han alineado para crear una serie pragmática y exitosa de diferentes enfoques para prevenir y detectar la financiación de grupos terroristas.

Reconocido como un punto de referencia global y estándar universal para el ALD y CFT, las 40 Recomendaciones del Grupo de Acción Financiera Internacional (GAFI) combinan medidas de la ONU existentes sobre las actividades criminales y no terroristas para dirigir la ejecución de los programas de sanciones financieras selectivas, proteger los sectores vulnerables y fomentar la presentación efectiva de reportes de operaciones sospechosas. En el corazón del enfoque de la CFT del GAFI se encuentran cuatro recomendaciones:

- La Recomendación 5—Delito de financiamiento del terrorismo
- La Recomendación 6—Sanciones financieras elegidas relacionadas con el terrorismo y la financiación del terrorismo
- La Recomendación 7—Sanciones financieras elegidas relacionadas con la proliferación
- La Recomendación 8—Las organizaciones sin fines de lucro (ONG)

Estas recomendaciones significan que para detectar actividades terroristas en las actividades financieras de otra forma legítimas, las instituciones financieras requieren una fuerte aplicación del principio de conozca a su



cliente, además de las políticas y procedimientos de debida diligencia. Normalmente, esto se equilibra con el reporte de transacciones sospechosas que se cree que indica actividades ilícitas que apoyan el terrorismo.

La distinción entre la financiación del terrorismo y el lavado de dinero

A diferencia del ALD, las prácticas preventivas y de investigación de la CFT no necesariamente abordan el producto del delito. En lugar de ello, la realidad indica que los fondos legítimos destinados al terrorismo no necesariamente tienen que ser lavados. Simplemente tienen que ser encubiertos. Sin embargo, lo que el lavado de dinero y la financiación del terrorismo logran, a pesar de los diferentes objetivos finales, es la creación de la oscuridad que rodea el proceso en el que fluyen los fondos. Esta es una práctica notablemente menos desafiante para la financiación del terrorismo ya que los montos involucrados son normalmente menores que los asociados con el lavado de fondos ilícitos. Esto ha impulsado el debate en torno a las

diferencias entre el ALD y la CFT, ya que ambas prácticas se llevan a cabo a través de tres etapas. Se ha creado una difuminación de la línea divisoria entre el delito organizado y las organizaciones terroristas, ya que el continuo del delito/terrorismo aparentemente ha evolucionado para permitir que los grupos recorran la escala en función del entorno en el que operan. No es raro que algunos grupos delictivos demuestren motivaciones políticas, mientras que los grupos terroristas se centran en las ganancias delictivas a través de una fachada alineada a la retórica política. Esto se muestra en ese momento, en cierta medida, en Irlanda del Norte, donde las facciones remanentes de ambas partes están en parte utilizando esa fachada ideológica para enmascarar el delito adquisitivo.

Tal como lo entendemos, el lavado de dinero es la práctica en la que los activos ilícitamente obtenidos se transfieren a fin de proporcionar un velo de legitimidad. Para tener éxito, las actividades de lavado de dinero simplemente tienen que ocultar con eficacia el vínculo entre los fondos y la actividad delictiva original mediante las tres etapas siguientes: colocación, estratificación e integración. Cada etapa facilita una característica particu-

lar que, cuando se combina, permite que los fondos una vez ilícitamente obtenidos y contaminados parezcan legítimos.

De manera similar, la financiación del terrorismo proporciona la capacidad de los terroristas para levantar, mover, almacenar y distribuir los fondos, otros activos o recursos; sin embargo, por lo general se lleva a cabo en una escala menor en comparación con la magnitud de la economía delictiva. A pesar de la priorización de las transacciones de valores más altos asociados con el delito organizado, el enfoque en la financiación del terrorismo ha crecido debido a la mejora de la comprensión y el desafortunado crecimiento de grupos tales como ISIL.

Al igual que el lavado de dinero, la financiación del terrorismo evoluciona continuamente. Sin embargo, existen diferencias fundamentales entre el lavado de dinero y financiación del terrorismo. La principal diferencia es que en el lavado de dinero todo el dinero sujeto al proceso de lavado está sucio desde el principio, ya que se deriva de los productos del delito. Sin embargo, en la financiación del terrorismo, si bien una parte del dinero de los terroristas es, sin duda, producto del delito, una proporción significativa de la misma no es en realidad dinero sucio desde el principio. Naturalmente, si los fondos se consideran ilícitos, es normal asumir que los terroristas recurrirán a actividades delictivas de lavado de dinero para financiar sus actividades.

Donde un grupo terrorista no está más allá de cometer un delito no terrorista para recaudar fondos, el proceso para financiar el terrorismo se convierte en “lavado de dinero al revés” con la asistencia de la legitimidad de los fondos involucrados al inicio del proceso. En otras palabras, el dinero comienza limpio y luego se ensucia debido a las intenciones de sus poseedores; por ejemplo, donaciones de caridad posteriormente objeto de uso terrorista. Por lo tanto, reconocer los fondos relacionados con la financiación del terrorismo requiere el conocimiento de la intención última. Esto se puede lograr mediante la identificación de forma retrospectiva de tipologías sobre la base de los ataques terroristas reales, los supuestos sobre los individuos nombrados en base a las actividades o las asociaciones anteriores o informaciones en directo sobre las actividades y las comunicaciones interceptadas. Con el fin de apoyar de manera efectiva, la CFT requiere un enfoque amplio y sofisticado para la detección de los flujos financieros dirigidos a las células terroristas. Esto incluiría las sugerencias postuladas al final de este artículo, pero también requiere una estrecha colaboración entre los servicios de inteligencia y unidades de inteligencia

financiera/policía, por lo que la explotación máxima de la inteligencia financiera que rodea a sospechosos de terrorismo pueda llevarse a cabo, como fue el caso de la conspiración en el bombardeo líquido de 2006 (Operación Overt).

ALD/CFT contemporáneos

El entorno actual de ALD/CFT se encuentra impulsado por controles y regulaciones financieros más estrictos. Lo que existe es un régimen de ALD/CTF—un régimen formalizado definible para proteger los intereses de negocio en sectores considerados viables en la prevención de la colocación y la estratificación de los fondos ilícitamente obtenidos y el apoyo a la financiación del terrorismo (apuntalados por las Recomendaciones del GAFI). Las Recomendaciones del GAFI revisadas ya han promovido la normalización de las políticas y marcos legales para combatir el lavado de dinero y la financiación del terrorismo como un colectivo.

El desafío es que el ALD y la CFT sólo son iguales donde el dinero asociado con la financiación del terrorismo se deriva de la delincuencia. Además, como el medio ambiente ALD/CFT ha indicado, existe también la aceptación teórica de que delincuentes y terroristas participan en el proceso de colocación, estratificación e integración como un medio para lograr sus intenciones separables. Donde la financiación del terrorismo no se deriva de la delincuencia este modelo no se ajusta. Esto indica que la integración y la estratificación son irrelevantes. Esto significa que la financiación del terrorismo no es tanto “lavado de dinero al revés”, como colocación inversa. Por ejemplo, la financiación no es revelada por su origen, sino por su destino.

El exceso de confianza en las recomendaciones del GAFI revisadas presume que las prácticas de ALD serán eficaces en la identificación de la financiación del terrorismo. Esta presunción ha evolucionado gracias a un nexo evidente entre el delito organizado y el terrorismo. Esto conduce a un exceso de confianza en las recomendaciones revisadas para hacerles frente a ambas actividades igualmente. Sin embargo, mientras que los enfoques que separan el lavado de dinero y la financiación del terrorismo indican una similitud conceptual, hay una diferencia metodológica distinta. Además, esto puede no afectar la investigación previa o posterior al evento, ya que el enfoque es simplemente conectar el dinero a los terroristas y sus patrocinadores.

Por lo tanto, la diferencia esencial entre el ALD y la CFT es:

- El ALD pretende vincular la información disponible sobre el dinero a un tipo de delito. Esto incluye el dinero que entra en el sistema financiero (colocación), lo que ya está en el sistema (estratificación) y la que está saliendo del sistema (integración).
- La CFT busca conectar la información acerca del dinero ya en el sistema (transferencia) o saliendo del sistema para apoyar el terrorismo o un acto terrorista (utilización).

Evaluación

A pesar de la creciente riqueza de evidencia para apoyar la prevención y detección de la financiación del terrorismo, parece que los conocimientos existentes ascienden a la comprensión rudimentaria en una amplia gama de posibilidades. La literatura disponible es vaga en la representación de cómo las fuentes y los métodos han cambiado en los últimos años, el crecimiento potencial de la diversidad y la complejidad o la influencia que ha tenido la legislación ALD/CFT. Por otra parte, estudios de casos documentados dependen de casos resueltos y demuestran esas actividades utilizando empresas de fachada para disimular los beneficiarios efectivos.

Si bien es aceptable revisar los casos anteriores, el enfoque limita la consideración de todas las opciones de financiación del terrorismo (delitos adquisitivos, donaciones, secuestros por rescate, impuestos ilegales, las ONG apropiadas, etc.). Las actividades basadas en la comprensión actual se hacen representaciones de hecho de la financiación del terrorismo apoyadas por la creencia de que las Recomendaciones del GAFI proporcionan seguridad total. Este enfoque está limitando el progreso de la CFT por miedo a aventurarse en el área desconocida de las tendencias y enfoques para la financiación del terrorismo. Por ejemplo, el aumento del uso de la financiación del terrorismo basada en el comercio, abuso de los recursos naturales y la trata de personas. Del mismo modo, las evaluaciones se generalizan con frecuencia o se simplifican demasiado con las unidades nacionales de inteligencia financiera (UIF) que reciben en muchos casos insuficiente cantidad de reportes de operaciones sospechosas (ROS) vinculados a las prácticas terroristas potenciales. Por ejemplo, en 2015 el UIF del Reino Unido recibió 381.882 ROS de los cuales sólo 1.899 fueron identificados como relacionados con la financiación del terrorismo.¹

Por otra parte, las complicaciones se presentan para determinar el origen de los fondos sospechosos ya que las tácticas de financiación del terrorismo simplemente pueden

¹ “Suspicious Activity Reports (SARs) Annual Report,” National Crime Agency, 2015, <http://www.nationalcrimeagency.gov.uk/publications/677-sars-annual-report-2015/file>

involucrar de forma incorrecta que revelan detalles que luego no concuerdan con personas en una base de datos de detección. Los encargados de la detección de la financiación del terrorismo y de desentrañar estas prácticas reciben una tarea casi imposible. Ya que los financistas de terroristas no poseen el monopolio de cualquier fuente o método en particular, tratan de utilizar actores lícitos e ilícitos para financiar actividades no terroristas, (por ejemplo, la conclusión de empréstitos, o la realización de fraudes de caridades o de impuesto sobre el valor añadido), o alinearse con el lavado de fondos ilícitamente obtenidos. Esto permite a los financistas del terrorismo actuar funcionalmente de manera idéntica a comportamientos perfectamente inocentes o al menos políticamente neutrales. Este fue un modelo utilizado en la financiación del Bombardeo de Londres en julio de 2005, en el que el total de los fondos se derivó de un préstamo bancario y retiros de tarjetas de crédito a los que se accede legítimamente, y préstamos estudiantiles falsos se obtuvieron para beneficiar a las familias de los bombarderos.

Por lo tanto, lo que también se está haciendo evidente es la incapacidad para confirmar, o en un aumento mínimo, la sospecha sobre una transacción particular que pueda constituir algún aspecto de la financiación del terrorismo. El grado de sofisticación y complejidad de los sistemas de financiación ilícitos se mantiene prácticamente infinito y limitado en términos reales sólo por la imaginación y la experiencia de los participantes. Por lo tanto, es posible que los terroristas eludan los indicadores de alertas rojas y, posteriormente, reduzcan al mínimo la probabilidad de detección a través de prácticas de debida diligencia profesional de ALD y las prácticas sugeridas en las recomendaciones revisadas del GAFI que apoyan la prevención de la financiación del terrorismo.

Por otra parte, la serie existente de normativas internacionales establecidas por el GAFI no pueden realmente ser totalmente apropiadas para hacerle frente a la financiación del terrorismo como una actividad independiente desde el punto de vista preventivo. A pesar de las sugerencias que indican un cambio en la financiación del terrorismo, que involucra a grupos terroristas que desarrollan comportamientos delictivos para financiar actividades, e indicaciones de Europa que sugieren poca necesidad de utilizar el delito organizado para financiar ataques terroristas, una diferencia clave entre el terrorismo y el delito tiene que ver con la ideología, visto que los

terroristas operan en el nombre de ideales más elevados que pueden no ser compatibles con la actividad delictiva sencilla. Con diferencias metodológicas, la comprensión inexacta e indicadores de alertas rojas mal alineadas, los profesionales de la CFT reciben retos para entender de quién es el dinero que se debe buscar y cuándo se debe destacar la preocupación por el destino de una transferencia. Las prácticas existentes y las perspectivas indican también que el enfoque de CFT se ha hecho parroquial, debido a la serie disponible de tipologías de lavado de dinero que han estrechado el foco a la ALD.

Las finanzas digitales han influido en mayor medida en las prácticas de financiación del terrorismo y es común que los fondos se envíen, por ejemplo, a través de PayPal a raíz de solicitudes en Twitter. Estas transferencias son inmediatas y por lo general caen por debajo del radar de las evaluaciones tipológicas. Del mismo modo, los pagos únicos pueden dejar de recaudar suficientes sospechas para forzar un reporte de operación sospechosa. Incluso cuando se genera, la UIF recipientaria nacional puede no investigarlo.

Conclusión

Si bien muchas de las prácticas se producen bajo el radar de la CFT, las prácticas alineadas con el movimiento de fondos con el propósito de la financiación del terrorismo se oscurecen con las prácticas de ALD solamente para los fines de investigación. Donde la financiación del terrorismo no puede ser identificada por prácticas de ALD, la acción disruptiva limitada o la prevención es posible gracias a la comunidad internacional.

Con el aumento de la presión que emerge del ALD en lugar de la CFT debido a las Recomendaciones del GAFI, las prácticas existentes siguen siendo insuficientes debido a los diferentes enfoques metodológicos que intervienen en el movimiento de fondos con el propósito de terrorismo que son típicamente discretos, irreconocibles y con frecuencia aparecen en las transacciones financieras. Por lo tanto, es probable que las prácticas de ALD tendrían dificultad de detectar dinero transferido a los efectos de la financiación del terrorismo a menos que las cantidades fueron lo suficientemente altas como para justificar la activación de las señales de advertencia, se alinean a propósito con uno o más indicadores comunes de alerta roja, o el propósito verdadero de los fondos se identificara.

Surge entonces la pregunta de si existe la creencia del GAFI de que la financiación del terrorismo continuará adoptando los mismos procesos que los lavadores de dinero, basados

en el hecho de que no están tratando de lavar el producto del delito y asegurar el secreto a largo plazo. Del mismo modo, ¿el escenario actual sugiere esto como un ejemplo de un posible mejor enfoque del GAFI? En su lugar, es evidente que un mayor foco debe estar alineado para volver a calibrar los esfuerzos de interrupción de financiación terrorista con el fin de garantizar que se coloque una mayor atención hacia la financiación del terrorismo de bajo presupuesto.

Por lo tanto, sería conveniente introducir una serie de prácticas adicionales para apoyar las recomendaciones de la CFT sugeridas por el GAFI. Éstas incluyen:

- Fomentar las transacciones sospechosas/ reportes de operaciones sospechosas de bajo nivel para apoyar la mejora en la recopilación de información sobre sospechosos de terrorismo, sus direcciones, familiares y asociados.
- Fomentar la aplicación de la ley para extender el uso de la inteligencia financiera para detectar actividades delictivas, independientemente de los umbrales monetarios.
- La reducción de la aparente facilidad con la que se pueden crear personas jurídicas temporales artificiales con los beneficiarios reales desconocidos.

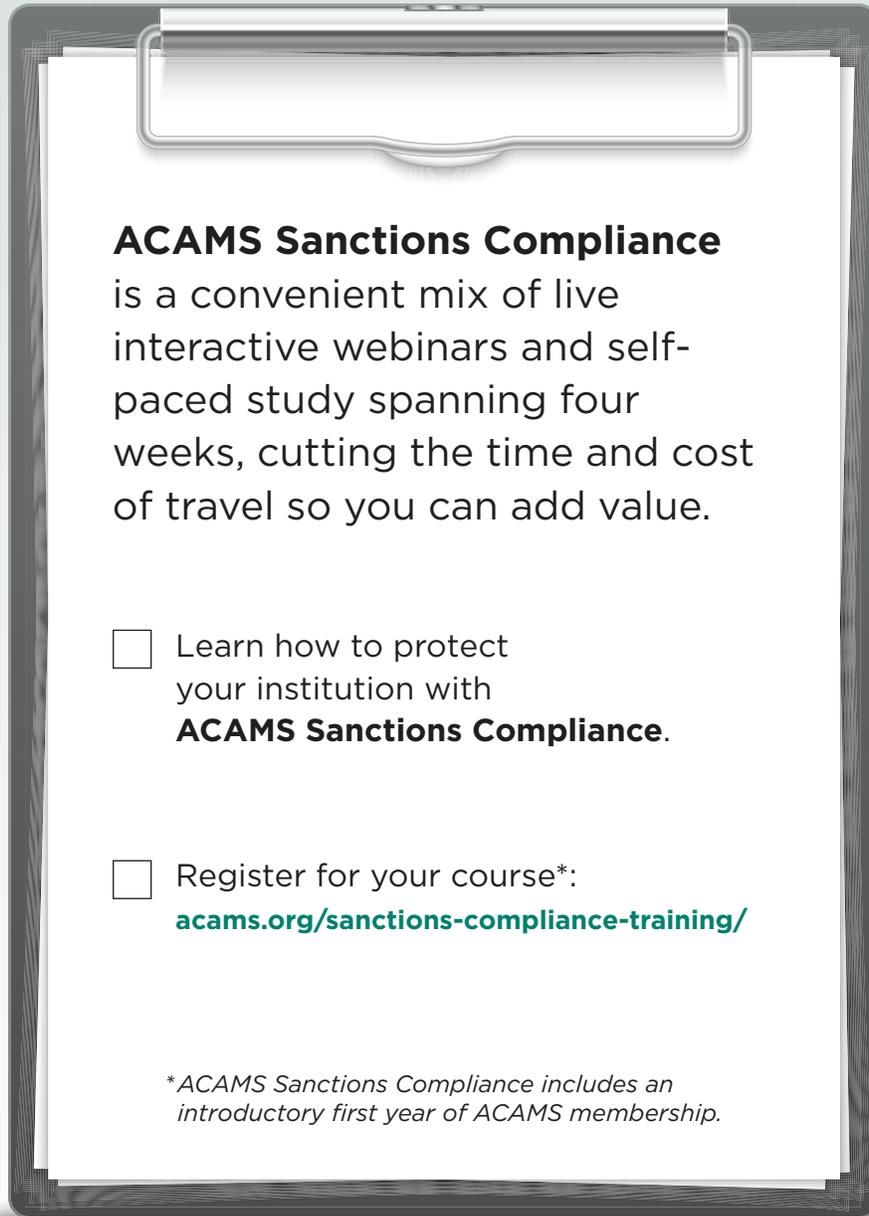
Como la evidencia indica, la financiación del terrorismo adopta el camino de menor resistencia. La cuestión es que este camino puede ser un camino que aún no ha sido identificado, o es un camino en el que los terroristas pueden fácilmente pasar de puntillas sin dejar ningún rastro o sospecha alineados con las Recomendaciones revisadas del GAFI. 

Simon Dilloway, CAMS, director, Lopham Consultancy, South Lopham, Norfolk, Reino Unido, sdilloway@lophamconsultancy.co.uk

Dr. Nicholas Gilmour, instructor de la policía, Centro de Estudios de Defensa y Seguridad, Wellington, Nueva Zelanda, n.j.gilmour@massey.ac.nz

Tristram Hicks, socio, AML Consulting (Global) Ltd, Londres, Reino Unido, tristram.hicks@icloud.com

Sanctions Violations Are Costly. Learning How to Avoid Them Shouldn't Be.



ACAMS Sanctions Compliance is a convenient mix of live interactive webinars and self-paced study spanning four weeks, cutting the time and cost of travel so you can add value.

- Learn how to protect your institution with **ACAMS Sanctions Compliance**.

- Register for your course*:
acams.org/sanctions-compliance-training/

**ACAMS Sanctions Compliance includes an introductory first year of ACAMS membership.*

Definiendo las empresas relacionadas con la marihuana



¿Qué es una empresa relacionada con la marihuana? La respuesta—o más exactamente la definición—debe ser considerada y discutida por todas las instituciones financieras. Independientemente de la política general de la institución hacia las empresas relacionadas con la marihuana (MRB por sus siglas en inglés), las políticas y procedimientos mal contruidos constituyen un alto riesgo para cualquier programa de cumplimiento efectivo. Aunque se anima a las entidades supervisadas a “adoptar un enfoque basado en el riesgo en la evaluación de las relaciones individuales de los clientes, en lugar de negarse a proporcionar servicios bancarios a categorías enteras de clientes sin tener en cuenta los riesgos que presentan”,¹ la postura actual de la mayoría de las instituciones financieras hacia el sector emergente de la marihuana es decir simplemente: “No”. Sin embargo, la mayoría de las instituciones no han definido claramente lo que es una “empresa relacionada con la marihuana” y, por lo tanto, pueden tener políticas y procedimientos poco claros o incompletos que pueden conducir a interpretaciones y aplicaciones incoherentes.

Este artículo comparte un marco global y coherente para la definición de las MRB y para clasificar categorías generales de MRB en tres niveles basados en el riesgo. Las instituciones financieras, reguladores y legisladores pueden encontrar este marco útil al formular, revisar o actualizar sus políticas y procedimientos relacionados con la marihuana.

¿Por qué es esto importante?

La Ley de Sustancias Controladas (CSA por sus siglas en inglés) clasifica la marihuana como una droga de Clase I, que se “considera la clase más peligrosa de drogas con un alto potencial de abuso y severo potencial de dependencia psicológica y/o física” e incluye la heroína, el LSD y el éxtasis.² Como tal, para la CSA “se hace ilícito bajo la ley federal fabricar, distribuir o dispensar marihuana” y “porque la ley federal prohíbe la distribución y

venta de la marihuana, las transacciones financieras relacionadas con una empresa relacionada con la marihuana, normalmente implican fondos derivados de actividades ilegales”.³ Incluso si la marihuana se reprogramara como droga de Clase II, que abarca “fármacos con alto potencial de abuso”, incluyendo el opio, la cocaína y la metanfetamina, la industria de la marihuana probablemente continúe siendo percibida como de alto riesgo y sujeta a escrutinio legal permanente y regulatorio. Por otra parte, una reprogramación de la marihuana es poco probable en el corto plazo. El 11 de agosto, la Administración de Control de Drogas denegó peticiones para reprogramar la marihuana “ya que no cumple con los criterios para el uso médico aceptado actualmente en tratamiento en los EE.UU., hay una falta de seguridad aceptada para su uso bajo supervisión médica, y tiene un alto potencial para su abuso”.⁴

De acuerdo con la Red Contra los Delitos Financieros:

“Debido a que la ley federal prohíbe la distribución y venta de la marihuana, las transacciones financieras relacionadas con una empresa relacionada con la marihuana generalmente implicarían fondos derivados de una actividad ilegal. Por lo tanto, se requiere que una institución financiera presente un ROS sobre actividad que implique una *empresa relacionada con la marihuana* (incluyendo las debidamente autorizadas por la ley estatal)... la decisión de abrir, cerrar, o rechazar cualquier cuenta o relación particular debe ser hecha por cada institución financiera sobre la base de una serie de factores específicos a esa institución.... El conocimiento de debida diligencia a fondo del cliente es un aspecto crítico para realizar esta evaluación”.⁵

Con el fin de responder eficazmente a estas directrices, todas las instituciones financieras tienen que determinar en primer lugar cómo definen “empresa relacionada con la marihuana” y luego desarrollar políticas y procedi-

¹ “FDIC Encourages Institutions to Consider Customer Relationships on a Case-by-Case Basis,” FDIC, 28 de enero del 2015, <https://www.fdic.gov/news/news/press/2015/pr15009.html>

² “Drug Schedules,” Drug Enforcement Agency, <https://www.dea.gov/druginfo/ds.shtml>

³ “FIN-2014-G001: BSA Expectations Regarding Marijuana-Related Businesses,” FinCEN, 14 de febrero del 2014, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-G001.pdf

⁴ “DEA Announces Actions Related to Marijuana and Industrial Hemp,” DEA, 11 de agosto del 2016, <https://www.dea.gov/divisions/hq/2016/hq081116.shtml>

⁵ “FIN-2014-G001: BSA Expectations Regarding Marijuana-Related Businesses,” FinCEN, 14 de febrero del 2014, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-G001.pdf

mientos basados en riesgo específico para las MRB, incluyendo los métodos eficaces para identificarlas y tratarlas sistemáticamente.

Enfoque de tres niveles de riesgo

El siguiente es el marco que el MRB Monitor utiliza para definir las MRB y para categorizarlas en tres niveles basados en el riesgo en función de la medida en que una empresa toca la marihuana literalmente e interactúa con otras MRB. Este enfoque escalonado puede ser de utilidad para las instituciones financieras—incluidas las que ingenuamente creen que tienen cero exposición a la industria—para determinar en qué nivel de la cadena de suministro de marihuana pueden estar dispuestas a ofrecer los servicios a sabiendas y en qué medida necesitan actualizar políticas, procedimientos y métodos de diligencia debida para identificar efectivamente, medir y mitigar los riesgos relacionados con la marihuana.

MRB de Nivel I

Las MRB de Nivel I son consideradas las más riesgosas, ya que, literalmente, tocan la marihuana en algún momento a lo largo de la cadena de suministro y con mayor claridad “fabrican, distribuyen o dispensan marihuana”.⁶ Las MRB de Nivel I en general incluyen las empresas con licencia de un estado o “comercio legítimo relacionado con la marihuana”, como se define en las propuestas leyes federales bancarias de la marihuana.⁷ Las MRB de Nivel I incluyen, pero no se limitan a, las siguientes categorías:

- Semillas de Cannabis
- Siembra
- Cultivo
- Cosecha
- Procesamiento
- Embalaje
- Productos de infusión
- Venta al por mayor
- Pruebas
- Transporte
- Dispensario médico
- Venta recreativa al por menor



- Entrega al por menor
- Cannabidiol
- Cáñamo industrial

Dentro de cada una de estas categorías surge una serie de posibles sub-categorías. Por ejemplo, el “Cultivo” podría incluir al aire libre, de interior y mixto (es decir, tanto en interiores como al aire libre). “Procesamiento” incluye una amplia variedad de empresas, como las que procesan la planta de marihuana o extractos de aceites para su uso en productos comestibles. Algunas categorías de Nivel I, como “Pruebas” y “Transporte”, pueden ser menos evidentes que el cultivo, el procesamiento, la distribución o la venta de marihuana y por lo tanto son más propensos a ser pasadas por alto por los equipos de cumplimiento. Los laboratorios de “prueba” que analizan la marihuana para toxinas y las compañías de “transporte” que mueven la marihuana desde el punto A al punto B pueden no necesariamente tener licencia del estado como una “empresa de marihuana”, pero se incluyen en el Nivel I, ya que, literalmente, tocan la marihuana y se podría presumir que obtengan todos sus ingresos de otras MRB de Nivel I. Otras categorías como los productos “Cannabidiol” y “Cáñamo industrial” a menudo se cree de ellos erróneamente que son legales (incluso a nivel federal), pero en realidad no lo son y, por lo tanto, a veces se los pasa por alto o son excluidos por el protocolo de cumplimiento. Al lego puede sorprenderlo el número de categorías asociadas con las MRB de Nivel I. En los primeros días de la industria de la marihuana, las MRB se integraban con frecuencia verticalmente y realizaban todas las actividades relacionadas con

el cultivo, la elaboración y venta de marihuana y productos relacionados. Sin embargo, como la industria de la marihuana continúa creciendo y evolucionando, cada vez se fragmenta más ya que las empresas se especializan en cada paso del proceso.

Por último, cualquier entidad que tenga un interés o control financiero (sin tener en cuenta el porcentaje de propiedad) en una MRB de Nivel I, incluyendo empresas fantasmas y de gestión que pueden estar buscando “ocultar o disfrazar participación de la actividad comercial relacionada con la marihuana”,⁸ también se clasifican como MRB de Nivel I.

MRB de Nivel II

Las MRB de Nivel II se consideran menos riesgosas que las MRB de Nivel I porque no “fabrican, distribuyen o dispensan marihuana” directamente y no suelen tener licencia del estado como “empresa de marihuana” por sí mismo. Sin embargo, las MRB de Nivel II se consideran “empresas” de marihuana en el marco, ya que se centran específicamente en el suministro de productos y servicios para las MRB de Nivel I y la industria de la marihuana en general. De la mayoría, si no todas, de Nivel II podría esperarse razonablemente que sus ingresos provengan de actividades de MRB de Nivel I y relacionadas con la marihuana. Por lo tanto, las MRB de Nivel II podrían ser consideradas “cómplices” del Nivel I de MRB que está más claramente definido y es federalmente ilegal. De acuerdo con un artículo de *ACAMS moneylaundering.com* de enero de 2016, los “funcionarios de los



⁶ *Ibid.*

⁷ U.S. Senate, “S. 1726: Marijuana Businesses Access to Banking Act of 2015,” 9 de julio del 2015, <https://www.congress.gov/bill/114th-congress/senate-bill/1726/text>; U.S. House of Representatives, H. R. 2076, 28 de abril del 2015, <https://www.govtrack.us/congress/bills/114/hr2076/text>

⁸ “FIN-2014-G001: BSA Expectations Regarding Marijuana-Related Businesses,” FinCEN, 14 de febrero del 2014, https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-G001.pdf

EE.UU. están elaborando una guía para las instituciones financieras preocupadas por aceptar depósitos de terceras empresas que sirven a los vendedores de marihuana con licencia del estado porque podría violar las normas federales de antilavado de dinero”, pero a partir de agosto de 2016, ninguna guía ha sido emitida.⁹ Las MRB de Nivel II se refieren a veces como MRB “auxiliares” o “indirectas” en oposición a las MRB de Nivel I “directas”. Las MRB de Nivel II incluyen, pero no se limitan a, las siguientes categorías:

- Suministros hidropónicos
- Fuentes de embalaje
- Licencias de consultoría
- Asociaciones industriales
- Procesadores de pago
- Publicidad y relaciones públicas
- Entrenamiento y educación
- Software de marihuana

MRB de Nivel III

Las MRB de Nivel III se consideran el nivel de menor riesgo y no “empresas de marihuana” en el sentido más estricto. A diferencia de las MRB de Nivel II, las MRB de Nivel III no se centran específicamente en vender a MRB de Nivel I o a la industria de la marihuana. Además, vender a las MRB de Nivel I es incidental al negocio y los ingresos en general de las MRB de Nivel III. Sin embargo, las MRB de Nivel III son negocios específicos conocidos para servir las MRB de Nivel I y, como tales, podrían ser consideradas “cómplices” de una actividad ilegal en un sentido estricto. Las MRB de Nivel III pueden ser cualquier tipo de negocio, pero en general incluyen empresas de servicios profesionales (por ejemplo, abogados, contadores, agentes registrados, etc.) y dueños de propiedades comerciales. Un escenario podría incluir una firma de servicios profesionales que, con conocimiento, ayuda a una MRB de Nivel I para crear una empresa de “gestión” con el presunto objetivo de ayudar a la MRB a evadir la detección como relacionada con la marihuana. Otro escenario podría incluir un inversor de bienes raíces que alquila locales comerciales a una MRB de Nivel I.

Margen de maniobra

Este marco permite un margen de maniobra y las instituciones financieras pueden aplicarlo a “adoptar un enfoque basado en el riesgo en la evaluación de las relaciones individuales de los clientes”.¹⁰ Unos pocos ejemplos podrían incluir:

- *Aumentar el Nivel de Riesgo:* Aunque la mayoría de las empresas de servicios profesionales que se sabe sirven las MRB de Nivel I podrían ser categorizadas como de Nivel III (el riesgo más bajo), si una empresa en particular es conocida por centrarse específicamente en la industria de la marihuana y uno puede razonablemente esperar que la mayor parte de sus ingresos vengan de las MRB de Nivel I, razonablemente podría clasificarse como de Nivel II.
- *Reducir el Nivel de Riesgo:* Aunque la mayoría de las compañías de vehículos blindados que se sabe sirven las MRB de Nivel I podrían ser categorizadas como de Nivel I (el nivel más alto de riesgo), si una empresa en particular no se centra en la industria de la marihuana, genera sólo un pequeño porcentaje de sus ingresos de MRB de Nivel I y no toca la marihuana (por ejemplo, tal vez sólo mueven efectivo), razonablemente podría ser clasificada como de Nivel II o Nivel III.
- *Excluir por Completo:* Una institución financiera puede optar por excluir por completo las empresas de servicios públicos de este marco, a pesar de que pueden ser conocidas por servir las MRB de Nivel I, ya que el porcentaje de sus ingresos de las MRB de Nivel I es extraordinariamente pequeño.

Una nota sobre el estado de la licencia de marihuana

La mayoría de los estados que han legalizado la marihuana lo han hecho en relación con robustos procesos de aplicación de marihuana, normas y reglamentos, que, en general, culminan en las MRB de Nivel I “con licencia” del estado. Sin embargo, algunos estados legalizados no tienen ningún marco para la concesión de licencias o regulación de las MRB de Nivel I (por ejemplo, California, Michigan, Montana), pero claramente existen

y operan las MRB de Nivel I dentro de esos estados. Por esta razón, si una empresa en particular está “con licencia” no es directamente relevante para determinar si ese negocio está relacionado con la marihuana. Para tomar esta lógica un paso más allá, este marco considera que las empresas con licencias de marihuana pendientes, fallidas y revocadas/canceladas también son las MRB de Nivel I.

Conclusión

La decisión de hacer negocios con cualquier cliente en última instancia recae en cada institución financiera, que tiene el privilegio de negarse a abrir una cuenta o cerrar una cuenta, siempre y cuando la razón para hacerlo no está motivada por la discriminación contra una clase protegida.¹¹ El objetivo de este artículo no es convencer a las instituciones financieras de servir o no servir a las MRB como una categoría entera, sino para compartir un marco para el desarrollo de políticas y procedimientos integrales para hacer coherentes y efectivas las decisiones basadas en el riesgo con respecto a las empresas relacionadas con la marihuana. 

Steven Kemmerling, fundador y CEO, MRB Monitor, Chicago, IL, EE.UU., steve@mrmonitor.com

La información proporcionada en este artículo no pretende ser y no debe ser considerada como un consejo o una guía autorizada sobre cualquier aspecto de cumplimiento de instituciones financieras con las leyes estatales, federales o internacionales. MRB Monitor no asume ninguna responsabilidad y no tendrá ninguna responsabilidad por la exactitud o integridad de la información contenida en este artículo. Las instituciones financieras deben consultar con sus departamentos de cumplimiento y legales con respecto a cualquier información y las interpretaciones de las informaciones como éstas pueden referirse a hechos y circunstancias de la institución y la aplicación de los procedimientos de cumplimiento.

⁹ Colby Adams, “FinCEN Weighs Bank Guidance for Ancillary Businesses Linked to Weed Trade,” ACAMS moneylaundering.com, 27 de enero del 2016, <http://www.moneylaundering.com/News/Pages/137002.aspx>

¹⁰ “FDIC Encourages Institutions to Consider Customer Relationships on a Case-by-Case Basis,” FDIC, 28 de enero del 2015, <https://www.fdic.gov/news/news/press/2015/pr15009.html>

¹¹ “Exam Procedure Update: Marijuana-Related Businesses,” Washington State Department of Financial Institutions, 20 de mayo del 2016, www.dfi.wa.gov/documents/credit-unions/marijuana-exam-procedures.pdf

Logrando el **riesgo**
de la empresa cuando las leyes
de ALD y de
privacidad entran en
conflicto



El riesgo empresarial es un tema conocido pero desafiante dentro de la lucha de antilavado de dinero (ALD) y la comunidad de cumplimiento. Con el fin de ofrecer valor a clientes y accionistas, una institución debe entender y manejar los riesgos que enfrenta en toda la organización. Los riesgos son inherentes a cualquier empresa y a menudo se clasifican como estratégicos, operacionales, de cumplimiento y de reportes financieros. Una visión empresarial de riesgo captura todos los elementos empresariales y la forma en que se cruzan para ofrecer valor e impulsar el éxito. También identifica los eventos potenciales que pueden afectar a una institución de manera que los riesgos asociados pueden ser gestionados adecuadamente. La identificación y la gestión del riesgo es especialmente importante en el entorno regulatorio elevado de hoy, donde los programas de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) han sido objeto de un escrutinio intenso que resulta en algunas acciones de aplicación de muy alto perfil y multas en los últimos años.

Los desafíos del futuro

Las instituciones financieras reguladas y otras se enfrentan a enormes desafíos al tratar de ver el riesgo en toda la empresa. La calidad de datos incoherentes, los silos de negocios, los sistemas dispares y las cantidades masivas de información cambiante hacen que sea difícil que las organizaciones reúnan fácilmente la inteligencia que necesitan para identificar, evaluar y gestionar los riesgos de la empresa. A esta mezcla se añade la multitud de leyes que rigen los datos financieros transnacionales que vienen con la globalización. Para las empresas multinacionales, cumplir requisitos regulatorios a la par de cumplir con leyes jurisdiccionales de privacidad diferentes complica aún más su capacidad para lograr una visión empresarial de riesgo.

En un informe del Instituto de SWIFT, "Multinational Banking and Conflicts Among U.S.-EU AML/CTF Compliance and Privacy Law: Operational and Political Views in Context", la Dra. Michelle Frasher, indica que "los datos financieros son tanto comerciales como una fuente de inteligencia y se rigen por dos regímenes jurídicos a menudo opuestos".¹ Publicado el 1 de julio del 2016, el documento analiza las leyes de antilavado de dinero/la lucha contra el financiamiento del terrorismo (ALD/CTF) y de protección de datos de los EE.UU. y de la UE e identifica 19 áreas de cumplimiento que plantean un desafío a las multinacionales que integran la privacidad en sus operaciones de AML/CTF. Estas incluyen actividades relacionadas con el cumplimiento con el potencial de riesgo de regulación y/o a la reputación, tales como:

- Las solicitudes de datos por parte de autoridades locales
- La recogida de datos sensibles
- Transferencias en que participan personas políticamente expuestas, familiares y asociados
- Cumplimiento del proveedor con el Escudo de Privacidad EE.UU.-UE
- Prohibición del uso de datos de coconocimiento a su cliente (KYC) con fines comerciales sobre titulares de los datos de la UE

La Dra. Frasher señala cómo la Cuarta Directiva sobre ALD de la UE "promueve programas de cumplimiento en toda la empresa con la protección de datos en todo el grupo", mientras que la ley estadounidense "restringe los datos debido a temas de confidencialidad y no requiere de la privacidad en los programas de cumplimiento".² Por lo tanto, en un mundo globalizado el concepto de una visión empresarial de riesgo se convierte en un desafío mayor cuando deben respetarse las normas de privacidad de múltiples jurisdicciones.

Muchos países tienen leyes que hacen que sea ilegal para las entidades, tales como los bancos extranjeros con sucursales, compartir cierto tipo de información a través de fronteras. Esto plantea la pregunta: ¿Son las expectativas regulatorias realistas y es una visión del riesgo de toda la empresa aún posible para los bancos globales?

Problemas de privacidad

La dicotomía de ALD y la privacidad es un enigma común de las instituciones globales. Cuando se opera en mercados extranjeros, la falta de comprensión de datos y requisitos

reglamentarios locales aumenta el riesgo potencial de grandes multas. Ya sea que la organización opte por implementar un programa de BSA/ALD consolidado o sigue uno en el que algunos o todos los controles de cumplimiento se gestionan exclusivamente en las filiales, subsidiarias o líneas de negocio, los reguladores (en especial los de los EE.UU.) siguen exigiendo una total transparencia a pesar de las leyes de privacidad y las diferencias culturales de otros países. El Manual de Examen de BSA/ALD del Consejo de Exámenes de las Instituciones Financieras Federales proporciona instrucciones muy específicas a los examinadores para evaluar la idoneidad de los sistemas de bancos de los EE.UU. al gestionar los riesgos de sus sucursales y oficinas en el extranjero. También proporciona instrucciones específicas para evaluar la capacidad de un banco al poner en práctica sistemas eficaces de supervisión y presentación de reportes. Los examinadores entienden que las leyes de privacidad en una jurisdicción extranjera pueden impedir que una sucursal o subsidiaria comparta información con su casa matriz en los EE.UU. Sin embargo, se espera que la supervisión del cumplimiento de las sucursales y subsidiarias en el extranjero asegurarán que políticas, procedimientos y procesos adecuados estén en su lugar para proteger contra los riesgos de

La dicotomía de ALD y la privacidad es un enigma común para las instituciones globales

lavado de dinero y la financiación del terrorismo. Aunque los gobiernos federales, estatales y locales de los EE.UU. han implementado leyes para proteger muchos aspectos de la vida privada de los estadounidenses, algunas áreas de tratamiento de datos personales siguen sin estar regulados. La Ley Gramm-Leach-Bliley prevé la protección de información financiera personal como nombre y número de cuenta. Sin embargo, existe una regulación limitada sobre la recogida de información. Por el contrario, la UE considera la privacidad como un derecho humano y por lo tanto regula la recogida y tratamiento de la información de identificación personal. La "Directiva de la Unión Europea sobre la protección de las personas con respecto al tratamiento de datos personales y sobre la libre circulación de estos datos" (Directiva de la UE) proporciona un marco

¹ Dra. Michelle Frasher y Brian Agnew, MPP, "Multinational Banking and Conflicts Among US-EU AML/CTF Compliance and Privacy Law: Operational and Political Views in Context," SWIFT Institute Working Paper No. 2014-008, 1 de julio del 2016, http://www.swiftinstitute.org/wp-content/uploads/2016/07/SIWP-2014-008-Conflicts_US_EU_AML_CTF_FINAL-1.pdf

² Ibid.

para la privacidad de los datos en toda Europa. Aún así, cada estado miembro de la UE debe aprobar su propia ley de privacidad local basándose en la Directiva, por lo que las leyes varían entre los miembros de la UE. Esta incoherencia hace que sea difícil para una institución mundial reunir y procesar información de forma centralizada con el fin de evaluar y gestionar los riesgos en toda la empresa. Las cuestiones de privacidad transfronterizas también han causado conflictos legales de cumplimiento y de la ley. En Asia-Pacífico, las instituciones financieras deben hacerles frente a los reguladores en diferentes jurisdicciones completamente autónomas. No existe un marco como la Directiva Europea para proporcionar orientación sobre las leyes de privacidad, lo que resulta en poca o ninguna superposición y reglamentos que no siempre se documentan en inglés.

La obtención de un equilibrio viable

Las cuestiones que plantea el conflicto de la protección de datos y las leyes de secreto bancario sólo se pueden resolver si existe armonía entre los requisitos reglamentarios y de datos. A falta de armonía, los bancos y los reguladores deben esforzarse para abordar estas cuestiones. Mientras que la Comisión Federal de Comercio y el Departamento de Comercio han iniciado esfuerzos para desarrollar una política de privacidad uniforme para los EE.UU., se espera que su implementación tome varios años. Por lo tanto, es responsabilidad de los bancos acumular los requisitos de privacidad desde el principio en el diseño de modelos operativos globales y sistemas de tecnología de la información. Mediante la integración de la privacidad en el diseño de todo lo que entra en contacto con la información personal, la organización crea un modo de funcionamiento por defecto. Por el lado empresarial, las cláusulas de consentimiento en los acuerdos de los clientes permitirán el uso de datos de los clientes para apoyar la vigilancia del ALD. Por el lado de la tecnología, los estrictos permisos de usuario aseguran que se accede y se ve en una base de las necesidades de conocer los datos. Mientras los departamentos de cumplimiento necesitan sistemas que optimizan la eficiencia operativa, la conformación con las normas de privacidad también se requiere. Esto hace que el manejo de la información personal y sus riesgos pasen al más amplio entorno de gestión de riesgos estratégicos empresariales, que es el objetivo final.

En toda la UE y en otros lugares, estamos empezando a ver algunos avances que se mueven en la dirección correcta. En enero de 2016, SWIFT anunció que más de 2.000 instituciones financieras en más de 200 países y territorios se habían anotado en su registro de KYC.³ Este repositorio centralizado mantiene un conjunto estandarizado de información KYC para los bancos correspondientes, los distribuidores de fondos y custodios. Soluciones estandarizadas, impulsadas por la comunidad, como ésta, nos pueden acercar al intercambio de información y a un equilibrio más viable entre la privacidad y los requisitos de ALD.

En octubre de 2014, el Grupo de Acción Financiera Internacional, dio a conocer su orientación sobre “La Transparencia y la Propiedad Efectiva”. Para facilitar un nivel práctico de la cooperación internacional, la guía incluye requisitos específicos documentados en las Recomendaciones 24 y 25.⁴ Las nuevas medidas sobre la propiedad efectiva fueron tomadas en 2016 cuando la Red Contra los Delitos Financieros del Departamento del Tesoro de los EE.UU. publicó una regla final sobre medidas de diligencia debida. A menudo llamado el “quinto pilar” de BSA/ALD, ahora se exige a las instituciones financieras identificar y verificar la identidad de los beneficiarios de una entidad legal en el momento en que la persona jurídica abre una nueva cuenta, así como el desarrollo de perfiles de riesgo y conducta en curso en el seguimiento de los clientes.

Es alentador ver que algunas leyes de privacidad están siendo examinadas en ciertas jurisdicciones de la UE, porque los gobiernos, las instituciones y las agencias de control legal están reconociendo que son un impedimento para la identificación de las actividades de lavado de dinero. Un proyecto de ley elaborado por el Ministerio de Justicia de Alemania permite a las autoridades confiscar mercancías sospechosas de ser compradas con dinero mal habido y se invierte la carga de la prueba al obligar a las personas bajo investigación comprobar que los activos fueron adquiridos legalmente.

Esta ley podría ser un hito en la reducción de actividades de la mafia en Alemania, bien conocida como un paraíso para la inversión de la mafia. También podría ser una gran victoria para los buenos si se modifican las leyes actuales de privacidad.

El logro de riesgo de la empresa

¿Es posible una visión empresarial de riesgo en el entorno actual? La respuesta es sí. Sin embargo, es algo lento y requiere la cooperación entre las jurisdicciones y gobiernos, así como las regulaciones en armonía con las leyes de privacidad. Además, se requiere de soluciones tecnológicas capaces de manejar el riesgo transfronterizo y con opciones de entrega flexibles (por ejemplo, despliegues organizados, in situ e híbridos) para acomodar las diferencias jurisdiccionales.

Para lograr una visión amplia de los riesgos, las instituciones deben buscar soluciones con características robustas y funcionalidad, tales como:

- Escalabilidad para manejar las masivas cantidades de datos de clientes y de referencia
- Vigilancia actual para capturar la información en constante cambio
- Coherencia y estandarización a través de líneas de negocio para destruir los silos y facilitar el intercambio de información
- Tecnología de vanguardia que emplee aprendizaje por medio de máquinas, inteligencia artificial, visualización de datos, alineación rotacional en coincidencias de nombres para facilitar la resolución de entidades y priorización integral de alerta y gestión
- Herramientas de análisis de enlace avanzadas que puedan identificar las relaciones entre las jurisdicciones sin violar las leyes de privacidad locales

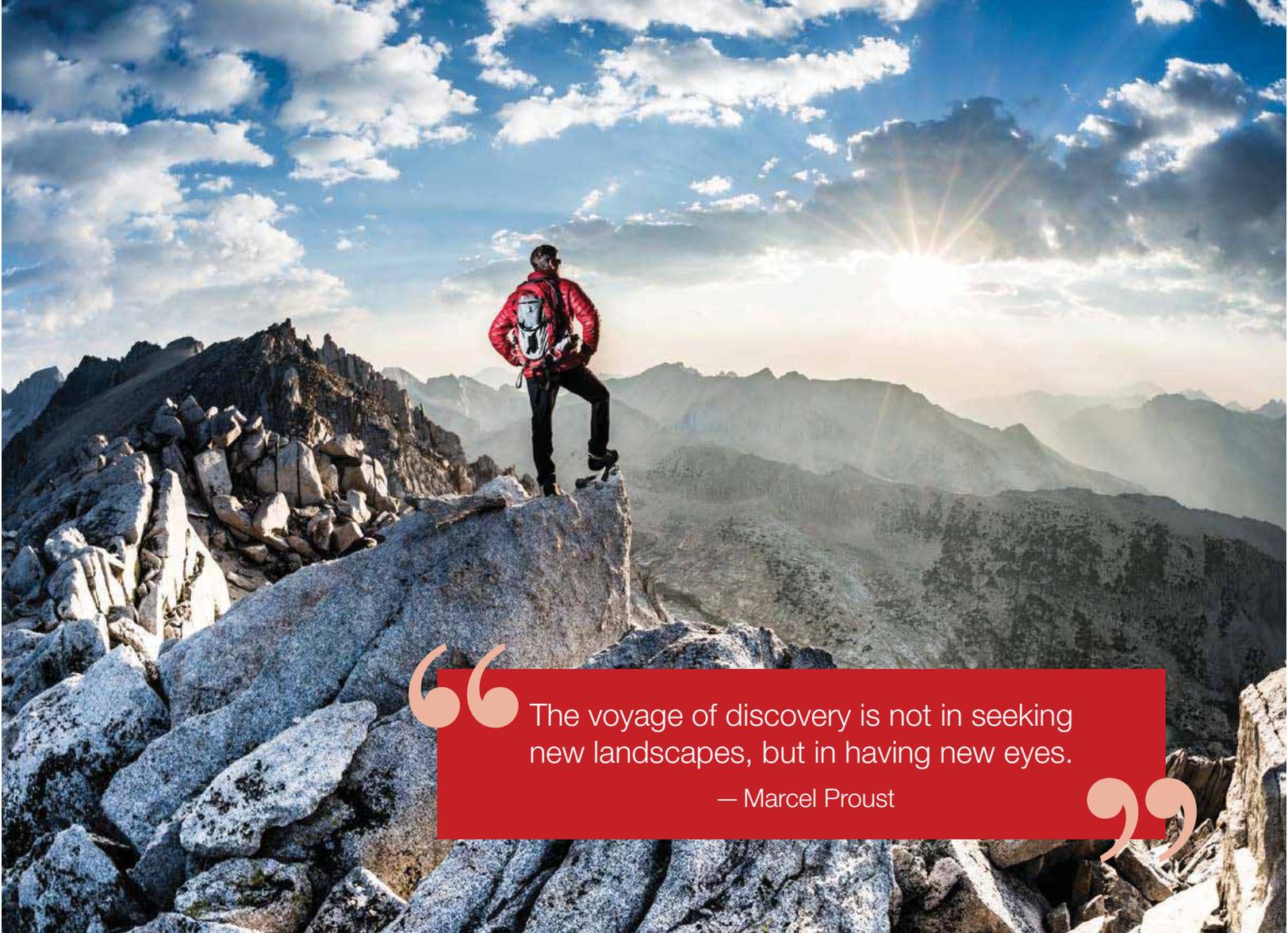
Conclusión

Mientras los requisitos de ALD y las leyes de privacidad sigan enfrentadas, la capacidad de identificar de forma proactiva y gestionar el riesgo en toda la empresa seguirá siendo un reto especialmente para las instituciones globales. Afortunadamente, la cooperación entre los gobiernos, las agencias de control legal, los reguladores y otras entidades y la tecnología más potente están ayudando a traer una visión empresarial de riesgo dentro del alcance. **FA**

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

³ “SWIFT’s KYC Registry surpasses 2,000 financial institutions,” 19 de enero del 2016, https://www.swift.com/insights/press-releases/swift_s-kyc-registry-surpasses-2_000-financial-institutions

⁴ FATF Guidance, “Transparency And Beneficial Ownership,” octubre de 2014, <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf>



“The voyage of discovery is not in seeking new landscapes, but in having new eyes.”
— Marcel Proust

Gain a new perspective on enterprise risk with SBS' SAFE Advanced Solutions® Visual Intelligence Platform. Its powerful visualization and robust functionality enable you to identify, assess and manage risk across the enterprise.

Think Big — handle scale, scope and uncertainty with confidence. Capture constantly changing risk in massive stores of data with dynamic surveillance for KYC screening.

Reach Across Silos — break down barriers with a consistent methodology for entity resolution that facilitates risk management across customers, lines of business and your entire organization.

See it All — bring actionable intelligence to your desktop with interactive data visualization. Manage workflows, view event timelines, see alerts prioritized by risk, identify links and more — all from a configurable dashboard.



SAFE BANKING SYSTEMS

www.safe-banking.com

Find risk that other systems miss. Call **+1 631-547-5400** or contact **sales@safe-banking.com**.

Cuando dos mundos chocan

Durante dos días en junio, el Consorcio de Certificación de la Criptomoneda (C4) fue sede de la primera edición de la Conferencia de Formación Blockchain en MaRS Discovery District en Toronto, Canadá. Este evento logró que algunas de las mentes más brillantes de Fintech se reunieran con empresarios, banqueros, reguladores, profesionales de antilavado de dinero (ALD) y agentes del control legal, para compartir una serie de conocimientos e ideas sobre un tema simple pero revolucionario: cadenas de bloques (blockchains, en inglés).

El consenso predominante en la conferencia fue que las cadenas de bloques, y por extensión las criptomonedas como Bitcoin, desempeñarán un papel cada vez más influyente en la economía mundial durante la próxima década. Sin embargo, se acordó que nadie puede predecir con exactitud el impacto exacto que esta tecnología tendrá sobre el comercio, la sociedad y el ALD.

Sin embargo, esta idea no impidió que los asistentes establecieran hipótesis de escenarios futuros en los que la tecnología de cadenas de bloques podría convertirse en la base para muchas empresas diarias, tales como el alquiler de un coche o la verificación de la identidad. Por ejemplo, un alto miembro de la comunidad de las cadenas de bloques que asistía a la conferencia predijo que, dentro de 10 años, la industria tradicional de la banca como la conocemos podría reducirse a una fuerza de trabajo que es sólo una tercera parte de lo que es hoy debido a las eficiencias que pueden ofrecerse a través de las cadenas de bloques de registros descentralizados y sin cuentas.

Cadenas de bloques y el ALD

Si esta teoría se manifiesta en la realidad se probará con el tiempo, pero los retos que la tecnología de cadenas de bloques presenta actualmente para los profesionales de ALD no se basan en una revolución de este tipo; existen ahora, pero poco se les toma en cuenta.

Las cadenas de bloques son la tecnología subyacente que sustenta las criptomonedas. Operan sobre el principio de que un sistema de contabilidad descentralizado y amplia-

mente distribuido puede utilizarse para grabar los registros permanentes e incorruptibles con la ayuda de la criptografía y una compleja red mundial de centros de verificación llamados nodos.

La combinación de la criptografía y la descentralización permiten que la tecnología de cadenas de bloques cumpla con las altas expectativas que se le atribuyen. Por ejemplo, tener un único libro de registros disponible públicamente y transparente para varios actores sin necesidad de terceros de confianza (intermediarios).

Algunos de los servicios financieros tradicionales, (por ejemplo, los productos asociados a las relaciones de financiación del comercio y la banca correspondiente), se podrían modificar drásticamente por medio del uso de la tecnología de cadenas de bloques. En consecuencia, los profesionales de ALD que entienden esta tecnología también estarán en gran demanda.

Criptomonedas

La remesa de fondos entre las personas o entidades en un libro de contabilidad descentralizado digital, con el apoyo de la tecnología de cadenas de bloques, se ve muy diferente de lo

que se ve en los libros mayores centralizados dentro del sistema bancario tradicional de hoy. Esta discrepancia altera la percepción de lo que puede ser inusual o sospechoso y, como resultado, un nuevo enfoque es requerido por los profesionales de ALD para identificar con precisión y reportar operaciones inusuales.

En el sistema tradicional, los bancos envían transferencias por lo que pueden ser complicadas relaciones de banca correspondiente. Por ejemplo, en el caso más sencillo, si el cliente subyacente (Alfred) del Banco A tiene que enviar un telegrama al cliente subyacente (David) del Cambista D, esto se logra fácilmente si los bancos A y D tienen una relación bancaria correspondiente. El Banco A de Alfred transfiere los fondos directamente a la cuenta del Cambista D, que se acreditan a David. A menudo, las relaciones correspondientes no son tan simples y el Banco A tendría, por ejemplo, que transferir al Banco B, que tiene una relación de correspondencia bancaria con la Cooperativa de Crédito C, cuyo cliente subyacente es el Cambista D. En este ejemplo se suponen honorarios y la duplicación de trabajo en cada instancia de la ruta.

Si se hubiera utilizado la tecnología de cadenas de bloques, el Banco A potencialmente podría transferir fondos directamente al Cam-

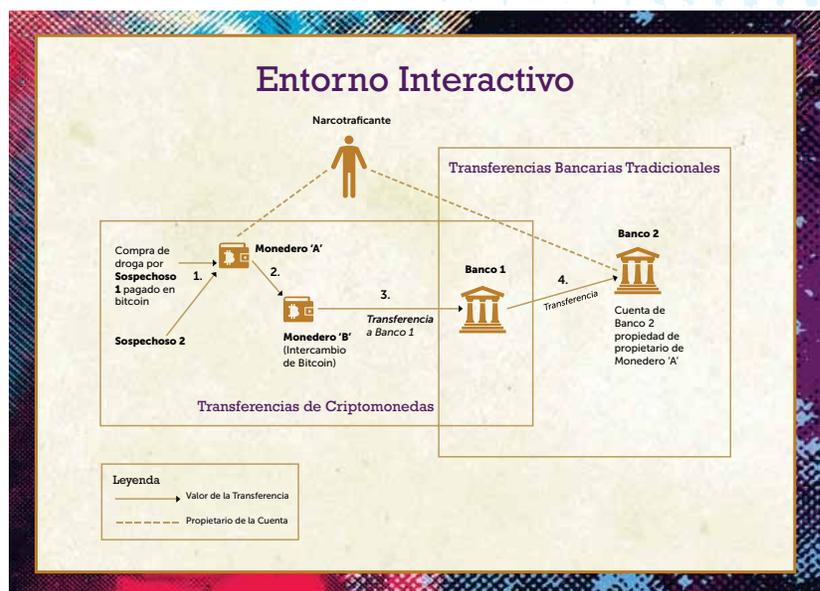


Figura 1



bista D, sin la necesidad de intermediarios. Esto se debe a que la tecnología de cadenas de bloques da a ambas partes que no se conocen entre sí la capacidad de realizar transacciones, sin temor a que se haya cometido fraude y sin la necesidad de intermediarios.

Hay varios proveedores de soluciones de terceros en el mercado que ofrecen herramientas para ayudar en la identificación de transacciones sospechosas o inusuales en cadenas de bloques tales como Bitcoin. Empresas como Blockchain Intelligence Group con sede en Vancouver ya han desarrollado sofisticados sistemas de monitoreo de transacciones de gestión de alertas y casos de aplicación en este mundo digital. Sin embargo, se recomienda que antes de dedicarse a vendedores en el espacio de cadenas de bloques, los profesionales de ALD se eduquen sobre los fundamentos de la tecnología y

de cómo las criptomonedas de cadenas de bloques se utilizan no sólo por los malos actores, sino para fines legítimos también.

Para ayudar a darle sentido a esto y para ayudar con la educación autoiniciada defendida, a continuación se describen dos definiciones simples pero importantes de los entornos transaccionales observados en la investigación de criptomonedas basadas en las cadenas de bloques. Los dos ambientes están etiquetados como el entorno interactivo y el medio ambiente contenido.

El entorno interactivo es uno en el que las actividades de criptomonedas se cruzan con el sistema bancario tradicional. La Figura 1 pone de relieve la interacción entre el sistema bancario tradicional y la criptomoneda de cadenas de bloques. En particular, es un ejemplo de cómo una cadena de bloque puede servir para ocultar el flujo de fondos relacionados con las transferencias ilícitas de riqueza.

Este escenario implica un narcotraficante que utiliza monederos Bitcoin, intercambios Bitcoin y transferencias de pago para estructurar las ganancias del delito. El traficante vende drogas y se le paga en bitcoin; los bitcoins son entonces estructurados por medio de dos monederos Bitcoin antes de que el valor se convierta a moneda fiduciaria en una bolsa de Bitcoin y luego se estructura aún más por medio de transferencias a través del sistema bancario tradicional.

Un investigador de ALD en el Banco 1 observaría la transferencia de la bolsa de Bitcoin, pero no necesariamente tendría en cuenta que el remitente era un intermediador de Bitcoin. Es por esta razón que los profesionales de ALD que trabajan en instituciones financieras deberían tomar conciencia de las distintas bolsas de criptomoneda, que son grandes, establecidos y mejor confiados.

En el Banco 2, los investigadores de ALD no verían el nexa con Bitcoin y verían simplemente una transferencia bancaria; el investigador sería incapaz de hacer el enlace que su cliente también es propietario del Monedero 'A.' Tales dificultades sugieren que los intercambios de criptomoneda también deberían tener regímenes eficientes de ALD de conozca a su cliente y diligencia debida mejorada (EDD).

Entorno contenido

En un entorno contenido todas las transacciones se realizan fuera del sistema bancario tradicional y sólo son visibles dentro de una cadena de bloque dada.

En la Figura 2, el traficante de armas/drogas puede recoger el dinero (transacción 1 y 2) y estructurar los ingresos de sus ventas de drogas (transacciones 3 y 4) en su totalidad en la cadena de bloque. En la transacción 5, el narcotraficante adquiere un bien de lujo por medio de un minorista en línea utilizando bitcoin. Es poco probable que un analista de ALD en una institución financiera estuviera de tanto de cualquiera de estas operaciones.

Si bien se podría sugerir que las cadenas de bloques son un presente griego para los agentes de control legal, ya que todo (transaccionalmente) se encuentra visible y disponible al público, tales declaraciones excesivamente simplificadas se enfrentan a muchas limitaciones causadas por la falta de conocimiento de las cadenas de bloques y las técnicas utilizadas para ocultar las fuentes de fondos.



Figura 2



Figura 3

Desafíos de ALD asociados con las criptomonedas

Al igual que las cuentas en el sistema bancario tradicional, los monederos de cadenas de bloques son susceptibles a las limitaciones de todo el mantenimiento de registros y la identificación de los titulares de cuentas y beneficiarios. En ambos casos, una persona puede, por ejemplo, utilizar identidades o sustitutos sintéticos para abrir cuentas. Una identidad sintética es una que no existe en la vida real. En otras palabras, la persona nunca nació y esto difiere de robar la identidad de una persona real (robo de identidad).

En virtud de su existencia en el entorno digital, las transacciones en las cadenas de bloques también se hacen más difíciles de seguir con anonimadores de direcciones de IP, así como mezcladores y/o tumbadores. Mientras anonimadores IP ayudan a ocultar la ubicación real de un dueño del monedero, los mezcladores (mixers, en inglés) y tumbadores (tumblers, en inglés) ayudan a ocultar el origen de los fondos.

La Figura 3 detalla un escenario real donde los investigadores en Rusia intentaron identificar operaciones sospechosas en la cadena de bloque de bitcoin. En este ejemplo, una transferencia de bitcoin se subdivide a través de 98 estructuras transaccionales y se paga a otros titulares del monedero bitcoin.

La caja rectangular superpuesta sobre el subconjunto medio de estas operaciones representa la inyección de mezcladores y tumbadores en la ecuación. Los mezcladores y tumbadores están libremente disponibles para los servicios ofrecidos por las empresas en línea. Algunas de estas compañías ofrecen abiertamente lavar bitcoins de suscriptores para tapar o, al menos, hacer que el camino transaccional y la secuencia de los acontecimientos sea más difícil de seguir. No es sorprendente que el uso de un mezclador/tumbador es de por sí una alerta roja de financiación del terrorismo/lavado de dinero.

Los mezcladores combinan bitcoins con los bitcoins de los demás. Los usuarios envían bitcoins a una dirección central. El mezclador envía una transacción de nuevo a cada usuario de la clave de control de la direc-

¹ Diana Mergenovna Sat, "Investigation of Money Laundering Methods through Cryptocurrency," Journal of Theoretical and Applied Information Technology, 20 de enero del 2016, <http://www.jatit.org/volumes/Vol83No2/11Vol83No2.pdf>

ción central. Cuando bitcoins robados (o bitcoins utilizados para lavar fondos) se mezclan con bitcoins “limpios”, se hacen difíciles de rastrear.

Los tumbadores intercambian bitcoins entre los usuarios. Un tumbador mezcla bitcoins y envía las transacciones con diversas cantidades a las claves que controla; en un intento de simular otras transacciones de red. Por ejemplo, un usuario que envía un bitcoin a un tumbador puede recibir transacciones múltiples, más pequeñas, a cambio durante un corto período de tiempo. Los bitcoins devueltos al usuario se habrán combinado, dividido y tramitado muchas veces.

Cuando identidades sintéticas se utilizan con los mezcladores y los tumbadores y el efectivo se ha convertido a bitcoins por medio de los cajeros automáticos de criptomoneda (que puede carecer de normas de debida diligencia del cliente/diligencia debida mejorada [DDC/EDD]), y las transacciones en línea se llevan a cabo desde el sigilo o direcciones anónimas y las partes operan en múltiples jurisdicciones, los desafíos que enfrentan las agencias de control legal y los profesionales de ALD no son difíciles de seguir, como se muestra en la Figura 4.

En la Figura 4, el Delincuente A convierte el efectivo en bitcoins utilizando un cajero automático de bitcoin y deposita los bitcoins en el Monedero A. Los fondos en el Monedero A son “mixtos” y se envían al Monedero B, propiedad del Delincuente B. Al recibir el pago en bitcoins, el Delincuente B le ofrece un arma al Delincuente A. Las redes de delincuentes organizados y terroristas pueden realizar ofertas nefastas fuera del sistema financiero regulado usando tales métodos.

Conclusión

La tecnología de cadenas de bloques está aquí para quedarse como el potencial que presenta—incluyendo registros de mantenimiento sin cuentas—ofrece demasiadas posibilidades de abandono. Sin embargo, en última instancia, aún no se ha visto cómo esta tecnología interactúa con las instituciones financieras tradicionales y la sociedad en su conjunto. Lo que es determinable en este momento es el efecto del primer caso de uso de la tecnología tangible de cadenas de bloques, las criptomonedas como bitcoin, tienen sobre los profesionales de ALD en todo el mundo.

Las criptomonedas abren una nueva dimensión en el control de las transacciones y procesos de ALD en su conjunto. Esta nueva dimensión se compone de entornos competitivos (interactivos y contenidos) y requiere diferentes enfoques para identificar con precisión las transacciones sospechosas cuando se le investiga a cada uno.

Como profesionales de ALD y de control legal, lo que está claro es la necesidad de conocimiento y educación en este espacio, no sólo para dar sentido a esta nueva tecnología, sino para competir en un mundo de ALD que puede ver un cambio drástico. La Conferencia de Cadenas de Bloques, la Criptomoneda y ALD en Toronto el 25 de agosto del 2016, es un buen ejemplo de la importancia de esta tecnología en el campo del ALD. Este es el futuro de ALD y es importante para el ALD y los profesionales de las agencias de control legal mantenerse al día. Entre los asistentes había de agencias de control legal, FINTRAC, autoridades gubernamentales, de los principales bancos, profesionales de cadenas de bloques y criptomonedas, los socios de la Alianza de Blockchain y de ACAMS.

Muchas instituciones financieras han creado centros de excelencia de cadenas de bloques que tienen como objetivo estudiar y probar posibles herramientas y productos basados en cadenas de bloques. Estas innovaciones deben venir de la mano con profunda investigación sobre las implicaciones relacionadas de ALD.



Figura 4

Joseph Mari, CAMS, CBP, gerente senior de investigaciones mayores, Bank of Montreal, Toronto, Canadá, joseph.mari@bmo.com

Peter Warrack, CAMS, CBP, CFE, director de inteligencia de riesgos, Bank of Montreal, Toronto, Ontario, Canadá, peter.warrack@bmo.com

Leonardo Real, CAMS, director de investigaciones de mercados de capitales de ALD, Bank of Montreal, Toronto, Ontario, Canadá, leonardo.real@bmo.com

Descargo de responsabilidad: Las opiniones expresadas en este artículo son las de los autores y no deben en modo alguno interpretarse como el reflejo de las opiniones, políticas, o los procedimientos del Bank of Montreal o de sus filiales.

La lucha contra el lavado
de dinero en el

SECTOR INMOBILIARIO

Para tener éxito en la lucha de antilavado de dinero de los EE.UU. por medio del sector inmobiliario, dos puntos débiles en nuestro régimen actual de antilavado de dinero/la lucha contra el financiamiento del terrorismo (ALD/CFT) deben eliminarse: 1) la falta de transparencia en las aprobaciones corporativas de los estados y 2) la exención de los agentes de bienes raíces de cumplir con los requisitos de la Ley del Patriota.

Los delincuentes que utilizan las propiedades inmobiliarias para el lavado de dinero no se limitan a los políticos corruptos, el delito organizado, los traficantes de drogas y de seres humanos o los patrocinadores del terrorismo. Un caso pone de relieve los graves daños que este tipo de lavado de dinero puede causar. En la ciudad de Nueva York, el gobierno iraní, por medio de una empresa fantasma, usó una serie de empresas para comprar y administrar un rascacielos de la Quinta Avenida valuado en \$750 millones. Los fondos de alquiler derivados de esta inversión ayudaron al terrorismo respaldado por Irán durante decenios, hasta que fue descubierto por las autoridades policiales de Nueva York.¹

El lavado de dinero por medio del sector inmobiliario es un método popular para los delincuentes, ya que es una inversión de prestigio, y puede llevarse a cabo en una sola transacción, se puede convertir fácilmente en dinero en efectivo, puede apreciarse en valor y puede generar ingresos por alquiler. Pero quizás el factor más importante es que el sector inmobiliario en los EE.UU. y en muchos otros países tiene menos supervisión regulatoria. De acuerdo con *The Economist*, las sociedades fantasmas imposibles de rastrear son vehículos populares para transferir y ocultar la riqueza—robada por funcionarios del gobierno—así como otros fondos ilícitos obtenidos por narcotraficantes, traficantes de armas y financieros del terrorismo.² Reconociendo esto, la UE incluyó un requisito de divulgación de propiedad efectiva en su Cuarta Directiva de ALD. Programada para entrar en vigor en 2017, no sólo permite el acceso a esta información por parte de las agencias de control legal sino también de los medios de comunicación. Teniendo esto en cuenta, los EE.UU. podrían resultar un país aún más atractivo en el que se pueden usar empresas para ocultar las ganancias del delito.

El fortalecimiento del proceso de registro de sociedades del estado

En los EE.UU. tenemos que exigirles a los estados obtener información sobre la verdadera propiedad de las empresas. En los EE.UU. más de 2 millones de corporaciones son aprobadas por los estados cada año. Las

empresas que desean formar corporaciones deben presentarse a los estados individuales y, si bien los requisitos difieren, no hay barreras significativas para las personas que desean formar sociedades con la finalidad específica de lavado de dinero. La información requerida es insuficiente, lo que permite el anonimato, y no hay manera de mantener la información y actualizar la lista de los nombres de los propietarios efectivos de corporaciones o sociedades de responsabilidad limitada. Algunos estados requieren listas de los accionistas, pero pueden ser nombres que sirven de fachada. Por lo general, los solicitantes deben proporcionar menos información que la requerida para obtener una licencia de conducir o para abrir una cuenta bancaria.

La legislación del Congreso introducida originalmente por el Senador Carl Levin, el 2 de agosto del 2011, y actualmente patrocinada en el Senado por el Senador Sheldon Whitehouse (D-RI) y en la Cámara de Representantes por Carolyn Maloney (D-NY) y Peter King (R-NY), requeriría verdadera información sobre el beneficiario y permitiría que las agencias de control legal federales, estatales y locales accedan a esta información. La Ley de Incorporación de la Transparencia y Cumplimiento de la Ley de Asistencia modifica la Ley de Seguridad Nacional de 2002 para exigir que los estados que reciben fondos bajo esta Ley cumplan con estos requisitos. El proyecto de ley “ordena al Departamento del Tesoro emitir regulaciones que requieren que las empresas y sociedades de capital constituidas en un estado que aún no requieren la divulgación de base le presenten información sobre su propiedad beneficiosa al Tesoro como copia de seguridad”.³ Proporciona requisitos mínimos de información que incluyen:

- “La identificación de los beneficiarios por su nombre, dirección actual y pasaporte vigente o licencia de conducir emitida por el estado;
- La identificación de cualquier entidad jurídica afiliada que ejercerá el control sobre la entidad incorporada; y
- La actualización coherente de las listas de los beneficiarios efectivos no más tarde que 60 días después de cualquier cambio en la propiedad”.⁴

Las sanciones civiles se imponen para los que:

- “Entregan información falsa o fraudulenta sobre el beneficiario;
- No proporcionan información completa o actualizada; o
- Divulgan, a sabiendas, citaciones u otras solicitudes de información sobre el beneficiario sin autorización”.⁵

El proyecto de ley requiere que los estados proporcionen información presentada cuando la soliciten las agencias de control legal y “ordena al Secretario del Tesoro promulgar una norma que obliga a las personas que participan en el negocio de formar sociedades establecer programas [de ALD]”.⁶

Además, “requiere que el contralor general informe sobre: 1) el grado en que los estados les permiten a las personas formar asociaciones, fideicomisos, organizaciones benéficas u otras entidades legales según las leyes estatales y requieren que dichas personas proporcionen información sobre los beneficiarios y 2) la efectividad de las prácticas de incorporación aplicadas en el marco de la ley al ayudar a las agencias de control legal”.⁷ Este proyecto de ley dará a conocer los verdaderos propietarios efectivos de las corporaciones y impedirá que los malhechores exploten vehículos corporativos para su beneficio y ayudará a las agencias de control legal en la detección y llevar ante la justicia al lavador de dinero.

Levantar la exención de agentes inmobiliarios

Desde 2002, el Departamento del Tesoro de los EE.UU. ha eximido a los agentes de bienes raíces de llevar a cabo la diligencia debida y reportar transacciones sospechosas. De acuerdo con Elise Bean, ex miembro del personal del Senador Carl Levin (D-Mich.) y experta en ALD, levantar esta exención haría conformar a los EE.UU. con la Recomendación 22 del GAFI, que establece que negocios no financieros y profesionales designados, tales como los agentes inmobiliarios, deberían tener los requisitos de la debida diligencia del cliente (DDC) establecidos en las Recomendaciones del GAFI 10, 11, 12 y 15. Los oponentes de hacer cumplir a los agentes

¹ “How Iran Built a Skyscraper in the Middle of New York City and Held onto it for Decades,” *Quartz Daily Brief*, 17 de septiembre del 2013, <http://qz.com/125430/how-iran-built-a-skyscraper-in-the-middle-of-new-york-city-and-held-onto-it-for-decades/>

² “The Secretive and Morally Dubious World of Shell Companies,” *The Economist*, 7 de abril del 2016, <http://www.economist.com/blogs/graphicdetail/2016/04/using-and-abusing-offshore-accounts>

³ “Reps. Maloney, King and Senator Whitehouse Introduce Bills to Stop Anonymous Money Laundering Operations by Requiring Disclosure of Shell Corporation Beneficial Owners,” 3 de febrero del 2016, <https://maloney.house.gov/media-center/press-releases/reps-maloney-king-and-senator-whitehouse-introduce-bills-to-stop>

⁴ *Ibid.*

⁵ *Ibid.*

⁶ “S.1465—Incorporation Transparency and Law Enforcement Assistance Act,” 1 de agosto del 2013, <https://www.congress.gov/bill/113th-congress/senate-bill/1465>

⁷ *Ibid.*

inmobiliarios dicen que la regulación no es necesaria debido a que otras entidades informantes están proporcionando cobertura.

En una carta de 2011 a la Red Contra los Delitos Financieros (FinCEN), la Asociación Nacional de Agentes Inmobiliarios defendió la exención declarando que:

“Observamos que en casi todas las operaciones de compra de bienes raíces en la que participan agentes inmobiliarios, los fondos son transferidos utilizando administradores de varias entidades reguladas diferentes, desde el pago del depósito de garantía cuando el contrato de venta se ejecuta hasta el cierre o liquidación”.⁸

Otros estudios han encontrado que el 22 por ciento de las compras de bienes raíces no implican una hipoteca. Esto deja un gran número de transacciones cada año que podrían ser casos de lavado de dinero. Sin incluir las transacciones comerciales de bienes raíces, las ventas totales de casas por sí solas ascendieron a 5,259,000 en 2015. Uno puede ver que un gran número de transacciones de bienes raíces no están cubiertas por la Ley del Patriota.

Papel de un agente de bienes raíces

Si los agentes inmobiliarios ya no están exentos, esto capturará para escrutinio el 22 por ciento de las transacciones de bienes raíces y proporcionará un segundo par de ojos para todas las transacciones. En la mayoría de las transacciones de bienes raíces, es el agente el que sabe más que cualquiera de las otras partes (por ejemplo, abogados, bancos o compañías de título) que participan en la transacción y se encuentra en una mejor posición para identificar una transacción sospechosa. Pero, lo más importante, el agente sabe a qué se parecen las transacciones normales y anormales que podrían ser indicativas de lavado de dinero. En concreto, son conocedores de cómo se llevan a cabo las transacciones de bienes raíces y pueden reconocer las diferencias que pueden indicar riesgos de ALD. Sin embargo, confiar únicamente en la experiencia de los agentes no es suficiente. Los agentes deben estar capacitados para reconocer el gran número de esquemas que utilizan los bienes raíces y saber cuándo y cómo presentar los reportes de operaciones sospechosas (ROS) y/o aplicación de la ley de contacto.

Hacer que los agentes inmobiliarios entren al cumplimiento puede ser visto al principio como una tarea enorme. Después de todo, la Asociación Nacional de Agentes Inmobiliarios es una de las asociaciones comerciales más grandes de los EE.UU., y sus agentes son más de 1.200.000. Pero con las recientes tendencias en el entrenamiento y el enfoque basado en el riesgo, la tarea no puede ser tan desalentadora. En primer lugar, materiales de entrenamiento adaptados específicamente a los agentes de bienes raíces ya están disponibles. Además, la capacitación basada en la web puede desarrollarse para proporcionar una forma económica de llegar a la gran audiencia. Otra medida eficiente sería la adopción de un enfoque basado en el riesgo utilizado actualmente por los bancos y otras entidades informantes. Los agentes sólo se centrarían en aquellos clientes de riesgo, las transacciones y los métodos de financiación. Por ejemplo, el riesgo de un cliente puede ser determinado por el fondo del cliente, el comportamiento y la motivación. Las señales de advertencia incluyen transacciones que no son transacciones cara a cara o ubicación de la propiedad frente a la ubicación en relación a la residencia del comprador. Las banderas de alerta financieras para buscar son el origen de fondos extraños, el uso de préstamos complejos u otros medios oscuros de financiación en relación a los préstamos de las instituciones financieras regulares.

La clave de esto consiste en alertar a los agentes inmobiliarios sobre las señales de alerta asociadas al lavado de dinero en el sector inmobiliario. Esto incluye el uso de pago en efectivo, las compañías fantasmas y nominadas, la financiación de un banco offshore, la sustitución del comprador y las transacciones realizadas en la compra a un valor significativamente diferente (mucho mayor o mucho menor) a partir del valor real de mercado de la propiedad.

En el estudio de posibles operaciones inmobiliarias sospechosas, ¿qué clase de proceso deben llevar a cabo los agentes de bienes raíces? En primer lugar, un agente debe conocer el interés del cliente y el uso previsto de la propiedad y conocer la verdadera identidad del cliente. Cuando una o más señales de alarma están presentes, el agente debería llevar a cabo CDD por medio de:

- La obtención de licencia de conducir, pasaporte u otros documentos de identificación fiables del solicitante para confirmar la verdadera identidad;
- Para las personas jurídicas, como una corporación o LLC, tomar medidas adicionales para verificar quién controla o es propietario de la empresa y otra información sobre el beneficiario; y
- Otra “información apropiada sobre la base de la experiencia y el conocimiento del agente de entender las circunstancias del cliente y del negocio”.⁹ Cuando un agente sospecha que las transacciones podrían ser lavado de dinero, él o ella debe ponerse en contacto con los agentes de control legal local o el FBI y/o presentar un reporte de operaciones sospechosas (ROS) en la FinCEN.

Resumen

Los políticos corruptos, narcotraficantes, traficantes de seres humanos, traficantes de armas y financieros del terrorismo reconocen las ventajas del lavado de dinero por medio de las propiedades inmobiliarias. La más importante de las numerosas ventajas es la falta de supervisión regulatoria adecuada en los EE.UU. y otros países. La falta de transparencia en las aprobaciones corporativas estatales les permite a las empresas fantasmas ser utilizadas para el lavado de dinero por medio de las propiedades inmobiliarias. El congreso de los EE.UU. debe aprobar leyes que requieren que los estados obtengan el nombre del verdadero titular y permitan el acceso a las agencias de control legal a esta información. Los agentes de bienes raíces están mejor posicionados para tanto prevenir como detectar el lavado de dinero en el sector inmobiliario. Ya no deben estar exentos de los requisitos de la Ley del Patriota y deben unirse a otras entidades informantes y profesionales en la realización de medidas de diligencia debida y la presentación de los ROS. **FA**

James M. Wright, consultor, James Wright Bank Advisor, Arlington, Virginia, EE.UU., jurightbankadvisor@verizon.net

⁸ Thomas Weldy, “Let’s Close the American Real Estate Money Laundering Gap,” The FCPA Blog, 6 de octubre del 2015, <http://www.fcpablog.com/blog/2015/10/6/lets-close-the-american-real-estate-money-laundering-gap.html>

⁹ “Anti-Money Laundering Guidelines for Real Estate Professional,” 2012, <http://www.realtor.org/sites/default/files/presentations/2012/2012-legal-seminar-anti-money-laundering-guidelines-2012-10-16.pdf>

Why spend 3 days with some of the brightest minds in AML audit or financial crimes investigations?

To earn the recognition you deserve for committing to protecting and elevating the status of your institution.

New Live Programs Announced:

Leesburg, VA

October 10-12, 2016

advanced-certification@acams.org

Bahrain

November 1-3, 2016

jlewis@acams.org

Hong Kong

October 20-22, 2016

asia@acams.org

Amman, Jordan

November 7-9, 2016

jlewis@acams.org

AML and Financial Crimes Professionals with ACAMS Advanced Certifications* are recognized as elite seasoned professionals with superior skills committed to and focused on growing professionally to benefit their institutions.

**You must be CAMS Certified in order to apply.*



5%

¿CUÁNTO PUEDES BAJAR?

50%

Las acciones de ejecución adoptadas este año por la Oficina de Control de Activos Extranjeros (OFAC) contra dos subsidiarias de Halliburton Energy Services, Inc., (Halliburton Limited Atlantic y Halliburton Overseas Limited) y Barclays Bank Plc, parecen estar en conflicto entre sí en el nivel de la diligencia debida que una empresa necesita llevar a cabo con el fin de determinar la propiedad beneficiosa de las organizaciones. Mediante el examen de estos dos casos en mayor detalle, una distinción importante se revela en lo que respecta a la información necesaria para cumplir con los requisitos de sanciones.

La acción legal de Barclays

A principios de febrero, Barclays Bank Plc, un banco con sede en Londres, llegó a un acuerdo con la OFAC por \$2.485.890 por 159 presuntas violaciones de las Sanciones de Reglamentos de Zimbabue.¹ Cada una de esas violaciones, cometidas entre 2008 y 2011, representaba una transferencia de fondos pagados a través de las entidades financieras con sede en los EE.UU., incluyendo la filial de NY de Barclays, en nombre de los clientes de su negocio de Zimbabue (Barclays Bank of Zimbabwe Limited [BBZ]) que estaban sujetos a sanciones de conformidad con la Regla del 50 por ciento de la OFAC. La pena resultante de estos \$3.375.617 de transferencias de fondos fue un poco menos de la mitad de la pena de la base de \$5.029.000.

Las autoridades de Zimbabue le prohibieron al BBZ la realización de sanciones de cumplimiento, entonces el personal de operaciones del Reino Unido llevó a cabo esas operaciones basándose en la documentación de cliente del BBZ. Sin embargo, los sistemas del BBZ fueron incapaces de capturar y monitorear adecuadamente la información relacionada con las partes, incluyendo la de los beneficiarios efectivos, incluso si dicha información estuvo documentada en otros lugares (por ejemplo, en los registros físicos). Además, los procedimientos del BBZ de conozca a su cliente presentaron desafíos que causaron error en identificar correctamente a los propietarios reales de algunos de sus clientes corporativos. La combinación de estos temas resultó en que la operación de U.K. Barclays no estuviera al tanto de y fuera incapaz de detectar esta información para ciertos clientes. Tres de ellos eran empresas que eran propiedad (50 por ciento o más) de la Industrial Development Corporation of Zimbabwe (IDCZ), que había sido designada por la OFAC en julio de 2008. Ninguna de estas relaciones de propiedad fue identificada por cualquiera de las unidades de Zimbabue o del Reino Unido de Barclays, que continuó procesando sus transacciones en dólares estadounidenses. Incluso después de que el BBZ descubrió la propiedad efectiva de estas firmas y actualizó sus registros en papel, esta información no

pasó al sistema de atención al cliente de la empresa del Reino Unido para el monitoreo de sanciones. Además, incluso después de que cuatro transferencias de fondos fueron bloqueadas por las empresas estadounidenses financieras que se inician a finales de 2012 y la investigación de Barclays NY confirmó la propiedad de IDCZ en el cliente relacionado del BBZ, la empresa no actualizó sus registros para que el filtro de detección de sanciones pudiera atrapar futuras violaciones potenciales y otras tres transacciones fueron procesadas para la cuenta (y posteriormente bloqueadas por empresas estadounidenses).

A pesar de los fracasos de Barclays para implementar controles adecuados y su sofisticación comercial, la OFAC señaló que la empresa no había recibido una penalización en el pasado reciente, y que cooperó con la OFAC y remedió su programa de cumplimiento de sanciones.

La acción legal de Halliburton

Dos filiales de Halliburton Energy Services de las Islas Caimán (Halliburton Atlantic Limited y Halliburton Overseas Limited) le pagaron a OFAC un arreglo de \$304.706 por presuntas violaciones del Reglamento de Control de Activos Cubanos.² Entre febrero y abril de 2011, las dos firmas exportaron bienes y servicios de apoyo a la exploración de energía y la perforación realizada en Angola. Las actividades se estaban llevando a cabo por un consorcio de producción de energía basada en Angola en el que Cuba Petróleo (también conocida como Cupet), una firma estatal cubana, tenía una participación del 5 por ciento. El valor de los bienes y servicios entregados fue de \$1.189.752. Sin embargo, es importante tener en cuenta que los productos y servicios proporcionados fueron los que permitieron las actividades de producción de energía del consorcio, lo que probablemente produjo un beneficio económico significativamente mayor a Cupet y, por lo tanto, al gobierno cubano.

La OFAC redujo la multa de la pena de base de \$423.202 tras examinar el fracaso de Halliburton para llevar a cabo la diligencia debida en base a la composición de su cliente (el con-

sorcio); su fracaso de no tomara en cuenta la participación de Cupet se observó en los documentos del consorcio, los artículos de prensa y un registro oficial de Angola; y su sofisticación comercial general. La mitigación fue concedida por la OFAC en este caso debido a que Halliburton no había sido objeto de una acción de reciente aplicación y, por tanto, tenía derecho a un descuento por “primeras violaciones” de hasta el 25 por ciento, y debido a que la participación limitada de Cupet restringía su beneficio económico.

¿El 50 o 5 por ciento?

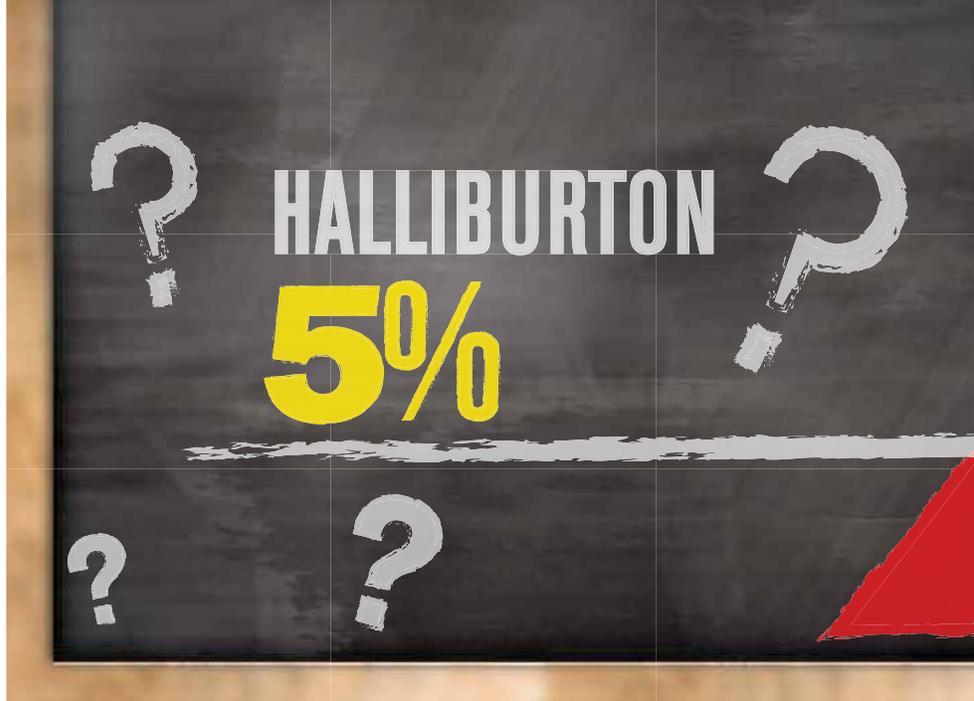
Así que, ¿por qué parece que hay diferentes estándares para estas dos empresas? La regla del 50 por ciento de la OFAC está muy claramente establecida en un documento de orientación de la OFAC: Una entidad que es propiedad, en un 50 por ciento o más, de una o más entidades sancionadas (en la Lista de Nacionales Especialmente Designados, la Lista de la Orden Ejecutiva 13599, o bajo la misma Directiva en la Lista de identificación de sanciones sectoriales) está sujeta a las mismas sanciones que las entidades propietarias. Por otra parte, la “regla” del 5 por ciento que se utilizó en el caso Halliburton no parece estar consagrada en ninguna parte, al menos con una figura de propiedad específica adjunta.

En realidad, hay dos estándares diferentes en el trabajo aquí porque los casos no son análogos. El diferenciador es la naturaleza de la relación entre la empresa y la parte sancionada.

En el caso de Barclays, la filial de NY de Barclays es la parte correspondiente a considerar. Si las transferencias de fondos hubieran pasado por otro banco con sede en los EE.UU., Barclays no habría incurrido en una penalidad civil monetaria debido a que la OFAC no habría tenido jurisdicción legal. Barclays NY estaba actuando como intermediario sin relación directa con la cuenta del originador de la transacción. Por lo tanto, la carga de su conocimiento de las partes mencionadas en los pagos se limitaba a la de la Regla del 50 por ciento. Si las partes de la

¹ “Zimbabwe Sanctions Regulations,” U.S. Government Publishing Office, 14 de julio del 2016, http://www.ecfr.gov/cgi-bin/text-idx?SID=5eae22affe2e3675b6deaa3fb796eb7a&tpl=/ecfrbrowse/Title31/31cfr541_main_02.tpl

² “Cuban Assets Control Regulations,” U.S. Government Publishing Office, 14 de julio del 2016, http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title31/31cfr515_main_02.tpl



lista de SDN poseyeran una participación minoritaria en los clientes de BBZ, no habría habido ninguna acción legal.

Por otro lado, Halliburton trató directamente con el consorcio que tenía la participación de Cupet. Por lo tanto, la responsabilidad de la empresa era una carga de estilo KYC de conocer la propiedad efectiva de ese socio de negocios lo suficientemente bien como para saber, con un grado razonable de certeza, que ninguna parte o país sancionado derivó un beneficio económico no despreciable de la relación. En general, las regulaciones de las sanciones de la OFAC bloquean “bienes o intereses en la propiedad” de parte de los destinatarios. La participación en la propiedad de Cupet representaba claramente un interés en la propiedad que proporcionaba un beneficio económico a Cuba.

¿El 50 o 5 por ciento—o menos?

¿Cómo se sabe cuando se cumple la carga de hacer la investigación de la propiedad? Las dos tareas de cumplimiento de la Regla del 50 por ciento y la identificación de intereses en la propiedad son en realidad un poco diferente.

En el caso de la Regla del 50 por ciento, uno tiene que determinar que la propiedad agregada alcanza el umbral del 50 por ciento. La orientación de la OFAC afirma que se debe actuar con precaución cuando se trata de una entidad en que las partes sancionadas tienen una “participación significativa que es menor al 50 [por ciento], o que una o más personas bloqueadas pueden controlar por medios distintos una participación mayoritaria”,³ porque dichas entidades pueden designarse a sí mismas, o ser objeto de la acción de cumplimiento en el futuro.

En el caso de Halliburton uno sólo necesita determinar la estructura de la propiedad de una de las partes interesadas, tales como un socio de empresa conjunta (proveedor o cliente) y si podría generar un interés de propiedad a una persona, entidad o país sancionado (incluyendo aquellos cubiertos por el 50 por ciento de la regla de orientación).

Hay consideraciones prácticas, basadas en el riesgo en cada caso investigado. ¿Tienen sentido?

La capacidad de entender la propiedad de una empresa a los efectos del cálculo de la regla del 50 por ciento está en gran medida determinada por la naturaleza de su organización, la disponibilidad de los registros públicos, el acceso a la información pública y el país donde se organiza una empresa. Mientras que una empresa pública tenderá a tener algún tipo de registros de propiedad disponibles para el público, las empresas privadas tenderán a no tenerlos. A menos que uno tenga una relación comercial directa con la empresa privada, la capacidad de determinar posibilidades de propiedad se verá obstaculizada significativamente. Dependiendo del país donde se encuentra la empresa, puede haber límites y excepciones a los requisitos de los registros de propiedad transparentes. Por ejemplo, es posible enumerar un propietario individual de las empresas en Rusia de forma anónima. Diferentes países tienen diferentes normas mínimas para la participación del accionista. Una

rápida encuesta, no científica, de los principales países de bolsa muestra que los valores mínimos varían de 3 a 10 por ciento.

Por lo tanto, ¿necesitaría uno entonces investigar cada propietario registrado públicamente que tenga el 3 por ciento o más de las acciones de una empresa? Como puede imaginarse, es probable que haya un número significativamente mayor de propietarios de empresas con el 3 por ciento en un país determinado que propietarios de 5 o 10 por ciento, lo que puede elevar considerablemente el costo del cumplimiento de sanciones.

Sin embargo, es discutible si el gran aumento de los datos tendría un impacto notable en la información relevante obtenida de él. Es probable que tendría sentido aprovechar la orientación de la OFAC sobre el uso de la precaución cuando se trata de participaciones significativas de propiedad de menos del 50 por ciento en el tratamiento de posibilidades de propiedad que se acercan a este umbral como si se hubiera alcanzado ese nivel. Por ejemplo, si una empresa trata a todas las empresas que alcanzaron un total del 40 por ciento de propiedad como si se hubiera cumplido el umbral del 50 por ciento, el riesgo de no investigar participaciones inferiores al 10 por ciento se reduciría significativamente. Como cuestión estadística, la probabilidad de que una firma es de un propietario del 32 por ciento y dos propietarios de 9 por ciento es significativamente menor que la del propietario de una mayoría simple o dos propietarios del 10 por ciento o más que sumen hasta un

³ “Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked,” Department of the Treasury, 13 de agosto del 2014, https://www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf



50 por ciento. En función de la propensión al riesgo de una empresa, considerarían el costo de esa investigación adicional como fuera de línea con el riesgo residual reducido.

¿Se atrapó su interés?

Al determinar posibilidades de propiedad para descubrir “intereses en la propiedad”, se aplica un cálculo diferente. Suponiendo que uno puede determinar toda la estructura de la propiedad, la regla debe ser explícita. Por ejemplo, si uno sabe de una participación prohibida, debe alejarse, independientemente de su tamaño (a menos que se pueda obtener una licencia de la OFAC).

¿Y si no es posible determinar todos los propietarios? Si una empresa se lleva estrechamente, no sería irrazonable tratar la falta de integridad como una señal de alerta y rechazar la oportunidad de negocio. En cualquier caso, uno podría también—sobre una base basada en el riesgo—considerar el tamaño relativo de los posibles beneficios económicos que podrían extenderse a los propietarios desconocidos. Después de todo, uno de los factores generales de la OFAC delineados en sus Directrices de Aplicación es la Vulneración de los Objetivos del Programa Sanciones, que incluye:

“El Beneficio Económico u Otros para el Individuo, Entidad, o País Sancionado: El beneficio económico u otro conferido o tratado de conferir a personas, entidades o países sancionados como consecuencia de una

violación aparente, incluyendo el número, tamaño, y el impacto de las transacciones que constituyen una violación aparente(s), la longitud de tiempo durante el que se produjeron, y la naturaleza del beneficio económico u otro conferido”⁴.

Cuando se tiene en cuenta la participación en la propiedad que no se contabiliza (por ejemplo, las limitaciones de reglas de divulgación de propiedad relevantes y la magnitud total de la relación comercial), una empresa puede decidir si el beneficio potencial concedido a un propietario desconocido sancionado podría ser menospreciado en una investigación de la OFAC. También hay que tener en cuenta si la participación en la propiedad en cuestión es incognoscible (por ejemplo, la propiedad de acciones por debajo de los umbrales de registro), o simplemente desconocida (por ejemplo, debido a la falta de cooperación por parte de la organización en la producción de una divulgación completa) cuando se hace la decisión.

Los límites exteriores

La OFAC proporciona una Regla de 50 por ciento orientativa, pero no proporciona incluso un ápice de los datos pertinentes para el cumplimiento. Lo mismo, quizá más razonablemente, ya que es realmente sólo relevante para relaciones directas, se aplica al determinar “los intereses de la propiedad”. Esto presenta una gran carga de la investigación en curso de la Regla del 50 por ciento para las empresas, así como de vez en

cuando haciendo participar una inmersión profunda en las estructuras de propiedad de los interesados.

Afortunadamente, hay proveedores comerciales. Una empresa ha identificado más de 8.800 entidades cuyos sujetos sancionados tienen un 10 por ciento o más de participación en la propiedad, cargos en el consejo de administración o control de voto sin propiedad (también mencionado en la guía de la OFAC sobre exhibir precaución fuera de los casos de propiedad del 50 por ciento) objetivos de sanciones tanto para la OFAC como para la UE. Además, en el lado más general de la propiedad efectiva de investigación, otro proveedor tiene información de más de 200 millones de entidades. Si bien ninguno puede ser comprensivo, pueden ser buenos puntos de partida tanto para el control de riesgos y de los costos de investigación, sobre todo si tenemos en cuenta los conocimientos lingüísticos necesarios para llevar a cabo este tipo de investigación en todo el mundo.

Limbo legal

Ni las acciones de aplicación de Halliburton ni las de Barclays fueron concebidas como ejercicios de “nombrar y avergonzar”, como debería quedar claro a partir de los tamaños nominales de los arreglos hechos. La razón por la que se impusieron multas, y se publicaron las acciones fue por reforzar el nivel de cuidado que los reguladores esperan actualmente. Al igual que el juego de limbo, con el tiempo, la cantidad de margen de maniobra que hay frente al reto que nos ocupa es cada vez menos. Por lo tanto, ¿cuánto está usted dispuesto a bajar en la búsqueda de posibilidades de propiedad que entran en conflicto con las regulaciones y orientaciones de sanciones? **A**

Eric A. Sohn, CAMS, director de productos de negocio, Dow Jones Risk & Compliance, Nueva York, NY, EE.UU., eric.sohn@dowjones.com

⁴ “Economic Sanctions Enforcement Guidelines,” Department of Treasury, 9 de noviembre del 2009, https://www.treasury.gov/resource-center/sanctions/Documents/fr74_57593.pdf

Rick McDonnell: Temas de ALD y GAFI

A *CAMS Today* tuvo el privilegio de entrevistar a Rick McDonnell sobre sus logros, las evaluaciones mutuas del Grupo de Acción Financiera Internacional (GAFI) y los desafíos de antilavado de dinero (ALD).

McDonnell es al presente el director ejecutivo de ACAMS y miembro del Consejo Asesor de ACAMS. McDonnell tiene muchos años de experiencia directa de trabajo con los órganos regionales, lo que le da una perspectiva global única sobre los retos de ALD y la delincuencia financiera.

McDonnell fue secretario ejecutivo del GAFI desde 2007. Bajo su dirección, el GAFI desarrolló una nueva metodología de evaluación estandarizada para el país y la Red Global de GAFI se amplió a nueve órganos del GAFI de estilo regional. Antes de esta función, trabajó para la Oficina de las Naciones Unidas contra la Droga y el Delito, donde fue jefe del Programa Mundial de la ONU sobre lavado de dinero. Anteriormente, McDonnell estableció el Grupo de Asia-Pacífico sobre lavado de dinero y se convirtió en su primer secretario ejecutivo.

Además, es abogado de profesión y ha tenido amplia experiencia como fiscal federal y en la realización de investigaciones complejas, además de ser responsable de muchos grupos de trabajo de investigación multidisciplinarios en casos de delincuencia organizada tanto a nivel nacional como internacional. También ha tenido experiencia en la práctica jurídica privada y como profesor universitario.

ACAMS Today: Desde la perspectiva de ALD, ¿cuáles crees que fueron los mayores desafíos de este año?

Rick McDonnell: Desde la perspectiva de ALD se ha hecho hincapié en el GAFI para tratar de asegurar que el intercambio de

información está a la altura. Lo que quiero decir es que su expectativa es que la información—de acuerdo con las normas acordadas a nivel internacional—debería ponerse a disposición de forma rápida y automática en muchos casos. Esto ha sido un gran reto, porque no son sólo las normas internacionales que se han acordado, son diferentes normas para la realización y procesamiento de información. Por lo tanto, todavía hay un largo camino por recorrer en términos de flujo de información eficiente y eso es exactamente lo que los tiempos requieren.

AT: ¿Cuál es el mayor error de la comunidad ALD con respecto del GAFI?

RM: Usted puede pensar que esto es un poco extraño, pero creo que el mayor error es que mucha gente fuera de los técnicos parece pensar que el GAFI es un cuerpo monolítico—una sola gran extensión internacional gigantesca que tiene todas las reglas, hace todas las normas y da todas las instrucciones cuando en realidad ese no es el caso en absoluto. Es una organización donde las decisiones se toman de conformidad y en los acuerdos entre países soberanos, y son los países los que realmente poseen, gestionan y son responsables del GAFI. La razón por la que estoy explicando esto es porque a veces se produce una situación extraña en la que se examina a los países en los estándares del GAFI y sobre cómo se están aplicando y cuáles son los niveles de cumplimiento, y se oye a menudo a estos países decir: “Mira lo que el GAFI me está haciendo. Están siendo demasiado duros, o están siendo demasiado esto o demasiado lo otro”. Suena un poco gracioso, pero es una indicación interesante que mientras que el nivel de propiedad se basa en los miembros, cuando se trata de observar las normas y ser examinado según ellas a todos les gusta culpar a un interlocutor externo

cuando en realidad les corresponde a los propios países individuales aplicar las normas, de acuerdo con lo que se espera de ellos y lo que han acordado hacer.

AT: ¿Podría describir la diferencia entre el proceso de evaluación mutua en el pasado y donde estamos ahora?

RM: Hay una gran diferencia entre lo que solían ser los requisitos de evaluación y lo que son ahora. En el pasado—es decir la tercera ronda de evaluaciones y las anteriores—la concentración fue de 95 por ciento en el cumplimiento técnico. La conformidad técnica significa si hay un delito de lavado de dinero, si hay una unidad de inteligencia financiera en su lugar y si existen investigaciones que se realizan. Estas son las preguntas y objetivos concretos basados en herramientas que necesitan ponerse en marcha en oposición a cómo se están utilizando en realidad esas herramientas y si se están utilizando con buenos resultados y qué efecto tiene ese uso sobre el problema general que se estableció que el GAFI controlara, que es el lavado de dinero, la financiación del terrorismo y la financiación de la proliferación.

Por lo tanto, la gran diferencia es que desde que la cuarta ronda de evaluaciones se inició el año pasado, el proceso de evaluación, las visitas in situ a cargo de expertos y el informe escrito final, se está concentrando ahora en el aspecto de la eficacia. Sin embargo, eso no quiere decir que la parte de conformidad técnica está siendo ignorada. No es una comprobación de si las leyes están en su lugar y si ningún país las ha rescindido o modificado. Sin embargo, ese aspecto se lleva a cabo por la Secretaría del GAFI, y se cubre en un anexo en el reporte de evaluación mutua. El cuerpo real del reporte realizado por el equipo de expertos evaluadores está ahora totalmente concentrado en la efectivi-



dad. En otras palabras, se están realizando investigaciones como deberían ser, cuál ha sido el resultado, cuál ha sido el porcentaje de condenas, cuáles son las tasas de confiscación o retención de activos, y qué tan bien están funcionando las agencias juntas y si no es así, ¿por qué no? Esos son los elementos principales en la determinación de si el sistema en su conjunto es eficaz en comparación con los componentes individuales del sistema, ya que la eficacia de la metodología se centra en que todo el sistema opere tan perfectamente como sea posible.

Por lo tanto, usted tiene que tener las medidas preventivas, los requisitos reglamentarios, las agencias de control legal y las instituciones financieras trabajando mano a

mano con el aparato de gobierno y mostrar, por ejemplo, cómo las investigaciones internacionales han superado los problemas tales como el intercambio de información. Por ejemplo, ¿cómo se comparte la información a nivel nacional como a nivel internacional entre las agencias?, ¿Hay silos aún entre los organismos (en caso afirmativo, por qué y qué se está haciendo al respecto?). Si no, ¿es eficaz y valiosa y cuál es la calidad de la información? Por ejemplo, en relación con casos de lavado de dinero, si usted se encuentra en el sistema federal, ¿están las autoridades federales y en algunos casos las autoridades estatales trabajando juntas para asegurar que toda la información está disponible?

El énfasis básico está ahora en las 11 variables de eficacia que figuran en la metodología de evaluación del GAFI, que son muy fáciles de leer, y usted verá cuál es el fundamento de los requerimientos de eficacia. Así que, a partir de una política y un punto de vista práctico, el objetivo del proceso de evaluación ahora es mostrar si el sistema está funcionando bien, si el gobierno y el sector privado están recibiendo valor de la inversión que están haciendo y si no, ¿por qué no? El informe señala estas cosas y hay un riguroso mecanismo de seguimiento.

La esencia del aspecto de eficacia de los informes está en que si los países han identificado los riesgos reales y las vulnerabilidades que enfrentan y si es así, ¿qué están haciendo acerca de aquellos y con qué eficacia se encarga de esas cosas? Se trata de un mecanismo dependiente de lo que son las amenazas y las vulnerabilidades.

AT: ¿Se puede hacer más en el sector privado o en el sector público para trabajar en estrecha colaboración con la misión del GAFI?

RM: No se hizo suficiente en el pasado. Se está mejorando ahora, pero creo que todavía no se hace suficiente. No lo digo injustamente y creo que los propios miembros del GAFI están reconociendo que todavía queda mucho por hacer. ¿Qué quiero decir con esto? El sistema se basa en gran medida en las sospechas del sector privado donde son necesarias debido a que, como usted bien sabe, no se puede tener y no se debería tener un policía en todas partes mirando todo en términos de transacciones financieras. Por lo tanto, siempre ha habido una confianza desde el principio del GAFI en la premisa de que el sector privado es el más indicado para determinar quiénes son sus clientes y dónde se encuentran sus vulnerabilidades o riesgos. Creo que el GAFI tomó bastante tiempo para determinar qué cosas aparte de los reportes de operaciones sospechosas se espera del sector privado. Se retrasó en llegar a una comprensión más detallada de que una asociación no sólo significa cómo se está haciendo el trabajo asignado en virtud de la legislación nacional de presentación de reportes de operaciones sospechosas sino si usted lo está haciendo bien y si también están ayudando en lo que la ley permite.

El nivel de presentaciones defensivas se redujo en los últimos años, pero tengo la sensación de que no se ha reducido tanto como posible. Hay una serie de razones para ello. Una de ellas es el nivel de las relaciones de trabajo entre los componentes del lado del gobierno de ALD y el aspecto financiero. Es

necesario que haya mucho más alcance para explicar al sector no bancario, en particular, lo que se espera de ellos y cómo pueden mejorar su identificación de transacciones sospechosas o inusuales. Creo que si esto continúa a lo largo de la pista que se ha iniciado en los últimos años, a continuación las asociaciones público-privadas significarían mucho más que el número de reportes de operaciones sospechosas presentados, sino más bien qué valor añadido tiene la institución financiera o que la designada empresa o profesión no financiera ha podido dar a las investigaciones legítimas.

El nivel de comprensión de las agencias gubernamentales que forman parte del sistema de ALD hoy en día es absolutamente increíble

Por ejemplo, ha habido un experimento en el Reino Unido a lo largo de los últimos 12 meses, donde el gobierno ha formado un grupo de tareas con un número de agentes examinados de los bancos comerciales privados y les ha dado una mayor autorización de seguridad. Pueden discutir con ellos los casos en curso en beneficio de las investigaciones de esos casos. Creo que es algo que vale mucho la pena probar. Todavía no se sabe cuál será el resultado, pero yo personalmente creo que cuando se tienen oficiales de cumplimiento profesionales en la institución financiera, como hemos tenido durante muchos años, no estamos haciendo suficiente uso de sus conjuntos de habilidades si únicamente dependemos del reporte de transacciones sospechosas en lugar de en sus juicios profesionales sobre por qué se producen las transacciones de carácter sospechoso.

AT: ¿Cuáles son tus mayores logros mientras estabas en GAFI?

RM: Mi historia comienza cuando yo era fiscal e hice investigaciones hace muchos años. Empiezo allí porque los obstáculos en lugar ya no están tan en lugar como solían estarlo en términos de seguir el rastro del dinero. Uno de los mayores cambios, mejoras y logros es que si alguien realizaba una investigación financiera que involucraba transacciones fuera de su jurisdicción, a menudo encontrarán una piedra en el camino. Ya sea una piedra en términos prácticos o jurídicos de un país determinado, que podía o no darles información. Y no estoy hablando sólo de información sobre el beneficiario y los paraísos fiscales secretos, aunque se trate de un elemento importante que se está superando gradualmente.

Pero el hecho mismo de que el GAFI ha podido ahora ampliar su modelo de operación a más de 190 jurisdicciones, y el hecho de que todas las jurisdicciones tienen leyes contra el lavado de dinero y se evalúan de la misma manera, las expectativas se entienden. A pesar de que no se cumplan todas en el mismo nivel, por diversas razones es la única mejora mayor que se ha producido, de la que me siento orgulloso de haber sido aunque no sea más que una parte pequeña. Esto ha significado que el mundo se ha convertido—en términos de transacciones financieras y rastreo de ellas—en un lugar mucho más pequeño de lo que solía ser. Por ejemplo, ahora hay nueve órganos regionales de tipo GAFI. Hace 20 años había uno o dos y en una etapa muy inmadura de desarrollo. Ahora el mundo está más o menos cubierto en términos del modelo de estilo GAFI y los órganos de estilo GAFI.

Pero ¿qué significa esto en la práctica? Significa que todos saben que todos esos cuerpos—mientras mantienen operaciones independientes suscritas a los estándares—tienen los mecanismos de cumplimiento para ayudar a sus países para el cumplimiento. El nivel de comprensión de las agencias gubernamentales que forman parte del sistema de ALD hoy en día es absolutamente increíble. Esto no quiere decir que hay un sistema perfecto. Sin embargo, en comparación con lo que fue el caso hace muchos años, estamos hablando del “día y la noche”. En otras palabras, un país en el hemisferio occidental que quiera llevar a cabo una investigación en relación con las actividades en un país en África o Asia, se encuentra en un mucho mejor lugar ahora que antes debido a la existencia de los órganos regionales de tipo GAFI y el hecho de que su existencia ha significado que los países

de esas regiones son todos miembros de estos órganos y deben aplicar las mismas normas y deben darles seguimiento a reportes de evaluación mutua en los que se han detectado deficiencias. Creo que tanto en un sentido estratégico y en un sentido práctico esto ha sido el mayor logro individual y está mejorando año tras año.

AT: Si estuviera hablando con una clase universitaria sobre el campo de ALD como una carrera, ¿qué diría?

RM: Les diría que ya no es sólo cosa de policías y ladrones. Se trata de todo un grupo de importantes cuestiones internacionales, la seguridad y la integridad financiera, porque mantener el rastro del dinero y de mantenimiento de los sistemas financieros lo más limpio posible es la esencia del trabajo. El GAFI maduró por la necesidad de los acontecimientos mundiales a una organización que se ha dado la tarea de ser esencialmente el principal órgano responsable de identificar, detener y mantener a raya todo tipo de fondos ilícitos que fluyen a través de los sistemas financieros nacionales e internacionales.

Por lo tanto, cuando se lo mira desde esta perspectiva, el mundo de interés para una persona joven es mucho más amplio que la simple aplicación de la ley. No me refiero a subestimar las agencias de control legal. Por el contrario, yo mismo solía trabajar en el campo. Sin embargo, creo que si usted mira este campo ahora, está mirando las relaciones exteriores, la diplomacia, el derecho internacional, los reglamentos financieros y las nuevas formas de pago (mecanismos) en las que se transfieren dinero y valor. Por lo tanto, existe toda una serie de nuevos énfasis y nuevas formas de mirar cómo se envía dinero y valor y cómo se tramita el dinero malo.

Estas son cuestiones que creo que son más atractivas para las personas más jóvenes que antecedentes más estrictos de agentes de control legal o una carrera como podría haber sido en el pasado. Por lo tanto, creo que es un espacio más amplio y mucho más emocionante y uno que para aquellos que tienen un interés en estos temas y un sentido del deber por sus puestos de trabajo, ofrece una capacidad más amplia para servir a esos intereses y ese sentido del deber. **TA**

Entrevistado por: John J. Byrne, CAMS, vicepresidente ejecutivo, ACAMS, Centreville, VA, EE.UU., jbyrne@acams.org

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 fit right in with what you're doing today, and reduce your cost of labor.

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

ACAMS IN PROGRESS

PREV 9 OF 13 NEXT

Money Laundering Basics

How the Financing of Terrorism Might Work

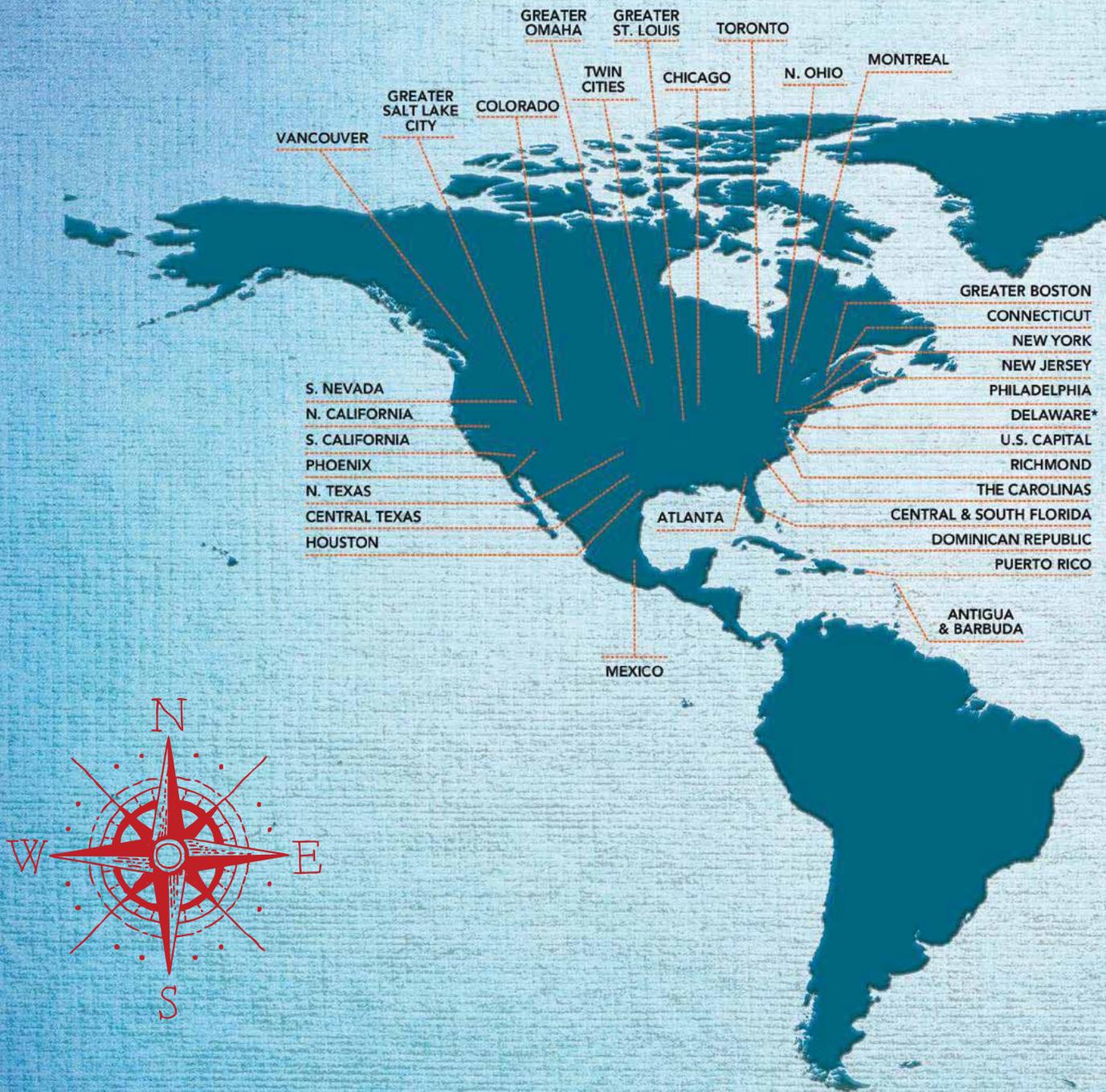
Key techniques reflected in this situation, which would not have been identified during customer due diligence, include:

- Using multiple bank accounts controlled by unknown person(s) in countries with less stringent banking regulations
- Using seemingly legitimate organizations as "fronts"
- Engaging in what appear to be legitimate merchant transactions
- Exchanging money from one currency to another

CONTINUE

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

ACAMS® | CHAPTERS



The ACAMS Chapter Development Program aims to focus the association's international efforts in anti-money laundering education and training at a local level. Chapters foster professional relationships and provide local forums for discussion around region-specific issues.

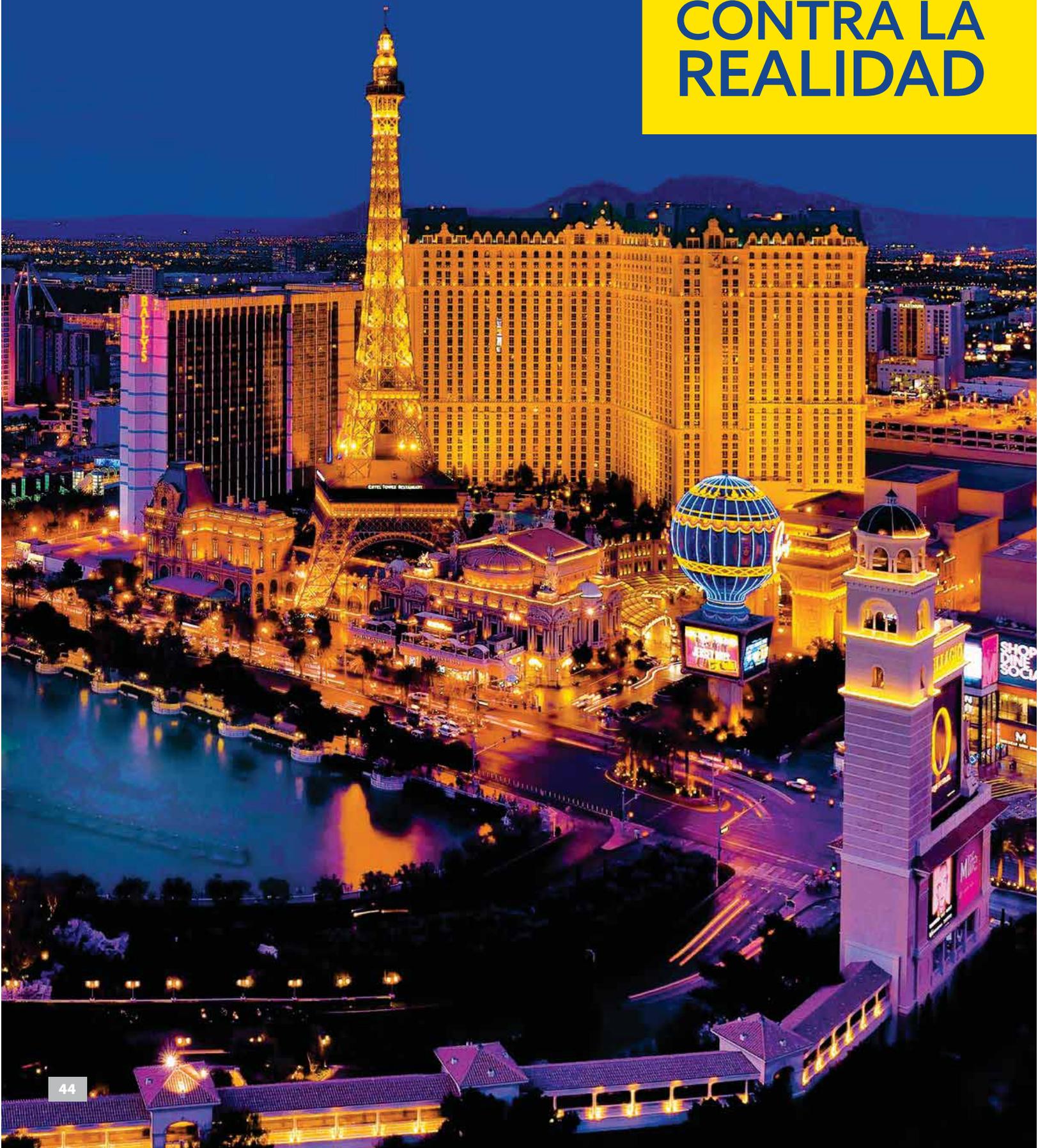
**Chapters launching soon*

Cultivating Comradery Worldwide



Find a local ACAMS chapter near you or start one today!
www.acams.org/chapters | chapters@acams.org

LA FANTASÍA CONTRA LA REALIDAD



Los casinos son un negocio bastante arcano ya que no hace mucho tiempo el juego legal se limitaba a los estados de Nevada y Nueva Jersey. Para que nadie piense de otro modo, operar un exitoso casino legal es mucho más difícil de lo que parece. Las caras sonrientes de los agentes y el ambiente festivo desmienten la intensidad de la operación. Todos los matices de la sala de juego están controlados para garantizar que los tramposos no tengan la sartén por el mango y que los clientes tengan un juego justo.

Los pocos a los que se les juzga dignos de operar casinos están expuestos a exhaustivos controles de antecedentes antes de recibir la codiciada licencia. Además, las comprobaciones intrusivas de idoneidad siguen, siempre y cuando la persona tiene la licencia. Cualquier atisbo de incorrección podría obligar a un licenciataria a presentarse ante un consejo regulador del juego para explicar sus acciones.

Gracias a Hollywood, abundan los estereotipos de casinos y de los que los operan. Un agente especial del Servicio de Impuestos Internos (IRS) de Las Vegas dijo una vez en una reunión de directores de cumplimiento de la industria del casino que “Hay quienes están fuera de Nevada, que piensan que todos los casinos son propiedad de Robert De Niro, y

que su programa de lucha de antilavado de dinero (ALD) está dirigido por Joe Pesci”. Este agente del IRS estaba reconociendo empáticamente los desafíos que enfrentan los casinos en la superación de vistas incubadas por la cultura pop. A pesar de que los casinos están muy regulados, con frecuencia auditados y cotizan en bolsa, la época pasada de figuras del delito organizado que subrepticamente gestionan ciertos casinos todavía persigue inmercedamente a la industria.

El establecimiento de una cultura de estricta adherencia a los procedimientos y el fomento de la integridad de los empleados es fundamental para una operación de juego. En este sentido, los casinos y bancos comparten algo en común. Sin embargo, los casinos en muchas áreas no son como los bancos. Si bien los bancos están en el negocio de transferir y almacenar el dinero de usted, los casinos se encuentran, en gran parte, en el negocio de ganar y perder dinero. Aunque los casinos proporcionan servicios para facilitar el juego, tienen poco interés en las transacciones financieras que no aportan clientes a las mesas o máquinas tragamonedas. Un mantra común entre los cajeros del casino cuando los clientes solicitan una transacción financiera no relacionada con el juego es, “Lo siento, no somos su banco”.

Incluso comparar los informes de transacciones en efectivo (CTR) de los bancos y casinos es como comparar manzanas con naranjas. Si un banco presenta un CTR por \$10.000, por lo general significa que el cliente entró con \$10.000 en efectivo. Sin embargo, esto no es cierto para los casinos. Esto es debido a que la Red Contra los Delitos Financieros (FinCEN) requiere de los casinos que totalicen cada vez que un cliente deposita dinero en una mesa de blackjack o alimenta dinero en efectivo en una máquina tragamonedas. La diosa Fortuna a menudo lleva a los clientes a retirar su dinero, tomar un descanso y pasar a otra mesa o tragamonedas. A pesar de que es el mismo efectivo, las nuevas apuestas todavía están incluidas en el total de dinero del día. Es como que un cliente de un banco depositara \$5.000, y de inmediato retirara todo para luego ir a otro cajero y repetir la operación. Hay una lógica a esta regla de la FinCEN, pero las agencias de control legal a menudo tienen que ser educadas sobre cómo interpretar los CTR de un casino.

Una manera práctica de entender los programas de ALD de los casinos es comprender primero cómo se produce el lavado de dinero en un casino y después cómo se detecta la mencionada actividad.

El disfrute del dinero sucio

La forma más común de lavado de dinero en un casino es simplemente el disfrute de las ganancias mal habidas.¹ Esta es la etapa final del ciclo de lavado de dinero (integración). La mayoría de las veces, los clientes disfrutan del “dinero malo” jugando sin ocultar su identidad. En estas situaciones no hay diferencias apreciables entre los delincuentes que gastan dinero ilícito y un jugador que usa fondos legítimos. La única excepción podría ser un aumento significativo en el juego. Un aumento sustancial en las apuestas mensuales promedio de un cliente podría indicar que alguien puede haberse enriquecido por medio de una actividad delictiva. Sin embargo, no es infrecuente que los jugadores legítimos tengan un pico en el juego. Esto sucede a menudo cuando un casino atrae a un cliente de la competencia.

Una manera práctica de entender los programas de ALD de los casinos es comprender primero cómo se produce el lavado de dinero en un casino y después cómo se detecta la mencionada actividad

Para examinar a los delincuentes que disfrutan de su dinero libre de impuestos, los casinos se basan en procedimientos de diligencia debida establecidos para identificar posibles casos de fondos ilícitos que entran en el casino. En marcado contraste con el pasado, la FinCEN ha aconsejado enérgicamente a los casinos que tienen la obligación de utilizar toda la información disponible para determinar el origen de los fondos de los clientes. Esto incluye lo que cualquier empleado del

¹ “National Money Laundering Risk Assessment,” United States Treasury, 2015, <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20E2%80%932006-12-2015.pdf>



Foto por: Joseph Sohm / Shutterstock.com

casino (tales como gerentes, anfitriones, o el personal de desarrollo de jugadores) sabe acerca del origen de los fondos del cliente.

La implementación de un proceso adecuado de diligencia debida incluye entrenar empleados que regularmente interactúan con los jugadores mayores sobre cómo detectar las alertas rojas—en particular como detectar a una persona que puede estar cometiendo fraude o malversación de fondos. Curiosamente, a veces los malversadores piensan que la diosa Fortuna va a resolver todos sus problemas. Sólo unas pocas “grandes ganancias” les permitirán proveer las cuentas de dinero robado de donde todavía sobrará dinero o se disfrazará el origen real de los fondos.

Evitando la detección (estructuración)

De acuerdo con FinCEN, los reportes de operaciones sospechosas (ROS) más comunes presentados son para la estructuración de transacciones para evitar un CTR. Muchos

De acuerdo con FinCEN, los reportes de operaciones sospechosas (ROS) más comunes presentados son para la estructuración de transacciones para evitar un CTR

ROS presentados por dinero en efectivo se refieren a la redención de fichas. Estas son situaciones en las que los clientes tienen más de \$10.000 en fichas en su poder, pero optan por cobrar menos.² La FinCEN ha utilizado el término “ficha caminante” para describir este comportamiento y poner sobre aviso a la industria para reportar casos en los que la ficha caminante indicaría un intento de evitar un CTR. La FinCEN reconoce que no todas las fichas caminantes son sospechosas, pero afirma que no puede haber “razones menos inocentes” por las que un cliente sale de un casino con fichas.³

Hay razones legítimas por las que una persona puede no querer efectivo por todas sus fichas, especialmente si el cliente planea regresar al casino para seguir jugando. Para mitigar el riesgo, los casinos revisan situaciones en las que aparece que un cliente ha retenido una cantidad excesiva de fichas. Cada circunstancia debe ser evaluada para determinar si hay aspectos que despiertan sospechas. Por ejemplo, el cliente continuamente hace reembolsos por debajo de la cantidad que hay que informar durante viajes posteriores. Curiosamente, las fichas caminantes están vinculadas por lo general a los clientes con más ganancias de juego que pérdidas en un día, y gran parte de los fondos legales originarios vienen del casino.

Evitando la detección (ocultación de identidad)

Los agentes de control legal han alertado a los casinos que vigilen a las personas que intentan usar una credencial falsa para inscribirse en los programas de fidelización de clientes o a delincuentes que utilizan la tarjeta del programa de fidelización de otro.⁴

Los casinos utilizan los programas de fidelización para fomentar el juego y recompensar a los clientes con compensaciones (comidas, habitaciones de hotel, espectáculos) en función de su nivel de juego. Cuanto más juega un cliente, más compensaciones gana. Los programas de fidelización monitorean el juego por medio de una tarjeta de fidelización, que se inserta en las máquinas tragamonedas o se entrega al distribuidor.

Para mitigar el riesgo de que alguien use una tarjeta de fidelización para ocultarse, los casinos requieren una credencial válida para entrar en el programa de fidelización. Además, sin tener en cuenta si un cliente utiliza la tarjeta de fidelización, los clientes estarían obligados a proporcionar una credencial válida para llevar a cabo las transacciones de divisas por arriba de cierta cantidad de dólares. Sea o no que se utilice una tarjeta de fidelización, si las transacciones de divisas agregadas de un/a cliente excede \$10.000 en un día y él/ella se ha negado a proporcionar una credencial válida y su número de seguridad social, al cliente se le prohibirá seguir jugando.

La conversión del dinero sucio

Las organizaciones del narco y las delictivas de uso intensivo de efectivo frecuentemente usan billetes de \$100 para la compra de contrabando y para almacenar sus ganancias mal habidas. Por lo tanto, los agentes de control legal hacen hincapié en buscar clientes que convierten billetes de baja denominación a billetes de \$100, con un énfasis cuando hay un mínimo de actividad de juego.⁵ Este método de lavado de dinero se conoce como “relleno de billetes”. El relleno de billetes podría aplicarse también a la conversión de billetes de

² Información compartida por agentes de control legal durante las reuniones de trabajo entre los directores de cumplimiento de casinos en Las Vegas y los agentes de control legal.

³ “Prepared Remarks of Jennifer Shasky Calvery, FinCEN, 12 de junio del 2014, https://www.fincen.gov/news_room/speech/html/20140612.html

⁴ Información compartida por agentes de control legal durante las reuniones de trabajo entre los directores de cumplimiento de casinos en Las Vegas y los agentes de control legal.

⁵ Información compartida por oficiales del gobierno durante la Conferencia de la Ley del Secreto Bancario de 2016 en Las Vegas.



Se ha sabido de delincuentes que usan fichas de casino como forma alternativa de moneda

\$100 a los nuevos billetes de \$100—los nuevos billetes son deseables si los criminales quieren deshacerse del dinero cargado de residuos de drogas o si sospechan que están marcados.

El relleno de billetes funciona de la siguiente manera: El cliente alimenta una tragamonedas y luego solicita un vale de caja. El cliente, a continuación, utiliza una máquina de quiosco para canjear el vale por billetes de \$100. Los quioscos se encuentran generalmente a lo largo de la sala de juego para la conveniencia de manejar las transacciones más pequeñas sin que el cliente tenga que ir a la caja (la caja del casino). Como un control de ALD, los quioscos son limitados en la cantidad de moneda que puede redimirse cada vez. Vales de más de este límite se canjean en la caja, donde a los clientes se les puede requerir proporcionar una credencial válida.

Además, los comprobantes de caja tienen una fecha de vencimiento—por lo general no más de 180 días—lo que limita su longevidad como forma de moneda. Sin embargo, la inteligencia proporcionada recientemente por el FBI sugiere que los delincuentes han utilizado los vales de caja para transferir fondos de un confederado a otro.⁶

Como mecanismo de prevención, los sistemas de quioscos de casino generarán alertas en tiempo real que identifican los casos de posible relleno de billete. Estas alertas les permiten a los casinos adoptar medidas inmediatas para detener la actividad, si se considera sospechosa, e informar de ello. En gran medida las cámaras de vigilancia omnipresentes desde varios ángulos ayudan a la identificación de los culpables.

El uso de fichas para facilitar la actividad ilegal

Se ha sabido de delincuentes que usan fichas de casino como forma alternativa de moneda. Las fichas se pueden usar para almacenar o transferir fondos a aliados. Los delincuentes creerán que la posesión de fichas de casino les da una coartada conveniente según la cual su dinero proviene de ganancias de juego. Como se detalla en una acción de cumpli-

miento reciente en un club de cartas del sur de California, los delincuentes utilizaron fichas de juego para facilitar “casinos” ilegales y clandestinos que operaban en casas de lujo. Como reveló la investigación, el principal acusado transfería fondos ilegales al club de cartas y el casino le daba fichas.⁷ Fuentes judiciales sugieren que los jugadores de póquer de altas apuestas son conocidos por acumular fichas en cajas de seguridad para evitar la detección del IRS.

Un control para reducir el riesgo de que se utilicen fichas para fines nefastos es la validación de si el cliente al redimir las fichas tenía ganancias de juego de fichas antes de la adquisición. Se aplican procedimientos similares a los que solicitan reembolsos de los vales de caja de salida del casino. Los casinos no hacen dinero en efectivo de las fichas de casinos de la competencia a menos que confirmen que el cliente ha adquirido legítimamente las fichas del casino de la competencia. Téngase presente que también hay una finalidad operativa en determinar la propiedad de las fichas en cuanto que estos procedimientos ayudan a identificar el robo de fichas del casino o de otro cliente.

Facilitar las operaciones de apuestas deportivas ilegales

Unos meses antes del Super Bowl de 2015, la FinCEN emitió una carta a la American Gaming Association (AGA) en relación con las apuestas deportivas legales. La carta decía: “Ha llegado a la atención de la Red Contra los Delitos Financieros y sus colegas de agencias de control legal y reguladores que

el aumento de apuestas deportivas realizada en nombre de terceros está facilitando la actividad delictiva y que presenta un riesgo de lavado de dinero al sistema financiero de los EE.UU.”. Como medio para equilibrar su riesgo operacional, se ha sabido que las operaciones de apuestas deportivas ilegales han utilizado subrepticamente a terceros para realizar apuestas deportivas legales en Nevada. Los corredores de apuestas ilegales, que operan principalmente fuera de Nevada, obtienen ingresos de la usura y el cobro de una tarifa basada en un porcentaje de la apuesta en lugar de tomar una posición sobre el resultado del juego. Estas empresas delictivas intentan equilibrar sus apuestas “despidiendo” sus posiciones sobreexpuestas sin que se las detecten.⁸

En la carta a la AGA, la FinCEN aconsejó a los de apuestas en Nevada que investigaran entre sus clientes de apuestas deportivas—cuyas transacciones de efectivo se acercan a los umbrales de notificación—si se están llevando a cabo la transacción en nombre de otro. De acuerdo con la FinCEN, estas investigaciones de clientes de apuestas permitirían cumplir con el requisito del CTR para informar si la operación la lleva a cabo un tercero.⁹

En respuesta a la carta de la FinCEN, Geoff Freeman, presidente de la AGA, declaró públicamente: “Si bien los casinos buscan rutinariamente apuestas sospechosas en las apuestas deportivas y han trabajado con los agentes de control legal para identificar la actividad ilegal, que en algunos casos conducen a condenas, tal supervisión no existe para el mercado de las apuestas deportivas ilegales”.¹⁰

⁶ Información compartida por agentes de control legal durante las reuniones de trabajo entre los directores de cumplimiento de casinos en Las Vegas y los agentes de control legal.

⁷ “Twenty Five People Charged as Members of \$10 Million Illegal Gambling and Money Laundering Operation,” U.S. Attorneys Southern District of California, 9 de diciembre del 2015, <https://www.justice.gov/usao-sdca/pr/twenty-five-people-charged-members-10-million-illegal-gambling-and-money-laundering>

⁸ Letter to Geoff Freeman, president and CEO of AGA, FinCEN, 24 de diciembre del 2014, https://www.fincen.gov/statutes_regs/guidance/pdf/01162015.pdf

⁹ Ibid.

¹⁰ Brett Wolf, “U.S. Treasury Warns Casinos on Illegal Sports Betting,” Reuters, 16 de enero del 2015, <http://www.reuters.com/article/gambling-sports-casinos-idUSL1N0UV2EK20150116>

Pagando los gastos de otros

Pagar los gastos o la deuda de otro es una técnica de lavado de dinero de un siglo de antigüedad utilizada para transferir fondos ilícitos sin crear rastro del dinero del pago entre los confederados. El IRS ha alertado a los casinos del riesgo asociado con los pagos de terceros utilizados para establecer cuentas falsas o marcadores de pago. Las cuentas falsas (front money accounts, en inglés) son las cuentas de saldo de crédito que los clientes utilizan para financiar los juegos de azar y los marcadores son préstamos de casino para financiar los juegos de azar.

El riesgo aumenta exponencialmente cuando los pagos de terceros están originados en una entidad o en individuos no relacionados, con mayor razón si tienen carácter internacional. Las transferencias extranjeras son de riesgo especial, dada la limitada capacidad para llevar a cabo la diligencia debida del pagador. Muchos casinos no aceptan estas transferencias a menos que puedan establecer la conexión legítima entre el pagador y el beneficiario.

En un caso reciente del FBI/IRS, los delincuentes utilizaron los pagos de terceros para transferir fondos ilícitos de una operación ilegal de apuestas deportivas para financiar una cuenta falsa en nombre de un cómplice.¹¹ Además, los agentes de control legal recientemente encontraron a un estafador tratando de financiar la cuenta falsa de un cómplice con una transferencia bancaria superior a un millón de dólares. El casino, sin darse cuenta de la malversación de fondos, se negó a la transferencia porque no podía validar la legitimidad de la transacción.¹²

Lavado

Se ha unido bastante intriga a la idea del juego para hacer que el “dinero sucio” parezca limpio. En internet no es difícil encontrar a alguien que pontifique sobre las posibles maquinaciones de apuestas que se pueden desplegar para dar la ilusión de que los fondos provenían de ganancias. Sin embargo, estos métodos deben tener una señal de advertencia con luces de neón. El intento de lavar los fondos por medio del juego está plagado de

peligros. Por ejemplo, un lavador de dinero en realidad podría perder todas las ganancias mal habidas en el casino. Es sólo la naturaleza de la inquebrantable ley de la probabilidad y la ventaja de la casa.

A menudo, el juego final de aquellos que tratan de “lavar” su dinero es obtener un pago en forma de cheque de casino. Depositar un cheque de casino en un banco es menos sospechoso porque el banco supondrá que se trata de ganancias del juego. Por desgracia para los lavadores de dinero, no se puede comprar un montón de fichas simplemente, caminar por el casino sin jugar e ir a la caja para obtener un cheque. Un cheque de pago no está permitido a menos que se valide que los fondos fueron puestos en riesgo (se jugaron) y el cliente obtienen ganancias. También se aplica cuando un cliente solicita que el dinero restante se transfiera.

A pesar de que los casos conocidos son infrecuentes, las técnicas de apuestas compensatorias permitirían que los lavadores de dinero pusieran todos sus fondos en riesgo sin exponer su dinero sucio a pérdidas significativas en el juego. La apuesta compensatoria consiste en el proceso de colocar apuestas iguales en ambas posibilidades de resultados de un juego del casino. Por ejemplo, en la ruleta, colocar apuestas iguales en negro y rojo sin esperanza de recibir demasiados verdes. Si sólo un cliente intentara apuestas compensatorias, se sospecharía. Para reducir la sospecha, un lavador de dinero contaría con aliados que coloquen el otro lado de las apuestas. El personal de vigilancia, sin embargo, también le presta atención a detectar clientes de apuestas en equipo.

Para identificar los casos de desplazamiento de apuestas para obtener cheques, los casinos pueden revisar a los clientes que reciben valor en dólares de pagos y determinan cómo cada cliente ha financiado su actividad de juego. Las situaciones en las que los clientes financian su juego con dinero y constantemente solicitaron un cheque pueden justificar aún más diligencia debida.

Un método que los narcotraficantes han desplegado para dar la ilusión de que los fondos fueron originados de las ganancias de juego es un esquema de W-2G. Un W-2G es una forma requerida para presentarla anualmente ante el IRS cuando un cliente obtiene un premio

mayor a \$1.199. Las reglas requieren que cuando un cliente logra un premio mayor de notificación obligatoria, la máquina tragamonedas se cierra y un empleado del casino se acerca al cliente para obtener un documento de identidad válido y su número de seguridad social. Al cliente entonces se le emite una copia del W-2G. En este punto, el cliente podría solicitar que se le pague en efectivo. Los pagos en efectivo del premio gordo (jackpot, en inglés) no se incluyen en el cálculo de la moneda para fines de CTR porque la FinCEN ha dictaminado que estas cantidades ya se reportan al gobierno federal por medio de los W-2Gs.

El esquema W-2G es bastante simple, ya que sencillamente se limita sólo a sentarse ante una máquina tragamonedas y jugar hasta obtener suficientes W-2Gs para apaciguar a cualquiera que pregunte sobre su monto de dinero. Porque los W-2Gs no son más que instantáneas de la actividad de juego durante todo el año son indicadores bastante pobres de los ingresos reales netos de juego. No es raro que los que están en posesión de numerosos W-2Gs sean perdedores netos al final del año.

Pero aquellos que no están familiarizados con la naturaleza de los juegos de azar pueden considerar que los W-2Gs son prueba de que el dinero de la persona venía de viajes exitosos a los casinos. Esta lógica defectuosa es similar a la evaluación de los ingresos por operaciones de bolsa con sólo sumar las ganancias brutas de la venta sin tener en cuenta el coste de dichas acciones. Las reglas bastante fosilizadas de W-2Gs fueron promulgadas por el Congreso en 1970. Cualquier intento de modificar las normas debe tener en cuenta la vulnerabilidad que el lavado de dinero les ha impuesto a los casinos.

Lo que ha alcanzado el punto máximo de interés de los agentes de control legal en los últimos tiempos es un cliente que utiliza pagos de terceros para dar la ilusión de ganancias en el juego.¹³ Un pago de terceros podría permitirle a un fondo común parecer que se originó de una ganancia de casino. El esquema tendría las características siguientes: Un usuario obtiene un marcador de casino para financiar sus apuestas durante su viaje. Si al final del viaje, el cliente tiene suerte, entonces utiliza sus ganancias para pagarle al marcador y le pide el

¹¹ “Twenty Five People Charged as Members of \$10 Million Illegal Gambling and Money Laundering Operation,” U.S. Attorneys Southern District of California, 9 de diciembre del 2015, <https://www.justice.gov/usao-sdca/pr/twenty-five-people-charged-members-10-million-illegal-gambling-and-money-laundering>

¹² Información compartida por agentes de control legal durante las reuniones de trabajo entre los directores de cumplimiento de casinos en Las Vegas y los agentes de control legal.

¹³ Discusiones recientes del autor con agentes de control legal.

saldo restante, ya sea como cheque o como transferencia bancaria. En viajes posteriores al casino, si el cliente es un perdedor neto, el cliente intenta pagarle al marcador por medio de un pago de terceros. De esta manera los registros bancarios del cliente sólo muestran los juegos de depósitos ganadores, pero no muestran el reembolso de los marcadores.

Una palabra sobre los clubes de cartas

Una revisión de las notas de prensa del Departamento de Justicia y de la FinCEN revela que una parte notable de las recientes acciones de aplicación de los casinos han sido en clubes de cartas. Hay una distinción reglamentaria entre los casinos al estilo de Las Vegas y los clubes de cartas. A los clubes de cartas se les emite una licencia de "Clase II", que sólo les permite ofrecer juegos donde los clientes juegan unos contra otros y el club de cartas obtiene ingresos en el "rastrillo" (la tasa cobrada por mano a cada jugador). En las operaciones de Clase II, los jugadores son sus propios bancos y el club de cartas participa en el juego. A los casinos que ofrecen juegos al estilo de Las Vegas se les concede una licencia "Clase III", que los autoriza a ser bancos de los jugadores y a obtener ingresos de las ganancias.¹⁴ En general, existe un régimen regulador más robusto para los casinos de Clase III.¹⁵ Se ha sabido de algunos clubes de cartas que subrepticamente han sido el banco de jugadores, lo que podría ser una violación del Título 18, Sección 1955, de apuestas ilegales.¹⁶

Conclusión

Ha habido una serie de acciones de aplicación de casino, pero un estudio reciente llevado a cabo por Ernst & Young demuestra que muchos de los casinos más importantes han estado tomando en serio sus responsabilidades para implementar robustos programas de ALD.¹⁷ Como ex directora de la FinCEN, Jennifer Shasky Calvery señaló en un discurso ante la American Banking Association que los

casinos han hecho grandes esfuerzos para mejorar sus programas de ALD y cumplir con las expectativas regulatorias actuales.

Sin lugar a dudas, los casinos sí plantean ciertas vulnerabilidades de lavado de dinero, dada la intensidad de las transacciones de divisas. Dicho esto, la Evaluación Nacional de Riesgo de Lavado de Activos de 2015 del Tesoro de los EE.UU. indica que los delincuentes no se han inclinado hacia los casinos sobre las instituciones financieras tradicionales y no tradicionales. Los casinos ni siquiera fueron mencionados en la Evaluación Nacional de Riesgo de la Financiación del Terrorismo de 2015 del Tesoro.

Sin importar dónde los casinos encajan en la gama del lavado de dinero, no tienen excusa para evitar hacer del cumplimiento una de las principales prioridades. La FinCEN y el IRS han demostrado que responden con rapidez y castigando a los casinos que empiezan a fallar intencionalmente en la responsabilidad reguladora. Para mantener el ritmo de los ciclos regulatorios de examen de la banca, el IRS está desplegando ahora más recursos para garantizar que se examina una franja más amplia de casinos.¹⁸

En los EE.UU., el régimen regulador de los casinos de Clase III desempeña un papel significativo en la reducción del riesgo de lavado de dinero, asegurando que los malos actores no puedan controlar los casinos. Casino es una película críticamente aclamada y clásica, pero cuando usted vea esas películas no deje que colorean su opinión sobre cómo operan los casinos de hoy. Hay pocos momentos en los que Hollywood se intersecta con la realidad. Los personajes interpretados por De Niro y Pesci no tendrían ninguna posibilidad de obtener una licencia de casino de Clase III en el ambiente regulatorio del juego de hoy. **A**

Paul Camacho, CAMS, vicepresidente de cumplimiento de ALD, Station Casinos LLC, Las Vegas, NV, EE.UU., paul.camacho@stationcasinos.com

¹⁴ Legal Distinction Between Class II and Class III Gaming, 4 de octubre del 2011, IndianCountry.com

¹⁵ California Tribes Score Victory in War with Card Rooms, 26 de febrero del 2016, Onlinepokerreport.com

¹⁶ Ibid.

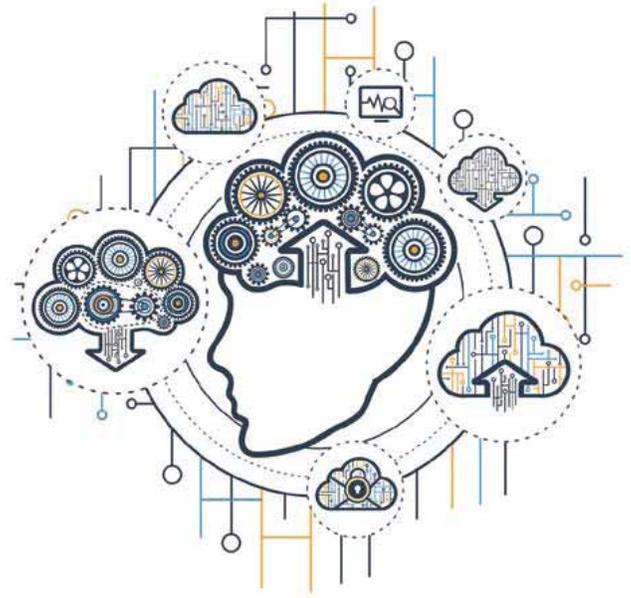
¹⁷ "Investing in America's Financial Security: Casinos' Commitment to Anti-Money Laundering Compliance," AGA, enero de 2016, <https://www.americangaming.org/sites/default/files/AGA%20AML%20Research%20Report%20Final%20011916.pdf>

¹⁸ Comentario de oficiales del Tesoro en la conferencia de BSA de Casino de 2016 en Las Vegas.



SOLUCIONES DE CUMPLIMIENTO:

La combinación de la computación cognitiva con la inteligencia humana



Históricamente, las herramientas de la tecnología han ofrecido soluciones que proporcionan conclusiones basadas en el análisis de datos estáticos y datos transaccionales asociados con actividades bancarias específicas. Los diferentes tipos de datos varían en gran medida. Para nombrar unos pocos, hay grandes volúmenes de datos, datos de diversos sistemas heredados, datos de archivos compartidos, archivos de datos dispares de sistemas incompatibles, datos incompletos, datos cualitativos, datos numéricos, datos no estructurados, datos que utilizan la terminología que compiten para describir las mismas actividades y más. Para satisfacer los requisitos de cumplimiento, las instituciones financieras, sus líderes de delitos financieros y de cumplimiento y sus respectivos equipos deben tener herramientas para darle sentido a todo. Para satisfacer la alta barra de cumplimiento, las unidades de delitos financieros a menudo han confiado en los equipos cada vez mayores de personas que peinan manualmente a través de resmas de información en un esfuerzo de hacerles frente a los retos con “sabiduría tribal”, experiencia profesional, razonamiento humano y fuerza bruta. El despliegue y la aplicación de la informática que puede simular el proceso de pensamiento humano están siendo considerados por la comunidad de delitos financieros. La implementación de soluciones probadas de computación cognitiva puede ser la respuesta para ayudar a la gente a ser más eficiente.

Hemos llegado a un espacio donde las plataformas de computación cognitiva han demostrado que ayudan a la gente a tomar mejores decisiones y que, en silencio, están demostrando un progreso real para apoyar una variedad de requisitos de negocio a través de muchas industrias verticales. De acuerdo con Allied Market Research,¹ se espera que el mercado de computación cognitiva llegue a \$13,7 mil millones a nivel mundial para el año 2020 con el procesamiento del lenguaje natural como el sector de la tecnología de generación de ingresos de computación cognitiva más alto. El crecimiento del mercado mundial de computación cognitiva se complementará con el creciente volumen de datos de gran tamaño sin estructurar a través de diversos mercados verticales como la salud, la banca y finanzas, de seguridad, y de TI y telecomunicaciones.

Con este avance, muchas organizaciones están empezando a sentir la presión de adaptarse a y adoptar un nuevo paradigma de computación o de riesgo que caiga por la parte trasera de la curva. Sin embargo, tenga en cuenta y no se deje engañar por los sistemas de razonamiento de base amplia que prometen el mundo. Para lograr el mejor éxito en el menor lapso de tiempo, el enfoque de la organización debe estar en sistemas especialmente diseñados que ofrecen soluciones específicas diseñadas para soportar con éxito los problemas de negocio más apremiantes y para ofrecer rápidamente un valor empresarial real. Una de las áreas en las que la computación cognitiva ya ha demostrado su valor en la banca es en la ayuda para automatizar la

ayuda en línea al cliente.² Una vez desplegados, los sistemas de computación cognitiva son capaces de entender rápidamente las solicitudes de los clientes en línea, y recuperar y devolver respuestas aprobadas por la empresa con precisión e inmediatamente mejorar el rendimiento del centro de llamadas para aumentar la satisfacción del cliente.

Los sistemas de computación cognitiva han sido durante mucho tiempo objeto de mucha fanfarria y atención. En su mayor parte, las organizaciones se han quedado en el banco a la espera de ver lo que traería el futuro prometido. Pero, ¿por qué esperan? Esperan porque sigue siendo una lucha ir más allá del marketing estratégico con el fin de identificar soluciones probadas que entregarán una promesa de computación cognitiva fuera de lo previsto. Las organizaciones continúan la búsqueda de evidencia de que las aplicaciones del mundo real se pueden implementar para cumplir con el valor reconocido de computación cognitiva sin una enorme inversión inicial de tiempo y dinero. Las empresas están buscando soluciones que ofrecen impactantes victorias y proporcionan soluciones que proporcionen un valor empresarial inmediato. Un gran lugar para buscar aplicaciones en el mundo real es el Cognitive Computing Consortium. El Consorcio fue co-fundado por Sue Feldman, CEO de Synthesis, y Hadley Reynolds, analista principal de NextEra Research. Fue fundado para proporcionar un foro para investigadores, desarrolladores y profesionales de la computación cognitiva y sus tecnologías afines y para desarrollar una comunidad

¹ <https://www.alliedmarketresearch.com/press-release/cognitive-computing-market-is-expected-to-reach-137-billion-globally-by-2020-allied-market-research.html>

² Customer support in banking, <http://www.expertsystem.com/customer/ing-direct/>

de expertos y profesionales para el intercambio de ideas e información. Según su sitio web, su objetivo es promover y apoyar la investigación en computación cognitiva mediante la creación de alianzas entre las comunidades de investigación, de académicos y de la industria, a través de informes de investigación y publicación de guías prácticas sobre computación cognitiva.³

Los servicios financieros y el cumplimiento regulatorio

Debido a las regulaciones cada vez mayores, la supervisión y el control aparentemente infinito, así como las sanciones financieras resultantes (y daños a la reputación), si no de cumplimiento, los bancos y sus analistas están requiriendo más herramientas de inteligencia para cumplir con la barra muy alta y costosa de cumplimiento. En estos tiempos complejos, la industria de servicios financieros está luchando para asegurar el cumplimiento ya que se encuentra obstaculizada por las brechas tecnológicas relacionadas con las soluciones de cumplimiento basadas en el legado de palabras clave. Para hacerles frente a estos retos, los analistas de cumplimiento están buscando sistemas que trabajen con rapidez, y también con el principio de la comprensión profunda del contenido, el contexto del contenido y el contenido de las conexiones del contenido. Están buscando las máquinas y la tecnología con capacidad de comprender y darles sentido a los datos de la forma en que la gente lo hace en tiempo real. Las soluciones de cumplimiento deben poder ayudar al analista en su proceso de “pensar”, apoyar su esfuerzo por asociar conceptos y conectar los problemas con las soluciones. Deben hacer mucho más que una búsqueda por palabra(s) clave(s).

Además, hay un creciente énfasis en la integración del análisis de la información no estructurada como parte de una solución de cumplimiento efectivo, lo que se traduce en el procesamiento de grandes cantidades de información en un corto período de tiempo. La incorporación de más personas para aumentar la velocidad y la escala ya no es suficiente para asegurar el éxito. La velocidad y la escala deben combinarse con el filtrado más preciso y completo de la información, junto con la flexibilidad de cambiar el alcance y los objetivos del análisis en tiempo real. Ellos deben ser capaces

de alejarse del enfoque de “recuadro negro” y comenzar a identificar con precisión y entregar información relevante de una manera correcta contextualmente. Para lograr esto, los analistas están empezando a entender que la capacidad de analizar mejor el significado de las palabras en contexto que utilizan las soluciones de computación cognitiva de hecho puede superar la dependencia de los métodos más tradicionales de las intervenciones humanas o de aprendizaje automático.⁴

La intersección de la inteligencia humana y la computación cognitiva ha llegado

Cuando se aplica a la gestión del cumplimiento, la computación cognitiva combinada con la inteligencia humana puede ofrecer un valor significativo. Permitir que la tecnología organice y conecte contenidos estructurados y no estructurados de tal manera que se ordena lógicamente, relaciona fácilmente de navegar y procese fácilmente por el cerebro humano es el objetivo de la computación cognitiva. El cumplimiento de esta promesa consiste en la implementación de sistemas electrónicos capaces de utilizar una combinación de palabras clave, la coincidencia de patrones, el análisis lingüístico y semántico profundo en la combinación justa que, cuando tiene éxito, imita la forma que los humanos leen, se relaciona y evalúa el contenido en tiempo real y va más allá de las limitaciones humanas. Inspirado por la capacidad humana de comprender a un nivel profundo, la computación cognitiva basa sus capacidades cognitivas en una combinación de algoritmos de inteligencia artificial que se asemejan a la capacidad humana de comprensión.

Sobrecarga de información

Los bancos están inundados de información y regulación. Una de las áreas clave para que un sistema inteligente ofrezca un valor inmediato es en apoyo de adherirse a los requisitos reglamentarios relacionados con el programa de identificación del cliente (CIP) y de conocer a su cliente (KYC).

El CIP es un requisito de la Ley del Patriota, que también se puede encontrar en muchos mandatos regulatorios internacionales, donde se requiere que las instituciones financieras

verifiquen la identidad de las personas/entidades que deseen realizar transacciones financieras con una entidad financiera.

Además, de acuerdo con la norma KYC de FINRA, “Cada miembro deberá usar diligencia razonable, en lo que se refiere a la apertura y el mantenimiento de todas las cuentas, para conocer (y retener) los hechos esenciales aplicables a cada cliente, dirigidas a la autoridad de cada persona que actúe en nombre de dicho cliente”.⁵

Una de las primeras expectativas de cualquier solución de cumplimiento debe estar en su capacidad para identificar y alertar de forma rápida y precisa las transacciones financieras que involucren a personas y/o entidades incluidas en las listas de vigilancia o identificar y alertar de transacciones sospechosas de todas las partes desconocidas. Para lograr el mejor éxito en el menor lapso de tiempo, el enfoque de la organización debe ser localizar un sistema específico que va a ofrecer una solución específica en apoyo de los problemas más acuciantes de negocio para ofrecer rápidamente valor de negocio real.

Conclusión

Más que software, los sistemas de computación cognitiva ofrecen una solución que permita a las organizaciones de servicios financieros una vía para descubrir la penetración, investigar cuestiones y ofrecer los procesos de toma de decisiones. Como su adopción sigue aumentando en este sector vertical, la computación cognitiva comenzará a ser utilizada para soportar una variedad de diversas funciones de negocios tales como operaciones sospechosas relacionadas con el lavado de dinero, monitoreo de medios sociales y análisis de tendencias, soluciones de autoservicio automatizadas para la atención al cliente, la marca y la reputación de gestión y se probará para proporcionar apoyo para muchos de los desafíos en curso de las industrias regulatorias de cumplimiento. 

Bryan Bell, vicepresidente ejecutivo, Expert System Enterprise Corp., Barrington, IL, EE.UU., bbell@expertsystem.com

Robert A. Goldfinger, presidente, Nominodata, Incline Village, NV, EE.UU., rgoldfinger@nominodata.com

³ <https://cognitivecomputingconsortium.com/mission/>

⁴ http://www.kdnuggets.com/2016/07/machine-learning-hype-reality.html#V6H_LNNk3To.linkedin

⁵ Rule 2090 (FINRA 2012): FINRA Rules, 2000., Duties & Conflicts, Rule 2090 Know Your Customer, SR-FINRA-2010-039 and amended by SR-FINRA-2011-01, 9 de julio del 2012, http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=9858

DESENMASCARANDO EL PREJUICIO EN LOS ALGORITMOS de ALD

El prejuicio dentro de los grandes datos (big data, en inglés) se ha encontrado en todas partes desde los resultados de búsqueda de Google hasta los lugares de entrega de Amazon Prime. A medida que los departamentos de antilavado de dinero (ALD) aumentan su dependencia del análisis y los algoritmos, la necesidad de desenmascarar prejuicios potenciales (incluyendo racial, étnico, religioso y de género) es un tema que ya no se puede evitar.

El movimiento hacia la tecnología avanzada aplicada al ALD y la detección de delitos financieros podría parecer superficialmente que da lugar a la presentación de reportes objetivos de operaciones sospechosas. Sin embargo, el *New York Times* informó que, “los algoritmos pueden reforzar los prejuicios humanos”,¹ mientras que los investigadores han observado que la minería de datos puede heredar los prejuicios de los anteriores responsables de tomar decisiones o reflejar los prejuicios generalizados que persisten en la sociedad en general.²

Los algoritmos son la piedra angular del ALD y de los programas de detección de delitos financieros en empresas de servicios financieros. Es importante entender que los algoritmos se construyen mediante el uso de conjuntos de entrenamiento extraídos de las decisiones humanas hechas en el pasado. Si los seres humanos hicieron regularmente decisiones discriminatorias o incluso involuntariamente discriminatorias en los materiales utilizados para desarrollar el algoritmo, el

CLASE PROTEGIDA:

Característica de una persona que no puede ser objeto de discriminación. Las siguientes características son consideradas “clases protegidas” por la ley federal de los EE.UU.:

- Raza
- Color
- Religión
- Nacionalidad
- Edad
- Sexo
- Embarazo
- Ciudadanía
- Estado familiar
- Estado de Discapacidad
- Estatus de veterano
- Información genética

algoritmo puede producir resultados discriminatorios.³ El resultado más grave de la actividad marcado por un algoritmo de ALD o de delito financiero resulta en que la institución financiera presenta un reporte de operaciones sospechosas (ROS) ante la Red Contra los Delitos Financieros (FinCEN).

Tipos de prejuicio en los conjuntos de datos

Los algoritmos se basan en los datos. El reporte de la Casa Blanca de mayo de 2016 sobre los grandes datos señaló que los datos en sí pueden plantear varios retos relacionados con la equidad:⁴

- *Los datos mal seleccionados, incompletos, incorrectos o desactualizados*—Esta es una manera elegante de decir “entra basura, sale basura”. Sin embargo, las consecuencias de la escasez de datos son significativas para las instituciones financieras que pierden el tiempo revisando falsos positivos y para los individuos identificados incorrectamente como sospechosos o de alto riesgo debido al prejuicio de los datos. Un ejemplo de datos inexactos es que las minorías raciales tienen mayores casos de error en sus informes de crédito que los blancos.⁵ Cuando los datos inexactos se incluyen en un algoritmo de manera desproporcionada, los resultados pueden impactar negativamente en los grupos históricamente desfavorecidos.

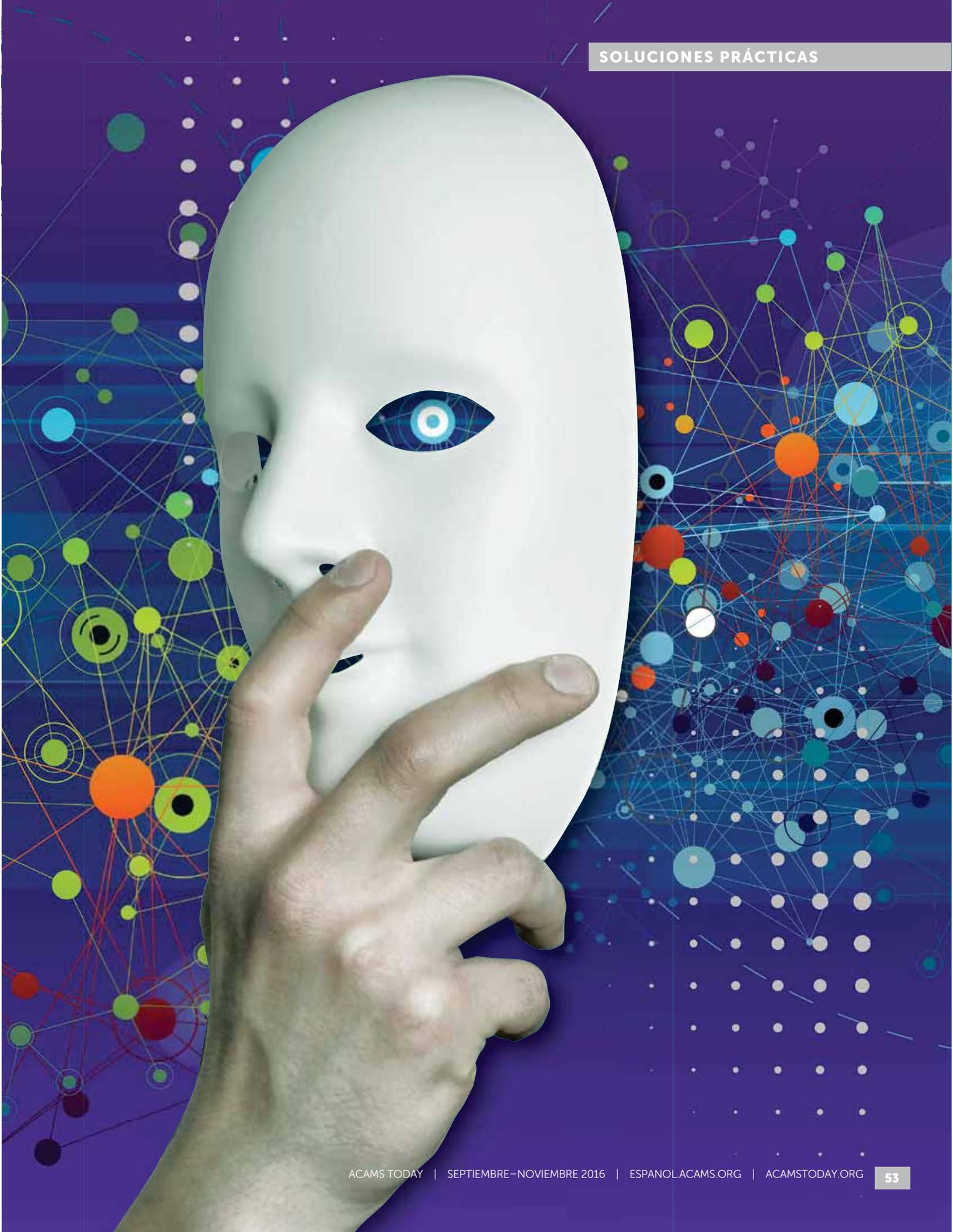
¹ Claire Cain Miller, “When Algorithms Discriminate,” *New York Times*, 9 de julio del 2015, http://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html?_r=0

² Solon Barocas and Andrew D. Selbst, “Big Data’s Disparate Impact,” *California Law Review*, Vol. 104, 2016, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

³ Emily Shaw, “Avoiding prejudice in data-based decisions,” Sunlight Foundation, 31 de julio del 2015, <https://sunlightfoundation.com/blog/2015/07/31/avoiding-prejudice-in-data-based-decisions/>

⁴ “Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights,” Executive Office of the President, mayo de 2016, https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

⁵ “Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003,” Federal Trade Commission, page 60, diciembre de 2012, <https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factreport.pdf>



- *Los sustitutos (proxies, en inglés)*—Los algoritmos pueden usar insumos que en valor nominal (por ejemplo, el código postal y el estado civil) son imparciales, pero en un examen más detenido operan lo mismo que un clasificador discriminatorio como la raza. Los investigadores han encontrado que las situaciones de este tipo son posibles cuando los criterios realmente relevantes en la toma de decisiones racionales y bien informadas también ocurren para servir como sustitutos fiables para miembros de una clase protegida.⁶ Si usted en puridad no completaría una narrativa ROS que declarara: “La transacción era sospechosa, ya que la llevó a cabo una mujer afroamericana”, entonces el algoritmo que utiliza un sustituto equivalente de raza también es objetable. Los sustitutos también se pueden usar para enmascarar el comportamiento discriminatorio.
- *Los conjuntos de datos que representan ciertas poblaciones de manera desproporcionada*—Considere un ejemplo de prejuicio explícito: Un gerente de sucursal bancaria dedica una atención desproporcionada en relación con el seguimiento de las actividades de los clientes hispanos y por lo tanto los reportes de operaciones “sospechosas” sistemáticamente son más para los hispanos que para la actividad similar llevada a cabo por los clientes no hispanos, en parte debido a que el gerente se abstiene de someter a otros al mismo grado de escrutinio. Los datos de la operación “sospechosa” de este director de la sucursal se incorporan en algoritmos que dan instrucciones a oficiales de ALD sobre dónde enfocar su atención, lo que aumenta aún más el escrutinio desproporcionado a clientes hispanos. La sobrerrepresentación en un conjunto de datos también puede

conducir a resultados adversos desproporcionadamente altos para los miembros de las clases protegidas.⁷

- *Los conjuntos de datos que carecen de información*—El acceso a los servicios financieros varía considerablemente debido a las barreras económicas, lingüísticas, estructurales o socioeconómicas. Esta falla sistemática puede reforzar tendencias a la discriminación por sobrerrepresentar algunas poblaciones y subrepresentar otras. Consideremos dos ejemplos, los “no bancarizados” y las tarjetas de identidad. La Federal Deposit Insurance Corporation encontró que el 17,9 por ciento de los hogares hispanos no tenían una cuenta en una institución financiera depositaria asegurada en 2013.⁸ Los hogares sin cuentas bancarias se basan en otros medios, como tarjetas prepagas de débito y dinero en efectivo, para realizar transacciones financieras. Del mismo modo, el 25 por ciento de los adultos afroamericanos no tienen una identificación actualizada con foto emitida por el gobierno.⁹ Como resultado, los algoritmos pueden sobre alertar potencialmente las transacciones con tarjetas de prepago para los clientes hispanos y los cajeros presentarían desproporcionadamente ROS en las tarjetas de ID “sospechosas” para los afroamericanos.
- *Los sistemas de toma de decisiones que asumen que una correlación implica necesariamente causalidad*—Si alguna vez ha usado la misma remera de la suerte para todos los eventos deportivos de su equipo favorito porque cuando se la pone gana, está familiarizado con la correlación frente a la causación. La remera claramente no fue la causa de que su equipo ganara, pero el equipo puede ganar con frecuencia cuando usted la usa. Del mismo modo, el código postal residencial de un

cliente (que a menudo sirve como un sustituto de raza) no provocará que el cliente participe en el fraude hipotecario.

La FinCEN no tiene en cuenta la raza—¿Debería hacerlo?

Se han encontrado conjuntos de datos de agencias de control legal que coherentemente tienen disparidades raciales en las operaciones de narcotráfico y las tasas de detención.^{10,11} Además, se encontró que un algoritmo muy utilizado de la libertad condicional y condena sobre-predecía rutinariamente la tasa a la cual los afro-americanos reincidirían y sub-predecía la tasa a la que los delincuentes blancos reincidirían.¹² Si un error similar fuera hecho por un algoritmo de ALD, resultaría en alertas de falsos positivos excesivos para los afroamericanos y produciría falsos negativos errantes para los blancos.

FinCEN ofrece a las agencias de control legal federales, estatales, locales e internacionales el acceso a los registros de la Ley de Secreto Bancario (BSA) incluyendo los ROS y los reportes de transacciones en efectivo (CTR). FinCEN ha recibido más de 1,8 millones de ROS nombrando clientes e individuos en 2015 y cuenta con más de 190 millones de registros de la BSA.^{13,14} FinCEN hace que los datos de la BSA estén a disposición de más de 9.000 agencias de control legal y los reguladores que realizan más de 30.000 búsquedas cada día.¹⁵

De acuerdo con la FinCEN, los “registros de la BSA proporcionan pistas importantes y claves para los investigadores”. A pesar de la dependencia de las agencias de control legal de los datos de FinCEN, la agencia nunca ha realizado un estudio sobre si el prejuicio se produce dentro de los documentos ROS presentados ni se ha llevado a cabo el análisis

⁶ Solon Barocas and Andrew D. Selbst, “Big Data’s Disparate Impact,” *California Law Review*, Vol. 104, 2016, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

⁷ Ibid.

⁸ “2013 FDIC National Survey of Unbanked and Underbanked Households,” Federal Deposit Insurance Corporation, page 5, octubre de 2014, <https://www.fdic.gov/householdsurvey/2013report.pdf>

⁹ Keesha Gaskins and Sundeep Iyer, “The Challenge of Obtaining Voter Identification,” Brennan Center for Justice, 18 de julio del 2012, <http://www.brennancenter.org/publication/challenge-obtaining-voter-identification>

¹⁰ “Racial Profiling and Traffic Stops,” The U.S. Department of Justice, 10 de enero del 2013, <http://www.nij.gov/topics/law-enforcement/legitimacy/pages/traffic-stops.aspx>

¹¹ Ojmarrh Mitchell and Michael Caudy, “Examining Racial Disparities in Drug Arrests,” *Justice Quarterly*, 22 de enero del 2013, <http://www.tandfonline.com/doi/abs/10.1080/07418825.2012.761721>

¹² Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, “Machine Bias,” *Propublica*, 23 de mayo del 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

¹³ FinCEN SAR Stats for 2015 excluding “Other” and “No Relationship” categories see <https://www.fincen.gov/Reports/SARStats>

¹⁴ Remarks by Jennifer Shasky Calvey, FinCEN Director at Predictive Analytics World for Government, 13 de octubre del 2015, https://www.fincen.gov/news_room/speech/pdf/20151013.pdf

¹⁵ Ibid.

La naturaleza incontestable de los algoritmos de ALD es especialmente importante dada la prohibición legal de revelar si un ROS ha sido presentado o no

de la diversidad racial, demografía religiosa o étnica de los sujetos de ROS.¹⁶ FinCEN también emplea algoritmos para “monitorear presentaciones [de BSA] sobre una base diaria e identificar los informes que merecen una revisión adicional por parte de los analistas”.¹⁷ Se necesita investigar para determinar el impacto potencial del prejuicio en los documentos ROS presentados y en los algoritmos utilizados por la FinCEN misma.

Cathy O’Neil, autora de *Weapons of Math Destruction*, señaló que los modelos que se utilizan hoy en día son opacos, no regulados, e incontestables, incluso cuando se equivocan.¹⁸ La naturaleza incontestable de los algoritmos de ALD es especialmente importante dada la prohibición legal de revelar si un ROS ha sido presentado o no. Un sujeto de ROS no tiene manera de saber si se le ha marcado debido a un algoritmo perjudicado y el individuo no tiene ningún recurso para apartarse de cualquier base de datos de la FinCEN.

El reporte de la Casa Blanca señaló que si las técnicas de grandes datos “no se aplican con cuidado, también pueden perpetuar, exacerbar o enmascarar la discriminación perjudicial”.¹⁹ Por otra parte, el informe de la Casa Blanca indicó que la nueva tecnología debe mejorar la confianza y la seguridad pública

“por medio de medidas que promuevan la transparencia y la rendición de cuentas y mitiguen los riesgos de disparidades en el tratamiento y los resultados basados en las características individuales”.²⁰ FinCEN involuntariamente puede desempeñar un papel perpetuando las desigualdades sociales mediante el almacenamiento y diseminación de datos de BSA sin determinando si la parcialidad existe dentro de los datos.

Avanzando

El primer paso de una institución financiera para eliminar el prejuicio en ALD y los reportes e informes de análisis es reconocer que la tecnología y los algoritmos fueron creados por humanos e incorporan prejuicios humanos con respecto a raza, sexo y religión. Sorelle Friedler, profesora de ciencias informáticas en la Universidad de Haverford, declaró: “Si no se está deliberadamente tratando de identificarlo y corregirlo, este prejuicio probablemente aparecerá en sus resultados”.²¹

El reporte de la Casa Blanca ofreció las siguientes sugerencias con el fin de evitar la toma de decisiones basada en datos de la reincorporación de los patrones de prejuicio:

- Auditar y evaluar conjuntos de datos y algoritmos para efectos potencialmente discriminatorios
 - Revisar la forma de recopilación de datos, los procesos de aprendizaje de máquinas y los materiales de formación y definiciones de categorías que podrían introducir—hasta inadvertidamente—elementos de prejuicio²²
- Además, las instituciones financieras deben:
- Comparar las referencias sospechosas para transacciones cara a cara frente a alertas de transacciones automatizadas
 - Comparar los documentos presentados obligatoriamente tales como CTR a las presentaciones discrecionales
 - Determinar si los problemas estructurales (por ejemplo, la falta de identificación con foto) está contribuyendo a la sobre-representación de ciertos grupos

Las instituciones financieras y los reguladores financieros deben tomar medidas que ahora incluyan el análisis de los datos de entrada y de formación, la revisión de las reglas de decisión de algoritmo, y resultados algorítmicos de auditoría para asegurar que la exactitud, la transparencia y la equidad también están integradas dentro de los algoritmos de ALD. **▲**

Alison Jiménez, CAMS, presidenta, Dynamic Securities Analytics, Inc., Tampa, FL, EE.UU., ajimenez@securitiesanalytics.com

¹⁶ Carta de FinCEN del 13 de mayo del 2016 en respuesta a la Freedom of Information Act Request de Dynamic Securities Analytics, Inc., <http://securitiesanalytics.com/wp-content/uploads/2016/08/2016-482-Jimenez-FOIA-Response-Letter-1.pdf>

¹⁷ Comentarios de Jennifer Shasky Calvery, FinCEN Director at Predictive Analytics World for Government, 13 de octubre del 2015, https://www.fincen.gov/news_room/speech/pdf/20151013.pdf

¹⁸ Cathy O’Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, (Crown: 2016), 18.

¹⁹ “Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights,” Executive Office of the President, mayo de 2016, https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

²⁰ *Ibid.*

²¹ David Ingold and Spencer Soper, “Amazon Doesn’t Consider the Race of its Customers. Should it?,” Bloomberg Businessweek, 21 de abril del 2016, <http://www.bloomberg.com/graphics/2016-amazon-same-day/>

²² Emily Shaw, “Avoiding prejudice in data-based decisions,” Sunlight Foundation, 31 de julio del 2015, <https://sunlightfoundation.com/blog/2015/07/31/avoiding-prejudice-in-data-based-decisions/>

El ALD y los préstamos:

La construcción de la concientización mediante la asociación

El crédito comercial es lo más a menudo la piedra angular de la rentabilidad de una organización. La presión de los prestamistas comerciales consiste en lograr metas agresivas que por lo general vienen con programas de bonos lucrativos para cumplir o superar las expectativas. El logro de un equilibrio entre el crecimiento, la calidad del crédito y el beneficio, al tiempo que mitiga el riesgo de antilavado de dinero (ALD), es un reto que la mayoría de las instituciones, independientemente de la magnitud de los activos, siguen enfrentando.

Los prestadores comerciales están capacitados para mitigar el riesgo de crédito; sin embargo, el enfoque predominante de un prestador es más a menudo encontrar una razón para hacer un negocio más que una razón para no hacerlo. El riesgo de ALD es a veces una idea de último momento o una casilla de verificación. Los prestadores sienten a menudo una falsa sensación de seguridad porque existe una red de control de seguridad de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) incrustada en su programa de cumplimiento y personal. Las acciones recientes y un número creciente de los hallazgos del examen son la identificación de lagunas en el proceso de riesgo de la empresa y la comunicación entre el personal de préstamo y el del ALD.

Una organización que fomenta una fuerte relación y colaboración entre los empleados de ALD y la función de los préstamos es una que verá el beneficio tangible más allá de los programas sanos de cumplimiento de BSA/ALD, y es probable que veamos una mayor

conciencia y conocimiento de los sectores empresariales de sus clientes y la mejora del riesgo de crédito.

Los números

A pesar de una mayor conciencia sobre el lavado de dinero y el riesgo de fraude en los préstamos comerciales, los números de reportes de operaciones sospechosas siguen siendo bajos.

Las estadísticas de reportes de operaciones sospechosas (ROS) de la Red Contra los Delitos Financieros de octubre de 2015 muestra que el fraude de créditos de consumo está clasificado número 12 por tipo de operación sospechosa, el fraude de hipoteca ocupa el número 20, el fraude de modificación de préstamo ocupa el número 46, y el fraude de préstamo de negocios el puesto número 49.

Los créditos comerciales tienen menos exigencias regulatorias y controles y equilibrios que provocan un incremento en la comprensión de los desafíos de actividad anticipada de una empresa, la estructura de propiedad y de explotación del negocio y las necesidades del negocio de financiación más allá del capital “de trabajo”.

Las organizaciones a menudo identifican el fraude de préstamo u operación sospechosa cuando se produce una pérdida. Un enfoque proactivo impide no sólo un riesgo de ALD, sino un riesgo crediticio también. La supervisión proactiva desde el principio necesita identificación en la fase de aplicación y de asegurar el proceso crediticio.

Al abrir las líneas de comunicación, ambas áreas funcionales deben primero entender que pueden no estar hablando el mismo idioma y que las designaciones de calificación de riesgo no son iguales. Los profesionales de ALD tratan a menudo con las denominaciones altas, medias y bajas y los profesionales de ALD que pueden traducir la identificación de riesgos a métricas utilizadas fácilmente en los préstamos a menudo pueden encontrar un camino más fácil para lograr la debida diligencia del cliente (DDC) y la gestión continua del riesgo de ALD.

Cerrar la brecha: El entrenamiento y la educación

La creatividad en el entrenamiento no sólo puede mejorar las relaciones a través de las áreas funcionales, sino que puede promover la retroalimentación constructiva que tanto los prestadores y profesionales de ALD pueden utilizar para romper los silos. Anne Archer, agente/gerente de BSA/ALD del Xenith Bank dijo: “Poco a poco, después de llegar a los prestamistas un par de veces para proporcionar entrenamiento y compartir nuestra perspectiva de riesgo, comenzaron a venir a nosotros con preguntas. Las victorias para nuestro banco fueron la confianza y una mejor comunicación”.

Antes de abordar el entrenamiento, los profesionales de ALD necesitan tener sus casas en orden con el fin de garantizar que ellos mismos entienden el riesgo que suponen los préstamos al programa de cumplimiento de BSA/ALD. También necesitan tener un proceso de

DDC sólido en su lugar. El grupo de cumplimiento debe averiguar cómo afectan las relaciones de préstamo el perfil de riesgo global del cliente y luego llegar a una comprensión de los riesgos de BSA/ALD en toda la cartera de crédito. La lectura de actas del comité de crédito y los informes de seguimiento del préstamo podrían ser útiles en esta tarea. Al principio de la relación de préstamo, considere qué información debe recogerse más allá de la CIP para ayudar a calibrar el riesgo. Los elementos por considerar incluyen el propósito del préstamo, la fuente de los fondos para préstamos de efectivo asegurados, las noticias negativas, la información de crédito y las finanzas en el principal de los préstamos. La buena noticia es que los prestadores probablemente ya reúnen alguna de esta información en sus procesos de incorporación y si no tienen la información, obtenerla sólo puede servir para reforzar la reducción del riesgo de crédito y de suscripción.

Una vez que se han hecho los préstamos, piense en los datos que serán necesarios para mantenerse al tanto de los riesgos que suponen los préstamos. Tenga en cuenta cosas como el número de préstamos de un cliente—mientras más préstamos tenga un cliente, mayor riesgo plantea. Decida qué otros tipos de elementos se necesitan para mantener una comprensión del riesgo, incluyendo, pero no limitándose a, los saldos de préstamos tempranos, las fuentes de fondos para los primeros pagos y la cartera vencida. ¿Es la condición financiera de la empresa la creación de un ambiente propicio para el fraude? Además, ¿alguno de sus pagos de préstamos está realizado por un tercero? Si es así, ¿por qué?

Con una comprensión del riesgo que presentan los préstamos en su institución y un programa de DDC establecido, puede convertir su enfoque a la formación de los prestadores sobre cómo identificar operaciones sospechosas. Si bien hay algunos indicadores evidentes de operaciones sospechosas, como tasaciones fraudulentas, hay otras pistas menos sutiles. Por ejemplo, mire las relaciones con los clientes desde una perspectiva holística. A veces la cuenta de explotación de su cliente o línea de crédito puede ofrecer información. Si se empiezan a ver transacciones grandes inusuales o transferencias o depósitos y retiros de estas cuentas, esto puede ser el reflejo de un cambio o tensión en el negocio, lo que puede apuntar a cualquier operación sospechosa. También, como se ha hecho alusión anteriormente, puede valer la pena investigar los saldos de préstamos inesperados. Otras señales de alerta pueden incluir no ser capaz de obtener datos financieros actualizados u otro tipo de información solicitada a su cliente y la información falsa proporcionada por el cliente. Si sus prestadores le están dando

retroalimentación que el cliente potencial está demasiado ansioso de dejar su relación actual de préstamo debido a “demasiadas preguntas sobre sus negocios”, esto también puede ser una señal de alerta.

Los métodos y formatos de entrenamiento pueden variar, pero usted tendrá más éxito si utiliza más de un canal para entregar su mensaje. Tenga en cuenta que usted y sus colegas de préstamos trabajan para la misma empresa y que son socios. Muestre a los oficiales de crédito que se entrenan que puede potencialmente ayudarlos a que sirvan mejor o entiendan a sus clientes por medio de la información de diligencia debida que proporcione. Asegúrese de que los oficiales de crédito entiendan que no quiere ser un obstáculo en la toma de préstamos y que como profesional de ALD puede mejorar su conocimiento de la empresa de los clientes y también ofrecer información sobre líneas de riesgo de negocio inherentemente superiores. En última instancia, hablar su idioma y explicar los riesgos en sus términos puede dar lugar a asociaciones exitosas.

Sea creativo con su entrenamiento. Si bien una presentación de PowerPoint puede ser apropiada en algunos casos, piense en formatos de capacitación que impulsen el intercambio de ideas. Considere invitar a los oficiales de crédito a las reuniones del comité de BSA en que se discute sobre los clientes. Los agentes de BSA/ALD a su vez podrían asistir a la función de préstamo o las reuniones del comité.

Cerrar la brecha: Comunicación

Del mismo modo que el entrenamiento es fundamental para cerrar la brecha entre las líneas de negocio, lo es también la comunicación. Una vez que los oficiales de crédito entienden lo que son las alertas rojas de operaciones sospechosas, pueden reportar de inmediato a sus socios de ALD para investigación o divulgación de ROS. A los profesionales de ALD también se les puede llegar a educar sobre los problemas de crédito que afectan a su negocio por medio de la comunicación con los oficiales de crédito.

Las funciones de ALD que vienen de un “no” con frecuencia cortan la comunicación antes de que la línea esté abierta. Tener una conversación de riesgo en la que ambas partes tienen la oportunidad de hacer preguntas y compartir puntos de vista es el resultado ideal. Para lograr este resultado, sea respetuoso de los objetivos de negocios de cada uno y esté abierto a diferentes formas de comunicación. Por ejemplo, si su institución requiere el uso de formularios de referencia ROS para comunicar las operaciones potencialmente

sospechosas, pero un profesional de préstamo le envía un correo electrónico o le da una llamada en su lugar, considere esto como un éxito de comunicación y documéntelo usted mismo en el formulario requerido. Lo que usted quiere que se sepa es que está disponible para consultas.

Además, los profesionales de ALD que necesitan elementos de diligencia debida necesarios deben considerar acercarse a los prestadores con esta solicitud y no al cliente. Los prestadores, después de todo, tienen la relación con el cliente. Utilice su necesidad de información como una oportunidad para interactuar con el oficial de crédito, de modo de construir su relación con esta línea de negocio. Si usted explica por qué necesita cierta documentación, les da a los prestamistas un contexto y les da poder para ser experto con su cliente.

Cuando los prestadores se asocian con los profesionales de ALD para bancarizar un nuevo cliente comercial o línea de negocio, cada lado a menudo comparte el punto de vista de que el otro no puede haber sido consciente. Cuando se produce la colaboración de funciones cruzadas, las dos partes seguramente no se encuentran tan distantes entre sí como se podría pensar. Los prestadores no quieren ver que un banco asuma un riesgo indebido o fuera de control, y los profesionales de ALD no quieren ver que su organización se pierda una oportunidad de crecimiento.

Conclusión

Las organizaciones que fomentan un ambiente de colaboración multifuncional tienen una oportunidad para mitigar el riesgo, disminuir las pérdidas por fraude, crear eficiencias y en última instancia un impacto en sus ingresos. Los profesionales de ALD deben estar facultados para dar el primer paso en romper los silos. Se puede comenzar con una simple petición a la función de préstamo: “¿Cómo podemos ayudar a aumentar la eficiencia en el proceso de incorporación al cliente?” Una vez que la puerta está abierta, la asociación probablemente progresará rápidamente. **A**

Elaine Yancey, CAMS, examinadora gerente, Banco de la Reserva Federal de Richmond, Richmond, VA, EE.UU., elaine.yancey@rich.frb.org

Amanda Tucker, CAMS, directora de operaciones y riesgo, Old Dominion National Bank, North Garden, VA, EE.UU., atucker@odnbonline.com

NO ECHE LOS

DADOS





En la Conferencia de 2014 sobre la Ley de Secreto Bancario (BSA), la ex Directora de la Red Contra los Delitos Financieros (FinCEN), Jennifer Shasky Calvery, declaró que “bajo las regulaciones existentes, se requiere que un casino desarrolle y mantenga un sólido programa de antilavado de dinero basado en el riesgo... [esto impone] la obligación de identificar y reportar operaciones sospechosas. El cumplimiento de esta obligación depende en gran medida de la capacidad del casino de entender con quién hace negocios. La FinCEN espera que los casinos, al igual que otras instituciones financieras, soliciten información sobre la fuente de los fondos apropiados de acuerdo con un enfoque basado en el riesgo”.¹

Aunque Shasky Calvery pronunció estas palabras hace dos años, los casinos todavía están luchando con la aplicación práctica de sus políticas de conozca a su cliente (KYC). Como muchos dicen, “El diablo está en los detalles”.

¿Tiene la obligación un casino de conocer a cada cliente que entra por sus puertas? La respuesta claramente es “No”. La BSA no requiere que los casinos tengan una política de KYC ni tienen que identificar a cada cliente que juega en su recinto. La BSA, sin embargo, impone ciertos requisitos de mantenimiento de registros y presentación de reportes. Por ejemplo, las transacciones que involucran más de \$10.000 en efectivo desencadenan un mantenimiento de registros y obligación de presentar reportes que exigen a los casinos obtener y verificar el nombre, dirección y número de identificación fiscal del cliente (por ejemplo, el número de la seguridad social).

Impacto del reporte de operaciones sospechosas (ROS)

La dificultad para los casinos surge de su obligación de presentar los ROS. Si bien los casinos probablemente cuentan con políticas y procedimientos para identificar y reportar operaciones sospechosas, muchos están enfocados principalmente en observaciones físicas por parte del personal del casino tales como que un cliente le pregunte a un cajero la cantidad de dinero que puede depositar antes de que se requiera reportar al gobierno. Algunos casinos también generan informes de transacciones periódicas para identificar posibles operaciones sospechosas, tales como juegos mínimos,² estructuración y otras actividades a veces asociadas con el lavado de dinero. Sin embargo, las expectativas de la FinCEN van más allá de las observaciones físicas y reglas de operaciones sospechosas.

La posición de la FinCEN, según lo declarado por Shasky Calvery, es que la obligación de presentar los ROS también requiere que los casinos conozcan a sus clientes. Incluyen indagar y obtener una comprensión del origen de los fondos de sus clientes. La razón es que tener conocimiento del perfil financiero de sus clientes, incluyendo la fuente de los fondos, le permitirá a un casino comprender mejor si su actividad relacionada con el juego es sospechosa. Por ejemplo, ¿cómo consideraría un casino a un cliente si supiera que el cliente se había declarado en quiebra, pero que, en lugar de disminuir su juego, el cliente casi lo duplicaba? Si una mayor investigación también permitía detectar las acciones civiles presentadas contra el cliente alegando que había desviado de manera fraudulenta los fondos de una sociedad que controlaba justo antes de la declaración de quiebra, esto levantaría una alerta roja. Esta información debería cambiar radicalmente la forma en la que el casino considera el aumento de la actividad de juego del cliente.

La expectativa de KYC de FinCEN no es nueva. Durante años, los bancos han creado perfiles de clientes que comparan con la actividad de cuenta. Cuando la actividad se encuentra fuera del rango esperado por la unidad de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) del banco ésta normalmente inicia una investigación para determinar si la actividad es sospechosa. Aunque no existe una norma que obligue a un casino a tener un programa de KYC, hacer caso omiso de las expectativas de la FinCEN sería imprudente.

Tomando un enfoque basado en el riesgo

Afortunadamente, la FinCEN no les está requiriendo a los casinos realizar un KYC de cada cliente. La expectativa es que un casino debería adoptar un enfoque basado en el riesgo. En concreto, los procedimientos de KYC deben aplicarse a los clientes de riesgo

¹ Jennifer Shasky Calvery, Bank Secrecy Act Conference Remarks, FinCEN, 12 de junio del 2014, https://www.fincen.gov/news_room/speech/html/20140612.html

² El juego mínimo incluye la actividad por medio de la cual un cliente lleva a cabo transacciones mayores que incluyen la compra de fichas o insertan billetes en una máquina pero apenas juega o no juega. En vez, redime los créditos de las tragamonedas por efectivo y/o se va del casino con fichas (a lo que a veces se le dice “fichas caminantes”).

alto. Estos son los clientes que juegan en niveles significativos, por lo general en el límite alto o en salas de juego privadas.

La evaluación del riesgo puede ayudar a identificar clientes de riesgo alto, ya que también será evaluar el riesgo asociado a los productos, zonas geográficas y otros factores. Téngase en cuenta que no se trata de un riesgo general, sino específico. En consecuencia, el mismo cliente puede plantear un riesgo elevado para un casino y un riesgo bajo para otro. Con todos los demás factores iguales, la participación del mismo cliente en la misma actividad en dos casinos diferentes sólo dará lugar a la presentación de un solo ROS. Esto es posible debido a la aplicación de un enfoque basado en el riesgo en lugar de un criterio rígido que obliga a que un KYC se va a realizar.

La ventaja para los casinos en virtud de este sistema es que determinan por propia cuenta quiénes son sus clientes de riesgo alto y cuándo se llevará a cabo un KYC. Mientras la metodología o criterio para la selección de los clientes de riesgo alto resulta razonable, debe cumplir con las expectativas del regulador.

Estableciendo una política de KYC

El objetivo principal de una política de KYC es permitirle a una entidad financiera comprender el riesgo general de BSA/ALD que un cliente y sus actividades transaccionales representan para la institución. La clave para identificar la actividad del cliente sospechoso es primero saber algo sobre ellos. Cuanto mayor sea el riesgo, más diligencia debida resulta necesaria para tomar decisiones informadas. Sin embargo, la difícil pregunta es: ¿Cómo determina un casino cuál de sus clientes es de riesgo alto? Los siguientes factores deben considerarse:

- **Poblaciones de jugadores de Platino, Oro y Diamante:** Se comienza por revisar la lista de jugadores del club, que por lo general clasifica a los clientes en diferentes niveles. Los que juegan al más alto nivel por lo general se ponen en platino, oro, diamante o algún otro término descriptivo. Los clientes de estos niveles altos del club son los que juegan una cantidad significativa de dólares y potencialmente son del mayor riesgo. Aunque sería fácil clasificar todos los clientes en los

niveles superiores del club como jugadores de riesgo alto, puede no tener sentido. Algunos clientes pueden tener un alto estatus del club basados en su juego desde muchos años antes. Usar la población de “jugador alto del club” puede ser el comienzo, pero no es la solución completa.

- **Clientes sin tarjeta de jugador:** Por muchas razones, algunos clientes prefieren jugar sin una tarjeta de jugador. Este hecho por sí solo no aumenta necesariamente la sospecha, pero un casino debe reconocer que algunos clientes que juegan sin tarjeta de jugador pueden plantear un riesgo elevado. En consecuencia, deben adoptarse métodos para identificar a los clientes de riesgo alto que están fuera de la población de jugador con tarjeta. Por ejemplo, ¿hay clientes con un número alto y la cantidad del premio gordo (jackpot, en inglés) sin registro de transacciones con la caja (aparte de procesar el Formulario W-2G) y no utilizan una tarjeta de jugador? Si bien su uso no es obligatorio, un cliente que juega a niveles altos que no participa en el programa puede merecer una mirada más detallada.
- **Las solicitudes de aplicación de la ley (citaciones):** Un área sensible surge cuando los agentes de control legal hacen preguntas sobre un cliente o presentan una orden judicial para conseguir los registros. Es probable que esto requiera cierto nivel de diligencia debida. Aunque no es concluyente, sería conveniente colocar al cliente en la categoría de riesgo alto.

Como se señaló anteriormente, los umbrales deben aplicarse en todos los conjuntos de datos relevantes mantenidos por un casino. ¿Deberían someterse a los clientes con dinero en efectivo de entrada/salida, apuestas, o premios de \$1 millón o más a la diligencia debida mejorada (EDD)?³ ¿El umbral debería ser \$500.000 o \$5 millones? Estas son preguntas difíciles sobre las que no se han publicado directrices reguladoras. En consecuencia, los casinos tienen que documentar completamente las razones y los fundamentos de cómo seleccionan sus poblaciones de riesgo alto para la EDD. Siempre y cuando sea razonable,



los reguladores probablemente sólo se centrarán en si los criterios de selección se siguen coherentemente.

Los umbrales de riesgo alto: ¿Usted ha pensado en lo que el IRS ya sabe?

Al aplicar los umbrales a varios puntos de datos para identificar a los clientes de riesgo alto, los casinos también deben tomar en consideración lo que el IRS ya sabe acerca de sus operaciones de juego en base a los documentos presentados de informes de transacciones en efectivo (CTR), los Formularios 8300, los ROS y Formularios W-2G. El IRS generalmente revisa lo que abajo se señala para decidir donde existen debilidades potenciales en el programa del casino:

- ROS: Las presentaciones de ROS ¿identifican tendencias o patrones que identifican asuntos particulares?
- CTR (efectivo entrante): ¿Se pueden identificar clientes de riesgo alto mediante los billetes insertados en la máquina o en los juegos de mesa?
- CTR (efectivo saliente): ¿Pueden los clientes de riesgo alto identificarse mediante reembolsos de vales entrantes/salientes y fichas u otros instrumentos, tales como cheques, tarjetas de crédito/débito o transferencias electrónicas?
- Formulario W-2G: ¿Hay anomalías en las ganancias del premio gordo de las tragamonedas que identifican a los clientes de riesgo alto?

El IRS también puede hacer una comparación de las solicitudes de CTR presentadas a los Formularios W-2G presentados. En concreto, pocas o ningunas presentaciones de CTR de

³ La diferencia entre CDD y EDD consiste en que en la CDD el casino podría tener información sobre el cliente (por ejemplo, marcador/aplicación de crédito), pero que cuando su actividad de juego u otra lo ubica en la categoría de riesgo alto de EDD, se le requiere cumplir con obligaciones de ROS.

clientes en comparación con su alto volumen de ganancias de Formulario W-2G pueden indicar juegos sin tarjetas. Si el IRS nota esta especie de brecha, se le puede pedir al casino información (es decir, KYC) sobre el cliente. De acuerdo con ello, realizar un análisis del ROS, CTR y W-2G del casino sería un paso prudente antes de que el IRS llame a la puerta.

Tengo mi población de clientes de riesgo alto, ¿ahora qué?

A pesar de que los casinos no tienen la misma información sobre el cliente a disposición como los bancos, por lo general tienen una gran cantidad de información a su disposición dentro de sus sistemas internos. Estos incluyen:

- **Los programas de tarjetas de jugador:** Los clientes que se anotan en estos programas suelen hacerlo proporcionando una credencial emitida por el gobierno (por ejemplo, licencia de conducir) que contiene, como mínimo, su nombre, dirección y fecha de nacimiento. El casino es entonces capaz de realizar un seguimiento de toda su actividad de juego y transaccional (por ejemplo, las máquinas tragamonedas, las transacciones de la caja, compras del restaurante). La información proporciona a los casinos la oportunidad de comprender mejor la actividad de sus principales clientes.
- **Departamento de gestión de crédito:** Este departamento es una valiosa fuente de información financiera. Por lo general se encarga de la contabilidad de las cuentas de dinero, marcadores y otras extensiones de crédito. Los registros incluyen generalmente las solicitudes de crédito, informes de crédito y otros registros financieros relacionados con el empleo y afiliaciones de negocios. Estas fuentes podrían proporcionar información crítica relativa a la fuente de los fondos de los clientes.
- **Caja:** Operando como el banco del casino, los empleados en la caja por lo general tienen la interacción del día a día con los clientes. Si bien no se espera que los empleados recuerden las transacciones de todos los clientes, los ubicados en habitaciones de límite alto por lo general tienen una relación más estrecha con los clientes.
- **Departamento de marketing:** El departamento de marketing por lo general lleva a cabo investigaciones sobre los clientes para encontrar maneras de maximizar su juego en el casino. Utilizan la información en sus esfuerzos de marketing para atraer, entre otros, los jugadores altos de su

casino. Además, las anfitrionas ejecutivas asignadas a determinados jugadores grandes obtienen una gran cantidad de información de sus conversaciones con estos clientes. Sin embargo, no es extraño que los clientes exageren, induzcan a error o les mientan a las anfitrionas ejecutivas. En consecuencia, aunque esta información es útil, no es un sustituto de la diligencia debida prudente independiente en la determinación de las fuentes de fondos.

Para complementar los controles de antecedentes internos, debe llevarse a cabo una investigación externa. Esto incluiría, entre otras fuentes:

- **Bases de datos comerciales:** Ampliamente disponibles, proporcionan servicios de noticias y de localización de activos de búsqueda. La información del cliente se puede obtener en relación con los artículos periodísticos, documentos de la corte, acciones delictivas, declaraciones de quiebra, afiliaciones de negocios, documentos de propiedad e información relacionada. Si bien el acceso a estas bases de datos comerciales no es libre, su utilidad es mucho mayor que los costos.
- **Investigación en internet:** Una variedad de motores de búsqueda (por ejemplo, Google y Yahoo) están disponibles de forma gratuita. Mediante esta investigación, la información del cliente puede ser obtenida de los medios sociales y sitios web de redes profesionales que pueden no estar en las bases de datos comerciales.
- **Intercambio de información 314(b):** La FinCEN ha animado a los casinos a participar en el programa de intercambio de información 314(b). Bajo este programa, un casino puede solicitar información de otro casino participante u otra institución financiera relativa a un posible lavado de dinero o financiación del terrorismo.

¿El perfil financiero del cliente se encuentra acorde con la actividad de casino?

La respuesta a esta pregunta se reduce al análisis, el juicio y la aplicación de políticas. En los extremos, puede haber situaciones en las que el cliente vive en un apartamento de vivienda de interés social sin empleo o sin activos identificados, pero tiene un largo prontuario relacionado con narcóticos y juega, por año, al nivel de \$1 millón. En el otro extremo, un casino puede tener un ejecutivo de una empresa pública con un sueldo anual

de \$10 millones que juega \$100.000 anualmente. Es evidente que uno de los escenarios levanta sospechas mientras que el otro no.

La dificultad es todo lo que queda en el medio. Si el cliente no tiene una fuente identificable de fondos, pero tiene 70 años, ¿en qué nivel de juego se levantaría una alerta roja? Suponiendo que el cliente está apostando \$300.000 en dinero nuevo (a diferencia de ganancias recicladas) por año, ¿se debe presentar un ROS de “sospecha de origen de fondos?” ¿Cuál es el umbral de apuestas (por ejemplo, \$100.000, \$500.000, \$1 millón) que crearía potencialmente sospechas? ¿Se debería considerar la edad del cliente desde el punto de vista de que él/ella probablemente esté jubilado y usa una pensión u otros fondos de retiro para jugar? Si el cliente tiene 35 años ¿haría una diferencia?

Estas son las decisiones de política de investigación que un casino debe formular por adelantado con el fin de asegurar una aplicación coherente por parte de los investigadores del personal. Una línea brillante no se puede aplicar universalmente como regla porque la política debe basarse en el riesgo y dependerá de cada conjunto particular de las circunstancias de cada casino, incluyendo su apetito de riesgo. Bajo un enfoque basado en el riesgo, lo que es importante es que las políticas y procedimientos sean claros para garantizar las decisiones de presentación coherente de un ROS o no-ROS. Esto incluye tener fundamentos razonables de los umbrales para determinar qué actividad se considera potencialmente sospechosa. El desarrollo de la evaluación del riesgo es pro-



CONOZCA A SU CLIENTE

bablemente el mejor momento para evaluar los umbrales que se incorporarán en las políticas y procedimientos de KYC/ROS.

Las medidas reglamentarias en materia de operaciones sospechosas y presentaciones de ROS se han centrado en los extremos. Las sanciones han sido reivindicadas debido a no presentar un ROS en los casos en que las circunstancias indican claramente que el cliente tenía una fuente ilícita de fondos (por ejemplo, el narcotráfico). Si bien en situaciones como las descritas anteriormente, con los de 35 y 70 años de edad, los clientes no han sido el foco de las acciones de aplicación, de todos modos requieren juicio y análisis cuidadosos.

El cliente de riesgo alto es un extranjero, ahora ¿qué debo hacer?

La aplicación de la debida diligencia a los clientes con sede en los EE.UU. es bastante fácil, pero ¿qué se hace cuando su cliente de riesgo alto es un extranjero con poca, o ninguna conexión a los EE.UU.? La investigación tradicional por internet y bases de datos comerciales, incluso con algunas empresas que pretenden tener una cobertura mundial, puede proporcionar poca información útil. Los casinos se encuentran con el dilema de enfrentarse a un cliente de riesgo alto con poca información acerca de quiénes son y cuál es su fuente de riqueza. Si después surgiera información adversa en los informes de noticias de que la fuente de los fondos del extranjero era de alguna actividad ilícita, sería difícil de justificar ante la FINCEN que la falta de resultados en “la investigación de los EE.UU.” era suficiente diligencia debida. En estas situaciones de muy alto riesgo, los casinos deben considerar hacer que el cliente rellene un cuestionario, así como aplicar algunos controles de EDD para mitigar el riesgo. El cuestionario debería cubrir las siguientes áreas:

- **País de residencia:** ¿Es el mismo que el del pasaporte? ¿Al país se le considera una jurisdicción de riesgo alto?

- **Ocupación/negocio:** Línea específica de negocio—no sólo un título anodino de “consultor”, “exportador” y/o “hombre de negocios”.
- **Filiales comerciales:** ¿Cuál es su relación con ellos (por ejemplo, propietario, directivo de la empresa)?
- **Los contactos de gobiernos extranjeros:** ¿El cliente es un funcionario de gobierno extranjero? ¿Tiene familiares o asociados cercanos que son funcionarios de gobiernos extranjeros?
- **Documentación:** ¿Tienen alguna documentación para demostrar el empleo, negocio/ propiedad de la empresa, o la propiedad de cuenta bancaria?

Los casinos se encuentran con el dilema de enfrentarse a un cliente de riesgo alto con poca información acerca de quiénes son y cuál es su fuente de riqueza

El aumento de los controles también debería establecerse para asegurar que las transferencias entrantes son de cuentas personales y/o comerciales pertenecientes al cliente. La limitación de las transferencias de salida a la(s) misma(s) cuenta(s) que las entrantes es otro control prudente. La mejora en la vigilancia de la actividad de juego y transaccional del cliente también debe llevarse a cabo para garantizar una actividad que no quede fuera de lo que se esperaba o no indique ninguna alerta roja (por ejemplo, juego mínimo).

Por último, otro paso podría incluir la tercerización de una investigación de antecedentes del cliente. El tipo de recursos y la experiencia necesarios para llevar a cabo una investigación de antecedentes financieros de un extranjero es mejor manejada por empresas especializadas. Esto puede considerarse como una medida extrema, pero cuando un casino toma “clientes de muy alto riesgo” que potencialmente podrían dañarle la reputación, los costos asociados con una medida de este tipo bien valen la pena.

Conclusión de KYC

Las preguntas y escenarios anteriores ponen de relieve la complejidad de cumplir con las expectativas actuales del regulador de KYC. Utilizando un enfoque basado en el riesgo, cada casino debe instituir una política eficaz de KYC con fuertes procedimientos de diligencia debida para entender a sus clientes de riesgo alto. La información para construir perfiles de clientes se puede aprovechar de los departamentos internos y las bases de datos externas para capturar datos relevantes en cuanto a fuentes de riqueza. Esta información les permitirá a los casinos supervisar mejor las operaciones para asegurar que son coherentes con el perfil de cada cliente de riesgo alto. Al tener un programa de BSA/ALD fuerte con una política eficaz de KYC, los casinos pueden ayudar a proteger su reputación y no, sin saberlo, convertirse en un conducto para el lavado de dinero o financiación del terrorismo. Hacer lo contrario potencialmente puede colocarlos en la mira de una acción de cumplimiento regulatorio. Esta es una apuesta que no deben hacer. **▲**

Peter S. Alvarado, oficial de cumplimiento jefe, San Manuel Indian Bingo & Casino, Highland, CA, EE.UU., palvarado@sanmanuel.com

Thomas J. Paramo, gerente senior de cumplimiento, San Manuel Indian Bingo & Casino, Highland, CA, EE.UU., tparamo@sanmanuel.com

NICE · ACTIMIZE

INTEGRATED MANAGEMENT OF THE **END-TO-END** **ANTI-MONEY LAUNDERING LIFE CYCLE**

Consistent monitoring and oversight across systems, data, operations, and lines of business, to help you mitigate risk and protect against breaches of compliance

Transaction
Monitoring
Customer
Due Diligence

Currency
Transaction
Reporting

Watch List
Filtering

FATCA
Compliance



**VISIT OUR BOOTH AT ACAMS TO LEARN
MORE ABOUT OUR AWARD WINNING
AML SOLUTIONS**

La comprensión del riesgo del cliente



En mayo de 2016, la Red Contra los Delitos Financieros (FinCEN), en virtud de la Ley de Secreto Bancario (BSA), emitió reglas firmes que describen los requisitos de debida diligencia del cliente (DDC) para las instituciones financieras tales como bancos regulados a nivel federal, cooperativas de crédito con garantía federal, fondos de inversión, corredores o agentes de valores, corredores de futuros y corredores introductores de productos básicos.¹ Junto con las respuestas del Tesoro a las observaciones formuladas en la notificación anticipada y el aviso de propuesta de reglamentación, las normas establecen estándares mínimos de DDC en toda la industria. Desde hace algún tiempo, mucha discusión se ha centrado en la exigencia largamente esperada de identificar y verificar los beneficiarios efectivos. Los retos organizativos, financieros y el momento de la aplicación del requisito anterior no deben minimizarse. Igualmente arduo es el cumplimiento del mandato de la FinCEN de que las instituciones financieras comprendan los riesgos planteados por sus clientes mediante el desarrollo de perfiles de riesgo del cliente y de que “sean capaces de demostrar esta comprensión”.² Mediante el establecimiento de un marco de gestión de riesgo de clientes, las instituciones financieras pueden tener éxito en la captura efectiva del riesgo del cliente y en la comprensión del riesgo general planteado por sus clientes.

Se puede argumentar que la comprensión de riesgo del cliente se logra a través de mandatos de BSA existentes y las prácticas de la industria, ahora simplemente reunidas bajo el paraguas de la DDC. Estas prácticas incluirían la recopilación de información básica al abrir la cuenta, monitoreo de transacciones y reporte de operaciones sospechosas. Si bien estas prácticas pueden estar vigentes, son

más robustas cuando se establecen, ejecutan y revisan por medio del objetivo de la gestión de riesgo del cliente.

Un marco de gestión de riesgos de clientes incluye una metodología bien elaborada de captar y recoger indicadores de riesgo del cliente, un proceso exhaustivo para evaluar riesgos y un mecanismo para volver a calibrar el riesgo basado en los eventos desencadenantes. Es una herramienta eficaz para registrar, medir y evaluar el riesgo, y para demostrar esta comprensión.

Requisitos de la FinCEN

Además de la identificación y la verificación tanto de los clientes como del beneficiario final, la FinCEN clasifica de manera explícita los dos elementos restantes de la DDC como:

- “La comprensión de la naturaleza y la finalidad de las relaciones con los clientes para desarrollar un perfil de riesgo del cliente, y
- El seguimiento continuo de reportar transacciones sospechosas y—sobre una base de riesgo—el mantenimiento y actualización de la información del cliente”³

Al llevar a cabo el monitoreo de transacciones, las instituciones financieras deberían utilizar el perfil de riesgo del cliente como una línea de base para evaluar si las transacciones son sospechosas. Además, cualquier nueva información descubierta sobre los riesgos relevantes en el transcurso de la supervisión debe dar lugar a una actualización del perfil de riesgo del cliente.

Lo anterior sugiere que las instituciones financieras se involucren activamente en la revisión y evaluación de nuevos datos que podrían mejorar un perfil de riesgo establecido o información de identificación del cliente.

Desafíos

En la ausencia de un sólido marco de gestión de riesgo del cliente, las instituciones financieras se enfrentan a una serie de desafíos. No capturar de manera integral los riesgos de datos relevantes que forman un perfil de riesgo del cliente podría dar lugar a la evaluación de la actividad inusual de forma incorrecta. No tener un mecanismo para evaluar la nueva información puede dejar los perfiles de riesgo estancados. Además, los problemas pueden agravarse en las organizaciones donde la información no se comparte fácilmente. Las prácticas de DDC pueden ser ejecutadas en las unidades de negocio que operan en silos y/o llegan hasta estructuras de organización no relacionadas.

Marco de gestión de riesgo del cliente

Las instituciones financieras deben considerar establecer un marco de gestión de riesgo del cliente para gestionar eficazmente la DDC. Un marco establecido mantendrá los procesos enfocados independientemente de los canales de información. Una vez que el cliente y los beneficiarios han sido identificados y verificados, los siguientes pasos básicos se deben seguir o ajustar en función de la base de clientes:

1. Identificar y registrar datos pertinentes de riesgos
2. Evaluar el riesgo colectivo
3. Definir el enfoque basado en el riesgo
4. Monitorear y evaluar los eventos en función del perfil de riesgo del cliente
5. Actualizar datos de riesgo relevantes
6. Volver a calibrar el riesgo colectivo

¹ “Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions,” FinCEN, 19 de julio del 2016, [https://www.fincen.gov/statutes_regs/guidance/pdf/FAQs_for_CDD_Final_Rule_\(7_15_16\).pdf](https://www.fincen.gov/statutes_regs/guidance/pdf/FAQs_for_CDD_Final_Rule_(7_15_16).pdf)

² “Customer Due Diligence Requirements for Financial Institutions,” FinCEN, 11 de mayo del 2016, <https://www.federalregister.gov/articles/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions>

³ Ibid.

Identificar y registrar los datos de riesgos pertinentes

Debe considerarse cuidadosamente la identificación de los elementos que forman el perfil de riesgo del cliente. La información se recoge típicamente al inicio de la apertura de la cuenta y puede actualizarse a lo largo de la vida de la relación. Los elementos de datos varían en función del tipo de cliente, la base de clientes y la oferta de la institución financiera, entre otros factores. Los indicadores de riesgo se manifiestan en cualquier etapa del ciclo de vida del cliente y durante todo el período de conflicto del interés económico. El esquema del perfil de riesgo debe diseñarse teniendo en cuenta las actualizaciones. Algunos valores, tales como el “tipo de negocio”, justifican la recopilación de información relacionada adicional para revelar exposiciones concebibles. La composición de un perfil de riesgo del cliente se puede formular en torno a lo siguiente:

- **Quién**—La identidad y naturaleza del cliente; el tipo de cliente; la ocupación o tipo de negocio (actual y anterior)—posibles destinatarios de las transferencias; la industria servida
- **Dónde**—Geografías de residencia y ciudadanía; destinos y orígenes de las transferencias; ubicaciones de las transacciones comerciales; regiones de posibles inversiones
- **Qué**—Transacciones esperadas, servicios, productos, divisas; historia de la actividad (si son un cliente existente); los factores de riesgo de la industria/profesión del cliente
- **Por qué**—Objeto de la relación con el cliente y de cada cuenta; objetivo de la actividad esperada
- **Cuánto**—Tamaño de las cuentas, los activos, el patrimonio neto; tamaño de las transacciones esperadas
- **Cuándo**—Tiempo esperado y/o frecuencia de las transacciones, pagos, entregas de productos/servicios

Evalúe el riesgo colectivo

Una vez recopilados los datos, el riesgo planteado por el cliente debe evaluarse. Un elemento de datos único puede tener un nivel de riesgo claro, tal como uno de los tipos de empresas citadas en el manual del Consejo de Exámenes de las Instituciones Financieras Federales. En otros casos, múltiples puntos de datos deben evaluarse en relación con otras variables. Las instituciones pueden con-

siderar crear escalas de riesgo para medir el riesgo colectivo. A pesar de que las reglas no requieren un sistema de calificación de riesgo, este proceso crea una definición coherente de riesgo mediante una unidad de negocio o una institución y elimina las interpretaciones subjetivas de los niveles de riesgo en otros procesos de DDC, como el monitoreo de transacciones.

Defina el enfoque basado en el riesgo

Este paso describe los procesos que se ocuparán de cada nivel de riesgo. Los niveles de detalle de las funciones o tareas posteriores están claramente establecidos. Una de las primeras decisiones que las instituciones deben tomar es si se acepta el riesgo o no. La decisión debería tener en cuenta la capacidad de la institución para asignar los recursos necesarios para gestionar los riesgos planteados.

Posteriormente, un proceso debería existir para definir el nivel de aprobación de gestión necesario en función del nivel de riesgo del perfil. Para el monitoreo de transacciones, ¿los factores de riesgo afectarán los parámetros establecidos y/o las reglas implementadas, o la frecuencia de las revisiones? ¿Qué factores podrían desencadenar una actualización de perfiles de riesgo del cliente, y con qué frecuencia se revisarán los niveles de riesgo del cliente?

Supervisar y evaluar los eventos en función del perfil de riesgo del cliente

Aunque no es un nuevo mandato, el monitoreo de transacciones es el cuarto elemento de la DDC. Desde una perspectiva de riesgo del cliente, este es un proceso crítico para verificar que el riesgo de cliente resulta como queda registrado y evaluado en el inicio de la relación. La actividad inusual detectada mediante el monitoreo de transacciones debe revisarse enfrentándola al perfil de riesgo del cliente para determinar si la actividad es sospechosa o si se necesita información adicional para evaluarla. Las noticias negativas, si son independientes del monitoreo continuo, también deben evaluarse a la luz del perfil de riesgo del cliente. Además, en esta etapa, se identifican nuevos factores de riesgo del cliente.

Actualización de los datos relevantes de riesgo

La FinCEN no impuso un requisito categórico para actualizar información del cliente o del beneficiario real de manera continua. La actualización es necesaria cuando una institución financiera detecta información que pueda tener un impacto en el perfil de riesgo

del cliente, incluyendo la identidad de los beneficiarios. Un catálogo de indicadores de riesgo que pueden desencadenar una actualización del perfil de riesgo del cliente debe estar a disposición de los analistas de vigilancia. Además, las instituciones financieras deben actualizar el perfil de riesgo del cliente basándose en correspondencia con clientes, visitas, informes de llamadas, eventos de mercado, etc. Al reunir información de todas las fuentes para actualizar el perfil de riesgo del cliente, las instituciones financieras se mantendrán al tanto de las exposiciones de los clientes y satisfarán sus necesidades de reportes de BSA con mayor éxito.

El ciclo de gestión de riesgo del cliente continúa durante toda la vida útil de una relación financiera

Recalibre el riesgo colectivo

Un perfil de riesgo actualizado podría tener un nivel de riesgo diferente del que previamente se había establecido. Los cambios en los valores de riesgo activarán las medidas presentadas en el enfoque basado en el riesgo de la institución. El perfil de riesgo de un cliente puede permanecer estable a través del tiempo, pero la gestión de riesgo cliente no debería estancarse.

Conclusión

El ciclo de gestión de riesgo del cliente continúa durante toda la vida útil de una relación financiera. La visión más profunda del riesgo del cliente sólo puede lograrse siguiendo un marco disciplinado de recogida, actualización y recalibración de perfiles de riesgo. La comprensión de la naturaleza y el propósito de las cuentas y el cumplimiento de las normas de DDC se logran con éxito mediante la adhesión metódica a la gestión de riesgo del cliente. **TA**

Rita Gemayel, consultora independiente, Global Compliance Analytics, Inc., Stamford, CT, EE.UU., rgemayel@gmail.com

El león al acecho:

El impacto del Memo de Yates sobre oficiales de cumplimiento y monitoreo

Como oficial de cumplimiento, director de antilavado de dinero (ALD), vicepresidente de esfuerzos antisoborno, o incluso ejecutivo, ¿se encuentra usted preocupado por el Memo Yates del Departamento de Justicia (DOJ)? Si la respuesta es negativa, usted compartiría la opinión de la mayoría. Kroll y el Instituto Ethisphere acaban de completar una encuesta de antisoborno y corrupción, que encontró que sólo el 29 por ciento de los encuestados estaban más preocupados por la responsabilidad personal que en años anteriores.¹ ¿Podría la actitud indiferente hacia el Memo Yates ser potencialmente un error de cálculo muy significativo? Carl Reichel, Dmitriy Harder y Thomas Haider no pudieron ver el león al acecho y sufrieron consecuencias significativas en su falta de previsión.

A lo largo de la historia, se nos ha advertido de ciertos eventos que iban a suceder. Aunque algunas advertencias resultan ser ciertas y otras no, ¿qué nos dirá la historia con el tiempo sobre las directrices esbozadas en el Memo Yates?

En la primera línea de la nota de Yates, se dice: “La lucha contra el fraude corporativo y otra conducta es una de las principales prioridades del Departamento de Justicia”.² Existe clara evidencia que el Departamento

de Justicia, así como la Oficina Federal de Investigaciones (FBI), está tomando esto en serio ya que el número de abogados del Departamento de Justicia que investigan los casos de Prácticas Corruptas en el Extranjero (FCPA por sus siglas en inglés) ha aumentado de 19 a 29 y el FBI también está aumentando el número de agentes especiales que investigan casos de la FCPA y la cleptocracia. Además, el Departamento de Justicia contrató a Hui Chen, un experto a tiempo completo en el cumplimiento, para ayudar al departamento a medir la eficacia real de los programas de cumplimiento.³ El FBI no persigue violaciones civiles de la ley. Los agentes persiguen investigaciones criminales, lo que significa que a las personas involucradas, si se las declara culpables, irán a la cárcel. El Memo Yates refleja este resultado final cuando dice: “Una de las maneras más eficaces para luchar contra la conducta corporativa es mediante la búsqueda de responsabilidad por parte de los individuos que perpetraron el delito”.⁴ Los agentes del Departamento de Justicia y el FBI representan el león al acecho como oficiales de negocios, poco acostumbrados a persecuciones judiciales agresivas en este ámbito, que subestiman o ignoran la amenaza potencial. Por ejemplo, a continuación hay tres casos de funcionarios de negocios que participaron en violaciones penales.

- El 29 de octubre del 2015, la empresa de asistencia sanitaria Warner Chilcott acordó pagar \$125 millones para resolver la responsabilidad penal y acusaciones de documentación falsa.⁵ Normalmente, esto habría sido el final del caso, y la corporación, así como sus ejecutivos, habrían continuado con sus negocios. En lugar de ello, el Departamento de Justicia fue aún más lejos y presentó cargos penales contra cuatro empleados de Warner Chilcott, entre ellos su ex presidente Carl Reichel. Tres empleados de Warner Chilcott posteriormente se declararon culpables de cargos de conspiración criminal y el juicio de Reichel comenzó el 23 de mayo del 2016. El 17 de junio del 2016, Reichel fue absuelto de todos los cargos. Este resultado puede interpretarse en un par de formas dependiendo de la perspectiva. Puede ser que sea prudente considerar a todos ellos al evaluar el estado de sus programas de ALD y anti-soborno. Los expertos legales han sugerido que la absolución puede haber resultado de la decisión del juez de cambiar ciertos términos en las instrucciones del jurado, mientras que otros han sugerido que este tipo de casos resulta difícil de comprobar para el gobierno.⁶ No importa la perspectiva que uno elija, la pregunta es si uno estaría dispuesto a correr ese riesgo.

¹ Stephanie Forshee, “Are Compliance Officers Naïve About the Yates Memo’s Implications?,” *Corporate Counsel*, 9 de marzo del 2016, <http://www.corpcounsel.com/id=1202751837264/Are-Compliance-Officers-Naive-About-the-Yates-Memos-Implications>

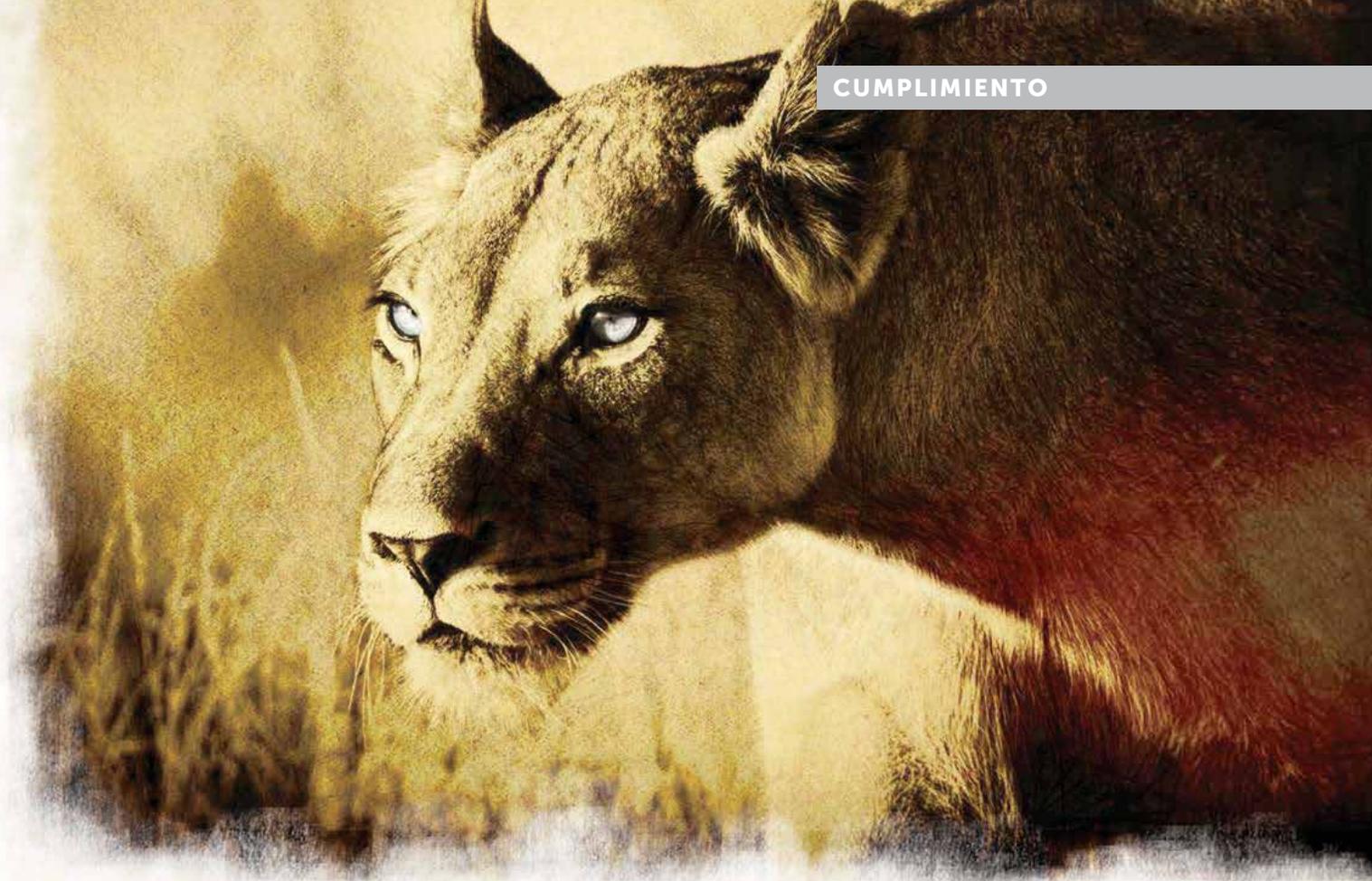
² Sally Quillian Yates, “Individual Accountability for Corporate Wrongdoing,” U.S. Department of Justice, 9 de septiembre del 2015, <https://www.justice.gov/dag/file/769036/download>

³ Ben DiPietro, “DOJ’s Caldwell: Plenty of FCPA Cases in Pipeline,” *Wall Street Journal*, 23 de febrero del 2016, <http://blogs.wsj.com/riskandcompliance/2016/02/23/dojs-caldwell-plenty-of-fcpa-cases-in-pipeline/>

⁴ Sally Quillian Yates, “Individual Accountability for Corporate Wrongdoing,” U.S. Department of Justice, 9 de septiembre del 2015, <https://www.justice.gov/dag/file/769036/download>

⁵ “Warner Chilcott Agrees to Plead Guilty to Felony Health Care Fraud Scheme and Pay \$125 Million to Resolve Criminal Liability and False Claims Act Allegations,” U.S. Department of Justice, 29 de octubre del 2015, <https://www.justice.gov/opa/pr/warner-chilcott-agrees-plead-guilty-felony-health-care-fraud-scheme-and-pay-125-million>

⁶ Samantha P. Kingsbury and Eoin Beirne, “Jury Acquits Former Pharma Exec in One of the First Post-Yates Memo Health Care Fraud Prosecutions,” *Mintz Levin*, 27 de junio del 2016, <https://www.healthlawpolicymatters.com/2016/06/27/jury-acquits-former-warner-chilcott-president-in-one-of-first-prosecutions-of-a-health-care-executive-following-doj-yates-memo/>



- Dmitrij Harder operaba una compañía llamada Chestnut Consulting Group, Inc., que se creó para ayudar a determinados clientes con la financiación del proyecto. En una estafa masiva en la que participó el Banco Europeo de Reconstrucción y Desarrollo (EBRD por sus siglas en inglés), Harder y otros supuestos conspiradores fueron capaces de obtener más de \$8 millones en honorarios, de los cuales cantidades significativas fueron remitidas a un familiar de la persona de EBRD que ayudó a originar el préstamo. El 20 de abril del 2016, Harder se declaró culpable de violaciones penales de la FCPA y fue programado para ser sentenciado el 21 de julio del 2016.⁷
- El 18 de diciembre del 2014, una demanda civil fue presentada contra Thomas Haider que era el principal respon-

sable del cumplimiento de MoneyGram International. En la denuncia, Haider fue acusado de violar la Ley de Secreto Bancario (BSA) y su normativa de desarrollo que implican ciertos esfuerzos de ALD, o la falta de ella, mientras servía en su cargo en MoneyGram International. A Haider se le penó personalmente con una multa civil de \$1 millón.⁸ Con la directiva del Memo Yates, la supuesta actividad de Haider en el entorno actual probablemente conduzca a un proceso penal, además de la multa civil impuesta.

Con las personas que puedan ir a la cárcel por estas violaciones y/o presuntas violaciones, ¿qué nivel de comodidad siente usted con los controles de su organización, así como de su cultura organizacional? En el estudio de Kroll y Ethisphere Institute, el 25 por ciento de los

encuestados no tiene confianza en su estructura vigente de control interno para la anticorrupción.⁹ En un estudio realizado por Dana R. Hermanson, Jason L. Smith y Nathaniel Stephens, corporaciones que cotizan en bolsa y empresas de servicios financieros tenían protocolos de monitoreo más amplios dentro de su estructura de control interno que daba a los empleados más confianza en su capacidad para evaluar con precisión las acciones en el lugar de trabajo.¹⁰ Incluso con esa confianza, PWC encontró que una de cada cinco empresas de servicios financieros ha experimentado las acciones de aplicación por un regulador.¹¹ En 2014, una encuesta de Reuters a altos ejecutivos de banco encontró que el 33 por ciento de ellos cree que su institución cuenta con escasos controles de ALD. En la misma encuesta, sólo el 50 por ciento de los ejecuti-

⁷ "Former Owner and President of Pennsylvania Consulting Companies Pleads Guilty to Bribing Official at European Bank for Reconstruction and Development," U.S. Department of Justice, 20 de abril del 2016, <https://www.justice.gov/opa/pr/former-owner-and-president-pennsylvania-consulting-companies-pleads-guilty-bribing-official>

⁸ Civil Action, U.S. Attorneys' Office, 18 de diciembre del 2014, https://www.fincen.gov/news_room/ea/files/USAO_SDNY_Complaint.pdf

⁹ Stephanie Forshee, "Are Compliance Officers Naïve About the Yates Memo's Implications?," Corporate Counsel, 9 de marzo del 2016, <http://www.corpcounsel.com/id=1202751837264/Are-Compliance-Officers-Nave-About-the-Yates-Memos-Implications>

¹⁰ Dana R. Hermanson, Jason L. Smith, and Nathaniel Stephens, "How Effective Are Organization's Internal Controls? Insights Into Specific Internal Control Elements," Current Issues in Auditing, American Accounting Association, 2012, 6(1), pp. A31-A50, <http://aaapubs.org/doi/pdf/10.2308/ciia-50146>

¹¹ Imran Farooqi, "Money laundering destroys value," PWC, 2016, <http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/anti-money-laundering.html>

vos percibió que los sistemas de control interno eran capaces de proporcionar una imagen completa del potencial de lavado de dinero de dentro de su institución.¹²

El Departamento de Justicia ha reconocido que este tipo de casos puede ser difícil de probar por lo que han incentivado a las organizaciones a cooperar. Sin embargo, con el fin de recibir el crédito para cooperar, los líderes de estas organizaciones deben proporcionar “los datos pertinentes relativos a los individuos involucrados en la supuesta mala conducta”.¹³ Recientemente, Johnson Controls, una empresa de tecnología global e industrial, arregló violaciones de FCPA con el Departamento de Justicia mediante el pago de una multa de \$14 millones. Debido a su amplia cooperación en la materia, Johnson Controls fue capaz de mantener el león al acecho ya que el Departamento de Justicia accedió a cerrar su investigación debido a la amplia cooperación de la compañía en la materia.¹⁴

El tono en la parte superior es esencial para que las grandes organizaciones eviten el león al acecho

Algunas personas argumentarán, especialmente en las grandes organizaciones multinacionales, que es imposible saber todo lo que está sucediendo dentro de una gran organiza-

ción. Sin embargo, el caso de Johnson Controls proporciona un modelo para otras organizaciones. Si los ejecutivos de la organización establecen el tono adecuado y crean una cultura en la que la transparencia se impone, el león puede quedar distante iniciando el contacto y divulgando información negativa al Departamento de Justicia. Habrá algunas organizaciones y ejecutivos que, a pesar de que se les da la información sobre posibles violaciones de la FCPA, tomarán la decisión de tratar de distanciarse de la actividad con la esperanza de que culpen a sus empleados y eviten el procesamiento. Como la persona encargada del cumplimiento, ALD y/o esfuerzos antisoborno, ¿cuál es su nivel de comodidad al saber que podría declarársele culpable de las violaciones? No importa en qué posición se encuentra, probablemente debería familiarizarse con los términos legales “ceguera voluntaria” e “ignorancia deliberada”. Lo que significan estos términos es que nadie puede ser un avestruz y meter la cabeza en la arena. Si se hubiera podido esperar que una persona razonable se encuentre al tanto de los hechos ocurridos, entonces usted es potencialmente responsable de estos actos. El caso Haider es un buen ejemplo de que él no puso fin a las relaciones de MoneyGram con ciertos puntos de venta a pesar de que habían sido identificados como incurriendo en prácticas fraudulentas.¹⁵ El desconocimiento no es una defensa legal confiable. Si bien puede funcionar en algunas ocasiones, los abogados y los juicios penales son caros. Incluso si ganara, usted habría gastado una cantidad significativa de dinero en honorarios legales. Si se perdiera el caso, entonces no sólo habrá gastado una fortuna, sino también es probable que vaya a la cárcel por un período de tiempo.

El tono en la parte superior es esencial para que las grandes organizaciones eviten el león al acecho. En el mismo estudio realizado por Hermanson, Smith y Stephens, el control

interno de menor potencia, con mucho, fue una evaluación periódica del tono en la parte superior.¹⁶ Si te detienes a pensar en las implicaciones de la afirmación anterior, se puede entender por qué el Memo Yates tiene el potencial de impactar las organizaciones de una manera muy significativa. Los estudios han demostrado que el comportamiento y las emociones del líder son contagiosos. Si un líder no muestra su preocupación por el riesgo y la estructura o el control interno global de una organización, es probable que los seguidores de la organización imiten el comportamiento. Esta falta de interés se verá reforzada si el consejo de administración y/o comité de auditoría no participan activamente en el tono en la evaluación de la parte superior como lo demuestra el estudio Hermanson, Smith y Stephens.¹⁷

El Departamento de Justicia y el FBI han advertido a todos que el pasado ya no refleja el futuro. ¿Si realizara una autoevaluación de los controles en su organización, usted estaría satisfecho o asustado? Si evaluara el liderazgo en su organización, ¿estaría seguro de que tomaría la responsabilidad de violaciones o rápidamente culparía a la gente a cargo del cumplimiento? ¿Es el riesgo en su organización acorde con la recompensa? Si bien puede ser fácil de responder a estas preguntas acerca de su organización a medida que lee este artículo, ¿llegaría a las mismas conclusiones si estas preguntas se plantearan durante un juicio penal, donde sus acciones, o falta de ellas, decidieran si lo encarcelan o no? **A**

Michael Bret Hood, director, 21st Century Learning & Consulting LLC, Woodbridge, VA, EE.UU., 21puzzles@gmail.com

¹² “One third of bank execs see poor money laundering controls-survey,” *Reuters*, 29 de enero del 2014, <http://www.reuters.com/article/laundrying-boardroom-idUSL5N0L33EK20140129>

¹³ Sally Quillian Yates, “Individual Accountability for Corporate Wrongdoing,” U.S. Department of Justice, 9 de septiembre del 2015, <https://www.justice.gov/dag/file/769036/download>

¹⁴ Stephen Dockery, “Johnson Controls Settles China Corruption Case With SEC,” *Wall Street Journal*, 11 de julio del 2016, <http://www.wsj.com/articles/johnson-controls-settles-china-corruption-case-with-sec-1468276763>

¹⁵ Civil Action, U.S. Attorneys’ Office, 18 de diciembre del 2014, https://www.fincen.gov/news_room/ea/files/USAO_SDNY_Complaint.pdf

¹⁶ Dana R. Hermanson, Jason L. Smith and Nathaniel Stephens, “How Effective Are Organization’s Internal Controls? Insights Into Specific Internal Control Elements,” *Current Issues in Auditing*, American Accounting Association, 2012, 6(1), pp. A31-A50, <http://aaapubs.org/doi/pdf/10.2308/ciia-50146>

¹⁷ *Ibid.*

With C6, it's easier to find
relevant compliance data.

CALL US ON 0203 741 1200 TO LEARN HOW



C6 Group

10 Queen Street Place, London EC4R 1BE, United Kingdom

Tel 0203 741 1200 | enquiries@c6-intelligence.com | www.c6-intelligence.com

NAVEGANDO LA RECOMENDACIÓN 16 DEL GAFI

En medio de la preocupación por el aumento de las organizaciones terroristas y otros grupos delictivos, se les pide a los bancos intensificar su papel en el control de pagos internacionales. Aunque se ha prestado mucha atención a cuestiones tales como las deficiencias del conocimiento del cliente (KYC) y las violaciones de sanciones—y las penas impuestas como resultado de estos problemas—la cuestión más fundamental de la calidad de los datos está empezando a atraer más atención.

Esto se confirma por las recomendaciones de 2012 del Grupo de Acción Financiera Internacional (GAFI)—en particular la Recomendación 16—que especifica la necesidad de que las instituciones financieras proporcionen información no sólo sobre el expedidor de un

pago, sino también el beneficiario. En virtud de esta recomendación, los bancos también tendrán una obligación más explícita de supervisar la calidad de los datos en las transacciones que reciben. La UE y Singapur ya han emitido normas que reflejan la Recomendación 16, y se espera que sigan otros miembros del GAFI, incluyendo los EE.UU.

El cumplimiento de los nuevos requisitos presentará algunos retos operativos y de cumplimiento significativos para los bancos. Sin embargo, al tomar las medidas necesarias para mejorar la calidad de los datos, los bancos pueden también esperar ver grandes beneficios de la utilización más eficaz de los filtros de sanciones para un mayor conocimiento de la inteligencia empresarial.

Antecedentes

Sabiendo quién está enviando y recibiendo el dinero es parte esencial de la lucha de antilavado de dinero, la financiación del terrorismo y otras formas de delitos financieros. La Recomendación 16 tiene como objetivo mejorar la trazabilidad de las transacciones, con la intención de prevenir y detectar la financiación del terrorismo y otras actividades ilícitas.

Los nuevos requisitos vienen como parte de un enfoque más amplio sobre la mejora de los procedimientos de conozca a su cliente como medio de prevención de lavado de dinero y la financiación del terrorismo y en el contexto de las nuevas regulaciones, como la Cuarta Directiva de Antilavado de Dinero de la UE. Si bien la comprensión del beneficiario final (UBO por sus siglas en inglés) de una entidad ha sido un elemento crítico de KYC desde hace años, los avances en los últimos meses

han intensificado el enfoque en esta área. “Los acontecimientos recientes, tales como la publicación de los Papeles de Panamá, han contribuido a acelerar la liberación de las reglas propuestas y finales en los EE.UU. y el Reino Unido en la formalización de la divulgación de la UBO”, comenta Daniel Tannebaum, director de la Unidad de Delitos Financieros de PwC y el líder de Global Financial Services Sanctions Practice.

Al mismo tiempo, con la mayor importancia que se le impone al tema de la prevención de la financiación del terrorismo, los bancos son vistos como la primera línea para detener que los fondos caigan en manos equivocadas. Tienen que equilibrar este deber con la necesidad de asegurarse de que los pagos realizados por los clientes sean tan rápidos, eficientes, baratos y fáciles como sea posible.

“La única manera de lograr esto es asegurarse de que los datos son de una calidad suficientemente alta para que las soluciones automatizadas pueden hacer su trabajo”, dice Stephen Lindsay, director de estándares de SWIFT. “Por eso hay un empuje para mejorar la calidad de los datos en la fuente—para que cuando se está cribando para países embarcados o clientes sancionados, se puede hacer de forma automática, eficiente y eficaz”.

¿Qué está cambiando?

Las Recomendaciones del GAFI, publicadas en 2012, constan de 40 recomendaciones. Están destinadas a proporcionar un marco que permita que los países combatan el lavado de dinero y la financiación del terrorismo de una manera consistente. Muchos países miembros del GAFI—y la UE (también miembro del GAFI)—se



encuentran en el proceso de incorporar las recomendaciones del GAFI en sus propios reglamentos y requisitos.

La Recomendación 16 se aplica a transferencias de dinero tanto internacionales como a nivel nacional. El objetivo de la recomendación, como se establece en las Recomendaciones del GAFI, es evitar que “los terroristas y otros delincuentes tengan acceso sin restricciones a las transferencias por cable para mover sus fondos, y para detectar un posible uso abusivo cuando se produzca”.¹

Partes de la Recomendación 16 ya están estipuladas por las normas anteriores del GAFI sobre este tema, la Recomendación Especial 7 (SR7), y por la regla de Viajes en los EE.UU., lo que obliga a los bancos a transmitir cierta información a otros bancos. Si bien estas normas se centran en la información del expedidor, la Recomendación 16 requiere información tanto del que la origina como del beneficiario para ser incluida en algunos mensajes financieros para transferencias electrónicas.

- Para las transferencias electrónicas transfronterizas, el nombre y número de cuenta del beneficiario deben ser incluidos en el mensaje financiero y deben viajar con la transferencia. Las transferencias también deben incluir el nombre del remitente, número de cuenta y dirección, u otra información para ayudar a su identificación, tales como su número de identidad nacional, el número de identificación del cliente, y la fecha y lugar de nacimiento.
- Para las transacciones internas (independientemente del país), que son más fáciles de seguir, los requisitos son menos onerosos, con la condición de que toda la

información debe ser proporcionada a las instituciones beneficiarias y las autoridades apropiadas por otros medios cuando se le solicite.

Seguimiento y reportes

Así como estipula la información que debe ser incluida en las transferencias electrónicas, la Recomendación 16 establece la necesidad de los bancos de monitorear las transacciones que reciben. Los bancos tendrán que asegurar que se proporcionan los datos necesarios y tomar las medidas necesarias si no lo son.

Se espera que los bancos adopten un enfoque basado en el riesgo con respecto a la falta de información del originario y el beneficiario. Esto podría incluir hablar con el banco en cuestión y favorecer el desarrollo para mejorar sus estándares. Este seguimiento puede ahora ser cada vez más robusto, con algunas instituciones financieras diciendo que si la calidad de los datos de ciertas contrapartes no mejora, buscarán poner fin a esas relaciones. Esto podría tener un impacto particular en los mercados en desarrollo, donde las regulaciones financieras son menos estrictas y los propios países no son miembros del GAFI.

Mientras tanto, según la Recomendación 16, las obligaciones de los bancos para monitorear los datos se hacen mucho más claras. Las instituciones financieras “deben contar con políticas y procedimientos eficaces basados en el riesgo para determinar cuándo ejecutar, rechazar o suspender una transferencia bancaria que carece de autor o información necesaria requerida sobre los beneficiarios; y la acción de seguimiento apropiada”.² Los

países individuales pueden ser incluso más estrictos, y la regulación de la UE habla de terminar las relaciones si hay incumplimiento repetido de los requisitos de información del ordenante y beneficiario.

La adopción de la Recomendación 16 del GAFI

A pesar de que las Recomendaciones del GAFI se publicaron en 2012, todavía se están implementando en varios países. Algunas jurisdicciones han avanzado más que otras en la adopción de las nuevas directrices. La UE publicó su legislación pertinente, el Reglamento de Transferencia de Fondos (*Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds*) en junio de 2015; sin embargo, la aplicación no comenzará hasta junio de 2017. Singapur también ha incluido la nueva normativa en la Notificación MAS 626.

El cumplimiento de la nueva normativa probablemente establecerá algunos retos significativos a la industria. Se necesitará capturar datos de buena calidad en la fuente y los bancos deberían invertir en sistemas de control de calidad sofisticados para hacerles frente adecuadamente a los desafíos de formato. En lugar de adoptar un enfoque de “bombero” y hacerles frente a las cuestiones mensaje por mensaje, los bancos deben tener un enfoque analítico con el fin de encontrar patrones y delincuentes y resolver los problemas en su origen.

¹ “Recommendation 16: Wire Transfers,” <https://www.cfatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers>

² Ibid.

En efecto, el cumplimiento de los requisitos existentes para la información del expedidor bajo SR7 no es necesariamente sencillo, sobre todo porque los datos proporcionados no están estructurados.

“Esto es algo por el que las instituciones han luchado durante años”, dice Tannebaum. “Por un lado, ha habido sanciones limitadas relacionadas con los requisitos de norma de viaje, a pesar de que ha habido legislación en vigor para un número de países que exige que cierta información acompañe la transacción. Las limitaciones de la tecnología también han sido un gran desafío. Muchas instituciones simplemente no tienen controles para detectar la información incorrecta o faltante en ciertos campos requeridos”.

Tannebaum dice lo que hemos visto en muchos bancos son desafíos relativos a fallos de sistemas que son poblados con datos incorrectos; por ejemplo, todas las transacciones habían incluido la propia dirección de la institución en lugar de las direcciones de los expedidores.

Otro obstáculo son las inconsistencias que puedan surgir entre los diferentes enfoques bancarios para la captura de datos de los clientes. Algunos bancos requieren datos completos para tanto el expedidor como el beneficiario, mientras que otros no lo hacen. “Esa incoherencia sin duda puede ralentizar las operaciones transfronterizas internacionales”, dice Tannebaum. “Un banco puede tener normas más laxas que un corresponsal de aguas abajo. Esto podría significar que una transacción se detiene debido a la falta de información que el banco es requerido por ley o política de coleccionar”, añade.

La colaboración puede desempeñar un papel importante en la mejora de la coherencia en toda la industria. El cumplimiento de la Recomendación 16 es uno de los temas que se discuten por el Payments Markets Practice Group (PMPG), que trabaja para mejorar las prácticas de mercado en relación con el uso correcto de las normas. A tal fin, PMPG ha publicado directrices específicas para el cumplimiento de la Recomendación 16 utilizando mensajes SWIFT MT.³ Las infraestructuras de mercado críticas, así como las organizaciones de la industria transnacionales como SWIFT, pueden desempeñar un papel de liderazgo en ayudar a las instituciones financieras para que trabajen conjuntamente para afrontar estos retos.

Lo que los bancos tienen que hacer

En primer lugar, los bancos tienen que asegurarse de que comprenden los cambios. Esto debe incluir hablar con otros bancos, grupos de la industria y los reguladores con el fin de entender las nuevas reglas y averiguar cómo están respondiendo los demás.

En vista de los nuevos requisitos, existe una clara necesidad de los bancos para que adopten políticas, tanto más explícitas para asegurar la exactitud de sus propios datos y para controlar los datos proporcionados por otros bancos. Los controles internos deben ser mejorados para asegurarse de que ciertos campos se rellenan con la información correcta. Los controles también deben estar en su lugar para erradicar los “datos simulados”—por ejemplo, cuando los campos se rellenan con cadenas de números en lugar de cadenas de letras.

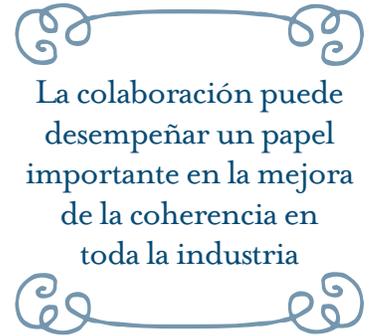
A nivel operativo, los bancos deben considerar si van a necesitar comprar software nuevo. También deben asegurarse de que tienen una visión general de todos los sistemas de pago en el grupo, así como la garantía de que cada parte del grupo está siguiendo el mismo enfoque. También tendrán que preguntarse si necesitan hacer seguimiento en tiempo real o seguimiento posterior, y la construcción de procesos y procedimientos adecuados en torno a estos puntos.

Sin embargo, el principal reto para los bancos es centrar la atención suficiente a esta zona, lo que puede ser difícil con tantas prioridades en competencia. Como comenta Tannebaum, “Muchos bancos operan bajo un enfoque basado en la clasificación, por lo que siempre se dirigen los recursos al regulador o los auditores que gritan más fuerte”.

Más allá del cumplimiento de la Recomendación 16 del GAFI

Hay más en la calidad de los datos que lograr el cumplimiento. Mientras que cumplir con la Recomendación 16 es el principal catalizador de los bancos para hacerle frente a esta área, también es importante tener en cuenta que la mejora de la calidad de datos aporta beneficios adicionales, tales como el uso más eficaz de los sistemas de sanciones relacionadas.

Esto es así porque los filtros y sistemas de las sanciones están siendo alimentados por datos que se remontan a la calidad de los pagos mismos. Si los bancos miran la calidad



de los datos y corrigen cualquier problema antes de que los datos lleguen al monitoreo de sanciones, monitoreo de transacciones, sistemas de conozca a su cliente o sistemas de antilavado de dinero, entonces esos sistemas serán capaces de operar con mucha mayor eficacia.

“El aumento de la coherencia en campos de la reducción de errores o falta de datos van a hacer nada más que acelerar las transacciones”, dice Tannebaum. “Si usted tiene una mayor confianza en los datos en el campo antes de que pasen por los filtros de detección de sanciones, tendrá una mayor confianza en su capacidad para cumplir con el mandato del programa en cuestión”, añade.

Otros beneficios secundarios pueden incluir el procesamiento directo mejorado y mejoras en los procesos de monitoreo de transacciones. Además, la mejora de la calidad de datos les puede permitir a los bancos utilizar sus propios datos de manera más eficaz desde el punto de vista de la inteligencia empresarial. Los flujos de pagos de un banco representan una rica fuente de inteligencia empresarial en áreas tales como qué relaciones son las más rentables, a qué países el banco se encuentra más expuesto y de dónde vienen sus negocios. Mientras más datos de calidad tenga un banco acerca de los remitentes y los beneficiarios de estos pagos, habrá más información utilizable.

En conclusión, la calidad de los datos puede no haber atraído tanta atención en el pasado como algunos otros temas. Sin embargo, la adopción de la Recomendación 16 sitúa este problema más arriba en la lista de prioridades—y a pesar de los retos que implica, la mejora de la calidad de datos también aportará beneficios considerables más allá del cumplimiento normativo. **FA**

Simon Muir, director de producto de la División de Servicios de Cumplimiento de Delitos Financieros, SWIFT, Bruselas, Bélgica, simon.muir@swift.com

³ Véase www.pmpg.info



or



Are you concerned by correspondents' de-risking plans?

Being in the 'no'

De-risking is now common. Correspondent banking relationships are under significant pressure. For smaller banks, or those working in places that are perceived to be high risk, this can have a significant impact on reputation and business levels.

Being in the know

Thankfully there's now a suite of accessible tools and services to help. At SWIFT, we enable you to put the right controls in place, to improve transparency and to ensure that partners can work with you efficiently and cost effectively. This will then help you to communicate your improved risk profile to existing and potential partner-banks.

Start today

Our tools and services can be used flexibly to meet your specific needs. To the right, we give an overview of some key tools. [To find out more, talk to your SWIFT representative today.](#)

The answer is transparency and compliance.

1

Improve efficiency, cut cost

[The KYC Registry](#) provides access to a central repository of standardised, up-to-date due diligence documents. It's a fast, cost-effective solution that enables you to monitor, manage and grow your correspondent banking network.

2

Strengthen your Sanctions Screening

[Sanctions Screening](#) is an easy to use, cost-effective SWIFT-hosted tool that enables you to screen all types of financial transactions in a standardised way.

3

Understand exposure with the SWIFT Traffic Profile

[The SWIFT Traffic Profile](#) is a low-cost tool that gives you an aggregate view of the bank's exposure to traffic with sanctioned and high-risk countries.

4

Test compliance with FATF Recommendation 16

[Payments Data Quality](#) is an advanced reporting and data analytics service from SWIFT. It enables you to evaluate the quality of originator and beneficiary information in SWIFT payment messages across your global operations, and also with your correspondents.

build better banking partnerships
swift.com/transparency





Anuncios europeos

Nota de la jefa de redacción: Conexión Europa es una sección de la revista ACAMS Today que actualizará las noticias y actividades de ACAMS en Europa para los socios.

A medida que avanzamos hacia el otoño, quiero llamar su atención sobre el blog de Samantha Sheen—un recurso grande y nuevo que se centra en temas de antilavado de dinero (ALD) que afectan el sector de la delincuencia anti-financiera en Europa. Visite www.acams.org/aml-resources/samanthasheens-blog/ para leer lo que piensa Sheen sobre temas diversos, incluyendo RegTech, la Cuarta Directiva sobre ALD, el reporte sobre ALD de la Autoridad Financiera de Conducta del Reino Unido para 2015/2016, el maltrato a personas mayores, la diligencia debida mejorada, la capacitación anti-delito financiero, la realización de negocios con Irán y la Cumbre Anticorrupción de Londres.

Actualizaciones de CAMS

CAMS en francés ahora está en vivo y nuestra primera aula virtual de CAMS en francés comenzó en agosto. Además, vamos a comenzar a traducir CAMS al alemán este otoño con el objetivo de ir en vivo en la primavera de 2017. Para obtener más información, póngase en contacto con europe@acams.org.

Certificaciones avanzadas

Planeamos celebrar nuestro primer programa de Certificación Avanzada en Europa este invierno y les escribiremos con más información a los de ustedes que en breve tendrán la certificación CAMS.

Eventos europeos

Vamos a ofrecer más capacitación en persona y eventos educativos en toda Europa, incluyendo seminarios y conferencias en Londres, Nicosia, Ámsterdam y Varsovia, y nuestra primera *Conferencia del Mediterráneo Oriental de ALD de ACAMS* en Chipre en febrero de 2017.

Capítulos en toda Europa

Además de lo anterior, los capítulos de ACAMS están ejecutando un programa integral en toda Europa con los eventos ya planificados, de septiembre a diciembre de 2016 para Ámsterdam, Berlín, Dublín, Frankfurt, Londres, Múnich, Nicosia, París y Estocolmo. Detalles del evento se pueden encontrar en las páginas de los capítulos individuales en ACAMS.org. Seguimos recibiendo comentarios de interés sobre establecer nuevos capítulos en Italia, Letonia y Malta, y nos gustaría hablar con los socios interesados en unirse a nuestras mesas directivas de capítulos de Luxemburgo y España. Si usted está interesado en unirse a o en establecer un capítulo local de ACAMS o en ser anfitrión de un evento de contacto entre pares, por favor envíenos un correo electrónico a europe@acams.org. 

Angela Salter, directora de Europa, ACAMS, Londres, Reino Unido, asalter@acams.org

MEASURE, UNDERSTAND & EXPLAIN YOUR MONEY LAUNDERING RISKS

This first-of-its-kind solution helps your institution:

- Identify risks within and across all lines of business
- Mitigate risk by filling in the gaps in your detection and prevention controls
- Present trusted reports that are up-to-par with the latest global regulation and guidance
- Clearly communicate risk to all stakeholders through standardized and automated presentation-ready reports

Schedule a product demo: riskassessment@acams.org

Visit our booth at ACAMS 15th Annual
AML & Financial Crime Conference
from September 26-28, 2016 in Las Vegas



Mary Bashore, CAMS:

El siguiente paso como directora ejecutiva emérita de la junta directiva

A *CAMS Today* tuvo el privilegio de hablar con Mary Bashore acerca de la reciente posición de directora ejecutiva emérita de la junta directiva del Capítulo de la Capital de los EE.UU. y su reciente nominación para llenar este papel.

Bashore es la presidenta de Bashore Business Solutions, LLC. En esta función utiliza su amplia experiencia y conocimiento en actividades de antilavado de dinero (ALD) y operaciones de instituciones financieras para asesorar a clientes en temas de gestión de riesgos.

Durante su carrera federal, Bashore avanzó desde un cargo de examinadora de institución financiera hasta convertirse en especialista de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) y asesora técnica de personal responsable de las acciones de fiscalización y de aplicación de más de 1.400 instituciones financieras. Bashore lideró, desarrolló y capacitó personal en varios sistemas y en la realización eficaz de los exámenes de la BSA, analizó datos y proporcionó orientación a las partes internas y externas. Preparó acciones administrativas, manejó los temas de regulación más complejos y delicados, en estrecha coordinación con la Red Contra los Delitos Financieros y otras agencias gubernamentales.

Como líder reconocida y colaboradora, Bashore capacitó a examinadores del Consejo Examinador de Instituciones Financieras Federales y es miembro del Comité Ejecutivo del Foro de ALD de la Costa Oeste. Además, se incorporó al Capítulo de la Capital de los EE.UU. en junio de 2012. Desde su incorporación, el capítulo ha más que doblado el número de socios, mantenido comunicacio-

nes con ACAMS, aumentado la asistencia a eventos de capacitación, escrito artículos y piezas de comunicación, hecho participar a socios individuales, y se ha promovido. Además, ella es un punto de contacto para los colegas de la junta directiva, así como de socios del capítulo. Sobre la base de su experiencia y participación en el capítulo, el 30 de junio del 2016 fue designada directora ejecutiva emérita del Capítulo de la Capital de los EE.UU. de ACAMS.

ACAMS Today: Usted fue nominada recientemente la emérita de la junta directiva del Capítulo de la Capital de los EE.UU.— ¡Felicidades! ¿Cuál será su nuevo papel como ejecutiva emérita de la junta directiva?

Mary Bashore: Mi nuevo papel va a ser más de carácter consultivo. Ya no voy a tener un voto en las decisiones de la directiva y no voy a tener las responsabilidades específicas de un miembro de la junta. Sin embargo, todavía estaré involucrada activamente en los asuntos del capítulo. Además, voy a ser el puente en la transición entre los actuales miembros, los miembros de juntas futuras y las nuevas personas que quieran involucrarse con el capítulo. Todavía estaré disponible como asesora para ayudar a que la gente que entra ocupe su nuevo papel y

contribuya a desarrollar un nuevo liderazgo. Voy a poder aprovechar mi experiencia y conocimientos adquiridos como miembro de la junta y compartirlos con mis compañeros de la junta y otros nuevos que están interesados en ascender.

AT: ¿Cuánto tiempo va a servir como directora emérita de la junta ejecutiva?

MB: Está armado como un cargo de tres años, que por supuesto es muy flexible. Puedo renunciar a la posición antes de tres años, pero preveo servir durante los tres y después de haber hecho la transición plenamente en ese punto seguir adelante. Pero, por supuesto, la puerta está siempre abierta. A los de la junta les gustaría que permanezca más tiempo y todavía cuentan conmigo para ayudar a medida que el capítulo crece y se siguen haciendo más cosas. Sin embargo, creo que voy a ser capaz de dar un paso atrás en tres años y ver los frutos de mi trabajo, por así decirlo.

En cuanto a la ampliación del plazo, los capítulos que buscan implementar este papel tienen la flexibilidad necesaria para hacer lo que funciona para ellos. He hablado con personas en otros capítulos de vez en cuando para obtener sus ideas y John Byrne estaba pensando que otros capítulos pueden querer adoptar un modelo similar. Sin embargo, no



tiene por qué ser exactamente de la manera que lo hemos hecho. Cualquier otro capítulo está bienvenido a adoptarlo como lo hemos hecho o de ponerlo en un segundo plano. Dado que el director emérito no tiene un voto, le corresponde a la actual junta establecer la dirección del capítulo.

AT: ¿Qué hizo que este fuera un paso importante para el Capítulo de la Capital de los EE.UU.?

MB: Creo que fue un paso importante para nosotros porque sentí que había estado en la junta lo suficiente y que había dominado mi papel y estaba lista para darle paso a otra persona. Además, pensé que otras personas de la junta podrían estar pensando en la misma línea. Todos nosotros hemos estado en la junta desde hace varios años y hemos estado en la misma posición. Quería ver cierta rotación. Sin embargo, yo quería ver una rotación ordenada donde mantuviéramos un poco de experiencia, pero dando cabida a nuevas personas que estaban interesadas en asumir un papel más importante. Así que en lugar de renunciar a la junta y tirándosela a un nuevo miembro de la junta sin experiencia o sin manera de ponerse al día, ideamos esto como una forma de tener una transición ordenada. Y parece estar funcionando muy bien.

Si nos fijamos en las calificaciones con cuidado, casi todo el mundo en nuestra junta podría calificar para ser director emérito de la junta en algún momento

AT: ¿Cómo está trabajando su capítulo para implementar esta función?

MB: La transición ha sido totalmente transparente, porque todos se conocen muy bien y ya hemos podido contar el uno con el otro y trabajar juntos. Además, hemos incorporado un par de gente nueva a la junta hace unos meses. Ha sido realmente una transición que ha estado en mente durante aproximadamente un año. Es algo que simplemente hemos seguido hablando

de a poco. Hace aproximadamente un año, planteé el tema de la transición y la contratación de nuevas personas a mis compañeros de la junta y de abrir la posibilidad de que otras personas puedan venir a la junta. He llegado al máximo de lo que creo que puedo contribuir como miembro de la junta, así que quería ir en una nueva dirección. Me gusta dominar algo y luego seguir adelante. Por lo tanto, logra varias cosas.

AT: ¿Qué impacto tendrá esta posición en el capítulo en su conjunto?

MB: Bueno, estoy esperando dos cosas: 1) Que no perdamos la experiencia de la gente que como yo ha tenido la experiencia de trabajar en el consejo y realmente ha llevado la posición a un nuevo nivel y 2) animar a la gente a convertirse en socios del capítulo y hacerla participar proporcionando también oportunidades para que puedan asumir un papel mayor. Por ejemplo, tenemos un comité de programas que tiene un número de miembros que participan en eventos de aprendizaje de planificación y esperamos que haya una etapa de transición de aprendizaje para reclutar gente como futuros miembros de la junta. Ya tenemos el ojo puesto en un par de personas que pensamos que van a ser buenos miembros de juntas futuras. Así que gran parte de ello depende de la disponibilidad y la voluntad. Tenemos una gran cantidad de personas nuevas y más jóvenes en el campo del ALD que nos gustaría que se involucraran en el capítulo porque de ahí es de donde el crecimiento va a venir.

AT: ¿Cómo funcionó el proceso de designación del director ejecutivo emérito de la junta?

MB: Cuando propusimos la idea de un director emérito de la junta, expusimos lo que pensábamos que eran algunas condiciones razonables. Por lo tanto, el primer paso para la junta fue adoptar el cargo en general y ver lo que era y lo que no era. El proceso de nominación fue un tema separado donde tomamos las calificaciones para director emérito de la junta y nos fijamos en los antecedentes y logros de un individuo para ver cómo él/ella encajaba. Las nominaciones fueron escritas y distribuidas por correo electrónico y luego adoptadas, por lo que podría incorporarse en las actas y hacerse oficial para el registro. El copresidente Dennis Lormel y tres o cuatro más me nominaron en base a lo que ya sabían acerca de mis antecedentes. La decisión fue básicamente unánime y recibí un montón de felicitaciones después de diferentes personas

que dijeron: “Usted sabe que esto es realmente una gran idea y no es algo en que yo habría pensado. Esto es algo que otras personas pueden utilizar”. El capítulo estaba muy feliz y emocionado de no perderme como miembro activo del capítulo y tener un papel diferente y forma diferente de usar a la gente en su experiencia. Después de las nominaciones, avisamos a ACAMS, para que apareciera en el sitio web de capítulos y comunicaciones.

AT: ¿Quién es elegible y qué atributos consideraba su capítulo al proponer candidatos?

MB: Con el fin de ser considerada, una persona debe ser un miembro actual o anterior de la junta ejecutiva del Capítulo de la Capital de los EE.UU. de ACAMS que:

1. Ha sido miembro de la junta directiva con distinción durante al menos tres años;
2. Ha mantenido un importante papel de liderazgo y ha hecho o sigue haciendo contribuciones significativas;
3. Ha ejecutado importantes actividades voluntarias o de promoción al servicio de la junta;
4. Ha finalizado el (los) término(s) para el cual él/ella fue designado; y
5. Ha participado en o liderado actividades del Capítulo de la Capital de los EE.UU. (por ejemplo, eventos de aprendizaje, comunicaciones, relaciones con los miembros, etc.).

Si nos fijamos en las calificaciones con cuidado, casi todo el mundo en nuestra junta podría calificar para ser director emérito de la junta en algún momento. Todos nosotros hemos estado en la junta durante más de tres años y todos nosotros hemos coordinado eventos de aprendizaje en diferentes momentos. Algunas personas han hecho contribuciones más significativas que otras, pero a veces las contribuciones de una persona están detrás de las escenas y la gente no las ve. Pero casi todo el mundo en nuestra junta tendría derecho a la nominación en algún momento.

AT: ¿Qué consejo les daría a los capítulos que buscan adoptar este nuevo cargo?

MB: Hay un montón de diferentes maneras de implementar esta función. Creo que parte de ello es sólo construir sobre el éxito que se

La gente quiere aprender y escuchar a los expertos en el campo

tiene, y también crear una oportunidad para que otros se comprometan. De esta manera todo no le quedará a una o dos personas que tendrán que llevar toda la carga.

Las personas que buscan servir en la junta tienen una ventaja en términos de crecimiento personal y profesional. Como miembro de la junta, se hacen contactos más de cerca no sólo con compañeros de la junta, sino también con otros miembros del capítulo y con ACAMS. El primer año como miembro de la junta uno está aprendiendo. Al año siguiente se ha aprendido dónde se está ubicado en la junta y se empieza a hacer las cosas y pensar en el futuro y cómo se puede hacer que el capítulo sea aún mejor. Por el camino, es importante considerar cómo el capítulo puede seguir basándose en los éxitos del capítulo, involucrar a los miembros del capítulo y darle cabida a gente nueva. Esta nueva función puede ser una buena manera de hacer esto; sin embargo, no es la única manera. Pero tal vez es una buena manera de involucrar a todo el que esté interesado en tener un papel activo en el capítulo.

Además, creo que es importante escuchar a los socios. En eventos de hacer contactos o de aprendizaje, la gente tiende a quedarse al final para hablar—ese es el momento en que se puede hacer el mejor trabajo porque la gente se siente libre de hablar con uno. Se establecen relaciones y comienzan a tirar ideas que suelen empezar con algo como: “¿No sería bueno si...?” o “¿Ha pensado en tener un programa de...?” o “Oí a un muy buen orador. Sería genial si esta persona llegara e hiciera una presentación para el capítulo”.

AT: ¿Cómo ve el crecimiento del capítulo en los próximos dos años?

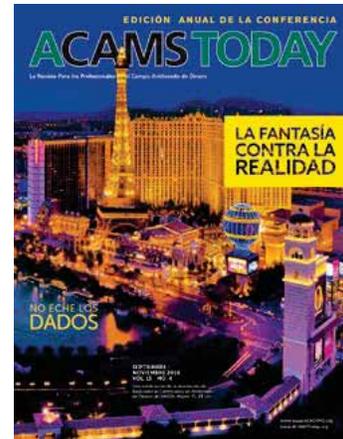
MB: No tengo un plan de lo que creo que la membresía del capítulo podría ser, pero estoy convencida de que nuestros números han aumentado porque ofrecemos valor (por ejemplo, eventos de aprendizaje). La gente quiere aprender y escuchar a los expertos en el campo. Quieren reunirse y compartir sus preguntas y preocupaciones con otras personas. Tenemos una enorme variedad en nuestro capítulo porque tenemos una fuerte presencia gubernamental, tenemos fuertes lazos con las agencias de control legal, tenemos grandes instituciones y también tenemos una gran cantidad de bancos comunitarios más pequeños, cooperativas de crédito y otras entidades no bancarias en nuestra membresía. La variedad es grande y la gente está en todas las diferentes etapas de su carrera. Creo que estamos en una posición única para reunirnos y discutir nuevas ideas para crecer. Parte de ello es la variedad. Tenemos acceso a algunas estupendas personas que son expertas en su campo y tenemos una gran cantidad de personas llenas de energía. Así que veo un gran potencial allí. 

Entrevistada por: Alexa Serrano, CAMS, asistente editorial, ACAMS, Miami, FL, EE.UU., aserrano@acams.org

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

Email: info@acams.org

Online: ACAMS.org ACAMSToday.org

Patricia Cabrera:

La experiencia de la conferencia



Patricia Cabrera es actualmente la gerente de eventos de los EE.UU. de ACAMS, donde es productora de la conferencia más importante del mundo de antilavado de dinero (ALD), la *Conferencia Anual de ACAMS de ALD y Delitos Financieros en Las Vegas*. Cabrera se unió a ACAMS en 2014, como gerente de eventos internacionales, produciendo conferencias en todo el mundo, incluyendo Hong Kong, Londres, Dubái y Toronto.

Antes de trabajar en ACAMS, pasó cuatro años produciendo y gestionando eventos educativos en la industria de servicios financieros. Antes de entrar en el espacio del ALD, Cabrera ocupó puestos de marketing en la industria de TI, donde representó a los principales proveedores en los mercados de Latinoamérica y el Caribe. Cabrera es bilingüe en inglés y español y tiene una licenciatura en marketing.

ACAMS Today: ¿Qué esperas con interés en los eventos de ACAMS?

Patricia Cabrera: Espero poder saludar a los oradores con los que he estado trabajando durante tanto tiempo en el programa.

AT: ¿Qué consejo les daría a los miembros que buscan sacar el máximo provecho de su experiencia de la conferencia?

PC: Animo a los miembros a aprovechar realmente las oportunidades de establecer contactos. Hay tanta gente con la que conectarse en estos eventos.

AT: ¿Qué será lo más destacado de la conferencia anual de este año?

PC: Los aspectos más destacados de este año incluyen un discurso de apertura del Honorable Thomas Curry, presentaciones especiales de Polaris y el ICIJ, el taller de simulacro de juicio sobre *La Fabricación de un Lavador de Dinero* y las sesiones de Connection Corner dentro de la pista de exposiciones del Salón de Interacciones.

AT: ¿Qué oradores o sesiones son los que más la entusiasman y por qué?

PC: Estoy con ganas de aprender de los profesionales consumados que llevan las sesiones de *Mujeres en ALD* dentro de las exposiciones del Salón de Interacciones. Es una de las muchas características nuevas en el programa de este año y estoy muy contenta de recibir retroalimentación de parte de los asistentes.

AT: ¿Cómo han cambiado las cuestiones de ALD/CFT desde que empezó a trabajar en la industria de los servicios financieros?

PC: Siento que la tecnología se ha convertido en un problema mucho más grande, tanto en el frente de la ciberdelincuencia y la ciberseguridad. Los oficiales de cumplimiento de hoy en día necesitan tener un firme conocimiento de cuestiones tecnológicas con el fin de ser gestores eficaces de ALD.

AT: Usted es una viajera ávida—¿adónde querría viajar próximamente?

PC: Me gustaría ir al Japón para echar un vistazo a la historia de Asia, tanto antigua como moderna, porque es un interesante contraste con las influencias culturales estadounidenses y cubanas con las que crecí. **A**

Entrevistada por: Alexa Serrano, CAMS, asistente editorial, ACAMS, Miami, FL, EE.UU., aserrano@acams.org

Graduados de la Certificación Avanzada



Brasil

Rosali Andrade, CAMS-Audit

Canadá

Chris Randle, CAMS-Audit

Estados Unidos

William Akel, CAMS-Audit

Miguel Alcántar, CAMS-FCI

Elizabeth Bethoney, CAMS-FCI

Patrick Brown, CAMS-FCI

Doug Bruggeman, CAMS-FCI

Susan Devine, CAMS-Audit

Brooke Ferris, CAMS-Audit

Kevin Harris, CAMS-FCI

Jody Hochstein, CAMS-FCI

Jason Honeycutt, CAMS-Audit

Daniel Kim, CAMS-FCI

Yunhong Liu, CAMS-Audit

Terri Luttrell, CAMS-Audit

Miguel Martinez, CAMS-FCI

Joseph Meyer, CAMS-Audit

Holly Peck, CAMS-FCI

Jeffrey Pedecine, CAMS-FCI

Debbie L. Rogers, CAMS-FCI

Conrad Tillett, CAMS-Audit

Siddhartha Valluri, CAMS-Audit

Donovan Williams, CAMS-FCI

John Wood, CAMS-Audit

India

Arun Krishnamoorthy, CAMS-FCI

Jamaica

Keron Burrell, CAMS-Audit

México

Andres Noren-Jacobson, CAMS-Audit

Países Bajos

Kathleen Veldhuizen, CAMS-Audit

Santa Lucia

Sylvia Auguste, CAMS-Audit



Graduados de CAMS: Mayo-Julio

Alemania

Daniella Fantoly
Michael Fehling
Sebastian Hegel
Janina Marx
Torsten Neuwirth
Susana Seghers-Aguilar
Tatiana Turculet

Andorra

Susana Arias Martinez

Antigua y Barbuda

Sheila Tomlinson-Brown

Arabia Saudita

Fahad A. Al-Musned
Mohammed Al Qahtani
Waleed Alajlan
Madullah Al-Enezi
Ahmed Al-Shareef
Faisal Ahmed Alzhrani

Aruba

Jilliann van der Biezen-Cuba
Doris Canwood
Lauranique Corsen
Enrique Dirks
Jennifer Jacobs
Letizia Stephanie Maduro
Larissa Oduber-de Cuba
Janice Sint Jago
Judeline Taylor Angel

Australia

Hannah Dougherty
Alexandra Heath
Georgina Larkings
Pierre Lindner
Jake Nicholson
Gerard O'Sullivan
Alla Polyanskaya
Ke Seeng Wong
Weiyun Wu

Austria

Tibor Baricza

Bahamas

Roberto Crespo
Stella Giani

Bahréin

Omar Al Bastaki
Faisal Alabsi
Ahmed Suraj Ali
Layla Yousif Almadhi
Maan AlSamahiji
Umer Arslan
Fahad Bakhsh
Kunal Deo
Mujtaba Habib
Ali Hussain Merza Mohamed
Sriraj Ramesan
Amit Sharma
Ananth Nag Surisetty

Barbados

Louis Parris

Bélgica

Narendra Choudhary
V. Dakshinamurthy
Prabhakar Gunasekaran
Prakash Paranthaman

Bermuda

Amit Malde
Martina Olcheski-Bell

Bonaire

Leydi Ortegon

Botsuana

Gaone Mathumo
Cosmas Ndlovu

Brasil

Felipe Ilg Brandão
Jose Da Silva
Daniela De Moraes Lizaso
Gabriela Dias
Arthur Dos Santos Neto
Alessandra Raspante Soares
Eduardo Silva
Shuo Wang

Canadá

Manoj Kumar Ahuja
Cynthia Alam
Zohair Allawala
Trinjna Bassi
Jessica Bello

Anne Marie Brubacher
Tania Brunet
Chadwick Burgess
John Cambareri
Latoya Campbell
Denise Carson
Francisco Chaves
Jason Chen
Derek Chiu
Denise Chow
Paul Chung
Louisa Chung
Chad Colston
Bryan Corriveau
David Cross

Deborah Doiron
Andrae Duhaney
Karen Duncan
Rogean Edwards
Mark Etwell
Charlene Faloon
Sabrina Fitzpatrick
Amanda Gaffney
Russel Godinho
Amy Harvey
Sandy Henry
Howard Hsin
Mohammad Tanveer Islam
Lepa Jankovic
Courtney Jordan
Pussellage (Madhu) Kandage
Volkan Karalar
Samuel Kiragu
Victor Korompai
Jason Chi Thanh Lac
Steven Lai
Alia Lalani
Anna Lang
David Lee
Brian Leung
Boubacar Leye
Kai Shing Jeff Lin
Kamila Llacuna
Mary Lozinski
Carinta Mannarelli
Maria Marlene M. Gomes
Tammy Mueller
Rhys Newman
Andy Ng
Yasmin Nizami
Wasif Noorani
Patience Oduro
Giselle Piepp
Yelena Popov

Clyde Roach
Bettina Rowe
Lisa Scotland
John Shoemaker
Amit Sonnilal
Christopher Sullivan
Robin Taylor
Hoa Tran
Rick Tsang
Anthony Tsang
Derick Twesigye
Akhil Uppal
Giovanni Vasiento
Laurene Watson
Daniel Wettlaufer
Kian Hock (Steven) Yeow
Dayna Young
Elena Zhrebenco

China

Jiahui Cai
Rui Cao
Weihua Cao
Xuemei Chang
Wei Chen
Min Chen
Hongguo Chen
Linman Cui
Ningling Deng
Libi Deng
Jiamin Deng
Ming Ding
Benjamin Kum Chuin Ee
Qingyun Fan
Zhihua Gao
Yue Gao
Mowa Gao
Ning Ge
Xiangli Ge
Lei Gong
Jun Gu
Xiaogeng Guan
Qianting Guo
Ping Guo
Huimei He
Pengyan Hou
Yijing Hu
Cheng Huang
Yinan Hui
Qiuxia Jiang
Zhiwei Jiao
Ye Jin
Le Kang
Yiqian Kang

Xiaowei Lai
Lin Li
Meihua Li
Chengyu Li
Peiyi Li
Guli Li
Bo Li
Jingjing Li
Yanke Li
Xiuqing Lin
Li Lin
Xun Liu
Kan Liu
Pingping Liu
Hua Lu
Zhihao Lu
Xiaoyan Lilly Luo
Lu Ma
Li Mao
Satyendra Narayan
Jing Ning
Zhenjie Qu
Ying Ying Shao
Bei Shen
Cencen Song
Yulong Tang
Yu Tian
Weidong Wang
Yan Wang
Lina Wang
Yanji Wei
Qianhong Wen
Yujin Wen
Yu Feng Wu
Chenjin Wu
Yuanqiu Wu
Yanwen Wu
Jun Xia
Tina Xu
Wei Xu
Keda Xu
Kenan Xu
Jinxi Xue
Liuqing Xue
Yan Yan Yang
Long Yang
Ruoyu Yang
Li Yang
Ming Yang
Lihua Yang
Fuming Yang
Ying Ye
Floyd Zhang
Wei Zhang

Jie Zhang
Aixia Zhang
Guoqing Zhang
Wanbing Zhang
Gaoju Zhang
Yi Zhang
Guo Xiong Zhong
Shaohuan Zhou
Ting Zhou
Liwei Zhou
Rui Zhu
Ya Zong
Xu Zuo

Chipre

Viktoria Askalidou
Elina Christofi
Christakis Hadjiconstantinou
Antonis Hadjieftychiou
Georgios Konstantinou
Yianna Stylianou Neocleous
Loizos Timinis
Frixos Zempylas

Corea del Sur

Minju Kang
Juhyun Lee
Sunmi Yim

Curaçao

Farah Betrian-de Haas
Gino Campbell
Melissa Haseth
Sharetti Kunst
Najola Martina
Genesis Martis
Nihaila Sambo
Margaretha van O.-Hofhuis
Susan Wong
Naesha Zunder

Dinamarca

Nina Jørgensen

Egipto

Tarek Abo Steit
Mohamed K. R. Mahmoud

El Salvador

Alicia M. C. De Beltran

Emiratos Árabes Unidos

Easha Abayasinghe
Mohammed Abrar
Prithvi Narendra Adnani
Rehan Ahmad
Rafi Ahmad
Maria Ibrahim Al Harastani
Tamer Tawfiq Al Sayeh
Raluca Alexandrescu
Shayista Arshad
Shmyila Kunwal Arshad
Rajeev Babel
Samrath Bachani
Mahmoud Baddar
Azra Bajwa
Sheraz Ahmed Bari
Alaa Eldin Bebars
Nisha Bhatia
Liesbet Brondeel

Xiaoling Chen
Tressy Crasta
Pijush Kanti Das
Nilanjan Dutta Roy
Asmaa El Monshed
Nayla El-khatib
Rajnish Kumar Gaurava
Mereena George
Dilani Gunewardana
Nipun Gupta
Phoebe Iacovides
Noman Iqbal
Jithin Jacob
Jeswin Jose
Manoj Kapur
Naqqash Narose Khan
Niaz Khawaja
Irina Kostenko
Rajinder Kumar
Dhruva Lawale
Xuanguang Li
Sonia Manek
Kartik Manohar
Ahmed Maouad
Arun Miglani
Nelly Mistry
Vanita Naik
Sobhie Nassar
Verghese Panackel Peter
Manoj Patra
Rajiv Philip

Anthonia Pinheiro
Ishela Pinto
Senthil Prabhu
Jennifer Rabener
Neethu Rajan
Joel Randleman
Manto Saikia
Derick Saldanha
Sudhakar Sanjeevi
Sadaf Shams
Saboor Siddiqui
Amit Singh
Kalyan Krishna Siripurapu
Laura Smith
Zohaib Soomro
Daniel Stewart
R. S. Tattanangalam
Herlina Susilo
Santosh Talada
Syed Asif Tanwir
Maryann Thekkekkara
Mohammad A. Ur Rehman
Kenneth Sertorio Vaz
Supriya Venugopal
Rasika M. Wickramasinghe
Manu Yoganand

España

Gema Alvarez Lopez
Carlos Carretero de Suelves
Ernesto Cebrian Amigo
Salvador Colomer Pellicer
Laura Garcia De Abia
Laurent Germain
Antonio Pizarro Cabello

Estados Unidos

Kelli Abawi
Lori Abbott
Muhammad Abdoolraman
Christopher Able
Eman Abu-Ajamieh

Emmanuel Adjei
Arumugam Agastheswaran
Akhil Agrawal
Nusrat Ahmad
Shalah Ahmed
Sungin Ahn
Mohammad Al Ghananim
Claudia Alcantar
Teri Alexander
Jonathan Alloy
Michael Altamirano
Phillip Ambrose
Abigail Amend
Roberto Amenta
Victoria Amey
Golriz Amid
Jessica Anaipakos
Nicholas Angerame
Chanida Angkanarak
Kazi Anisuzzaman
Aaron Ansel
Mohamed Shafeer Anzar
Roma Apuya
Liza Arcayena
Martha Arce-Alcala
Oscar Arevalo
Stephen Argenbright
John Bajcic
Heather Baker
Shelby Baldwin
Dharmesh Balsara
Heather Bannon
Cindy Sue Barbezat
Rodney Barge
Vanessa Barry
Maher Barsoum
Karl Bautista
Logan Beard
Kimberly Beatson
Amy Becsi
Mark Beeley
Joanna Beer
Denise Beighley
Nicholas Belani
Fernando Benito
Catherine Benjamin
Tom Berkovitch
Achilles Bernal
Jonathan Bernstein
Dan Bertch
Pierre Betzu
Carly Blades
Tracy Blaske
Paul Boland
Maxwell Boltz
Kristie Bond
Deborah Bonfield
Marietta Boniatos
Michelle Boursiquot
Victoria Bova
Gerald Boyd
Nancy Brady
Deliah Brantley
Morris Breitbart
Michael Breu
Deetria Bridges
Colleen Brinker
Judy Britt
Reid Brooks
Nancy Brooks
Gwendolyn Brown
Aaron Brown
Marc Brumm
Bridgette Brylla

Ahmad Bsharat
Corey Burd
Monica Burleson
Nora Busquets Arada
Ray Cabral
William Cadenilla
Patricia Cadilla
Edward Cahill
Pamela Calaquian
Thomas Carnoia
Richard Campbell
Kerian Campbell
Dinneen Candela
Nicole Canestrini
Jared Caracappa
Mary Ann Carpenter
Kathryn Carr
Sebastian Carrizosa
John Carroll
Sarah Carson
Kacey Carver
Carol Casale
Erica Case
Iwona Castro
Patrick Cave
Mirela Cekic
Anastasia Cembrovskva
Jaclyn Chall
Kwok Kong Chan
Sudhanshu Chandra
William Chang
Mici Chase
Justin Cheaves
Jorge Checo
Rosangela Chen
Hung Tse Chen
Henry Chen
Joanna Chiu
Nathanael Cho
Eun Chou
Sukjin Chung
David R. Clark
James Clay
Erin Clemens
Cherry Clendaniel
Cristie Cloutier
William Coates
Richard Coats Jr.
Megan Cobb
Selasie Coffe
Andrew Cohen
Mark Collum
Whitney Connell
Tonya Conner
Melanie Coon
Nicola Copeland
Jeffrey Cortese
William R. Costello Jr.
Richard Cottrell
Matthew Couillard
Jody Cranford
Rebecca Criswell
Jenry Cruz Jr.
Barry Currah
Patrick Curtin
Agnieszka Czarnecka
Amy Dadowski
Bettina Dal Santo
Kathleen Davin
Matthew Davis
April Davis
Justin Davis
Tricia Davisson
Matthew Dehaven

Geraldine Del Prado
Peter Dembinski
Ilir Demiri
Jennifer Demos
Chelsea Dengel
Cynthia Denissen
Samy Derival
Zachary Dikstein
David Dimov
Mark Donald
Wisdom Donkor
Charles Donnell
Janet Dougherty
Matthew Dougherty
Mary Doyal
Nicholas Doyle
Emily DuBreuil
Anthony Dufresne
Deborah Dunn
Mario Duron
Marc Eagle
Ebo Edonu
Scott Edwards
Michael Ehrlichman
Richard Elizarde
Staci Engi
Monica Enke
Johnathan Epps
Frank Espinoza
Natasha Esquivel
Edward Fahey
Adesola Fakiyesi
Thomas Falotico
Cheryl Farfan
Scott Farmen
Beatrice Faurescu
Pasquale Fedele
David Felt
Cassandra Fenstermaker
Diana Ferguson
Manisha Fichadiya
Christina Fisher
Kevin Flanagan
Susan Flores
Paul Florez
Siobhan Florvil
Carolyn Flowers
Erin Flynn
Brenda Fonseca
David Foppert
Charissa Ford
Ferenc Forintos
Hector Fortin
Kamla-Marie Francis-Jordon
Pamela Frank
Dara Frank
David Fransway
Andrew Frey
Stanley Fronczkowski
Kayleigh Fry
Jayakar Gadde
Stephen Gallagher
Drew Galow
Jing Gan
Tom Ganem
Gregory Garcia
Betty Garfias
Alberto Garza
John Geiringer
Elizabeth Gelsomino
Charlie Genao
James Gentile
Austin Geraghty
Michael Gerrity

Amanda Gerwel	Anthony Judycski	Daniel Mardakhayev	Olga Lucia Olaya Ramirez	Becky Rockwell
Tawny Giles	Purnima Kalahasthi	Linnea Maria	Oliviere Oliver	Cheryl Rodier
Emily Gill	Elinathan Kamau	Cassandra Mark	Lori Olson	Gabriela Rodrigues Epstein
Christopher Gill	Gurran Kane	Megan Marshall	Grace Oluyemi	Carlos Rey Rodriguez
Michael Gocklin	Naheed Karamali	Aridia Martin	Adaeze Onwuzuruike	Elida Rodriguez
Michael Goldstein	Daniel Karwowski	Philip Martin	Sean Ortiz	Raquel Romero
Jamee Gomez	Tami Kaster	Gilda Martinez	Deborah O'Toole	Kathleen Ronge
Juan Gonzalez Vigoya	Jeff Kearney	Aileen Martinez	Michael Owens	Karina Roque-Cabrera
Aaron Goodwin	Carla Kelly	Maria Marzec	Brandon Pacifica	Eric Rose
Marina Gordin	Paula Kelsey	Thomas Massey	Sindy Paiz	Zachary Rosenberg
Samuel Gottlieb	Michael Kenah	Justin Masterman	Antoine Palanca	David Ross
Alec Gouss	Daniel Kerlakian	Serge Masters	Innokentii Panteleev	James Rothe
Jon Grady	Kiratbir Khurana	Nicolas Mathurin	Tracie Parauda	Ilana Rothkopf
Christian Graham	John Kiremidjian	Douglas Mattei	Rajas Pargaonkar	Michael Rowan
Wendy Grant Mungroo	Paul Kirwan	Lucy Matthews	Kristin Parker	Mali Ruan
Deborah Greenway	Toni Knadle	Ryan May	Nilesh Patel	Carlos E. R. M. De Ubago
Harold Greer	Christopher Kovaly	Frances Mccall	Jasmine Patel	Anis Salah
Sergei Gremeniuk	Genevieve Kozlowski	Kristine McCormick	Audra Patrick	Vincent Salamon
Mikael Grigoryan	Hannah Kressler	Alyssa McCoy	Jason Paul	Brandon Salese
Kimberly Gross	Melanie Kring	Wendy McMillan	Janisha Paul	Philip Sam
Phillip Grubaugh	David Kroonblawd	Keshma Mehta	Kristen Paulish	Vasudha Sanghani
Kevin Guanaga	Agnieszka Kucharska	Wafa Mejdoub	Aristidis Pavlatos	Grace Sare
John Guest	Samuel Kyeremeh	Lorena Melcher	Fidel Pena	Darren Sawicki
Yvan Guiatheu	Manohar Lakshman	Sherwin Mendoza	Ana Peraza	Yolanda Scharf
Eric Hains	Matthew Lau	Karen Messer	Kimberly Perkins	Brian Schaumburg
David Hajec	David Lau	Dale Metoff	Robert Perry	Lori Schlatter
Michael Hammer	Fui Ling Law	Danielle Miller	Roberta Peterson	Soledad Schneegans-Cano
Caira Hane	Mily Lawrence	Christine Miller	Vanessa Pham	Gary Schweers
Christine Hang	Betsy Lawson	Bryan Miller	Benjamin Pierce	Ryan Schwoebel
Jessica Hanger	Jonathan Lee	Robbin Mitchell	Michael Pietrobon	Trevor Scott
Atsushi Harada	Melissa Leeds	Nikhil Mittal	Amareshita Pillalmarri	Ramiro Serrano-Garcia
Justin Hardin	Frank Leon	Rashmi Mogali	Hector Pineda	Suzanne Shaffer
Ryan Hardy	William Leopold	Cesar Monteverde	Nicole Pirz	Terence Shanahan
Keara Harman	Diego Letona	John Mooney	Jeffrey Pittman	Nishant Sharan
Courtney Harris	Ross Levin	Raymond Moore	William Ponce	Larry Sharon
Emmanuel Hayble-Gomes	Margaret Lewandowski	Michelle Morris	Heidi Ponder	Daniel Shin
Andrew Hayes	Juanita Lewis	David W. Morris	Ryan Pool	Lee Ann Sholansky
John Hegarty	Ron Leybovich	Yasmin Motivala	Rachel Posner	Yashika Shuman
Lishomwa Henry	Sin Ming Anita Li	Craig Motsinger	Cynthia Pow Chon Long	Matthew Shustrin
Dayana Hernandez	Hui Li	Susan Mowery	Aaron Powell	Jeffrey Silaggi
Henry Hernandez	Ruby Liao	Garikai Mparutsa	Leslie Powell	Rick Simon
Nicholas Hess	Lindsay Lightmas	Samantha Mucha	Kevin Pruitt	Victor Simonetti
Sheila Hilton	Hui Lin	Soumendu Mukhopadhyay	Philip Pyburn	Andrea Simpson
Michael Hodson	Thanh Lindboe	Jayalakshmi Mummidi	Sheleby Queen	Tiffany Sizemore
Erin Hoffinger	Elizabeth Lindenbaum	Simeon Munezero	Ellen Queen	Robert Sloan
Lawrence Hoffman	Lauren Linder	Shashi Munikrishna	Casey Ragsdale	Richard Smit
Michael Holle	Mark Lingafelt	Michael Murphy	Rasheed Raji	Amy Smith
Cynthia Holloway	Mariusz Lipinski	Mary Murray	Rajesh Ramachandran	David Smith
Rex Holmes	Emma Lofradez	Kieran Murray	Patricia Ramcharran	Stephanie Smith
Gregory Homayoon	Kathryn Lofy	Noah Muwanika	Charles Randall	Bradley Smith
Katherine Horneff	Brandon Lomba	Caresse Myers	Bharath Ranganathan	Janet Smithson
Ryan Hough	Brenda Lopez	Andrew Neilson	Stephanie Rangel	Ashley Smyk
Jaclyn Hrcirik	Cynthia Lopez	Casey Nelson	Hubert Recana	Scott Smylie
Jessica Hughes	Stephen Lord, II	Marcia Nesbeth	Kellen Reed	Jeffrey Snow
Jo-Ann Humphrey	David Lorio	Kevin Neville	Michelle Reed	Arthur Soule
Rebecca Hurley	Stuart Lott	Jacinth Newman	Cassandra Remmel	Denise Spada
Nnamdi Ihekaram	Stephen Lowery	Yuk Mei Ng	Barbara Renfro	Franklin Staker
Fabricio Ikeda	Paul Lucas	Johnny Ngai	Andrew Resnick	Crystal Stall
Petar Iliev	Saudhi Lugo	Pedro Nicasio	Jennifer Reynolds	Joseph Stephenson
Olapade Ilori	Yi-Ting Ma	Erica Nielsen	Marissa Riani	Lisa Sterenchuk
Seth Isom	Carla Mabry	Nancy Niro	Jonathan Rieth	Robert Stevener
Jesus Izquierdo	Elizabeth Macro	Katsiaryna Nissan	Tiffany Riggs	Daniel Stockwell
Gina Jacques	Carolyne Madison	Krista Noll	David Rios	Annelise Strader
Maren Jaffee	Stephen Maggiore	Debra Noll	Erika Rios	Leya Strauss
Rab Jafri	Molly Major	Etienne Nortje	Collen Ritchie	Erin Strauss
Marie Jago	Aniket Majumdar	Sheryl Nosel	Lisa Ritter	Adam Strawbridge
Timothy Jankow	Monica Mak	Boris Novikov	Pablo Rivera	Tallie Stubbs
Carissa Jefferis	Kamesh Mamidipudi	Christopher Nowak	Michael Riviezzo	Ivy Suryasentana
Jingshan Jiao	Ashley Mancuso	Courtney Nowlan	Marisa Rizzo	Noah Susskind
Mary Johnson	Thia Mandal	Sam Nyachwaya	William Roberts	Elaine Swartze-Campbell
Laura Johnson	Guido Mangione	Dora Nyantekyiwah	Ryan Roberts	Reid Swayze
Mary Joldersma	Joseph Manning	Robert O'Callaghan	Christina Robertson	David Szerlip
Erinn Lachner Jones	Sreela Manoj	Sun Oh	Anthony Robinson	Karim Tadjer
Harvey Joseph	Tippian Manske	Hiromasa Okada	Rachel Robinson	Ravit Tal

Louis Tan
 Mark Tawfik
 Jared Terry
 Zac Thaliath
 Brian Thomas
 Shane Thomas
 Kelci Thomasco
 Steve Thompson
 Eric Thomson
 Julie Thurber
 Clifton Tice
 Erin Tiernan
 John Tobon
 Monica Tourish-Hunter
 Karl Towns
 Junko Trainor
 Carly Tran
 Osvaldo Trujillo-Loza
 Edem Tsiagbey
 Jonathan Turnbull
 Brooklynn Turner
 Dana Twomey
 Jan Tyda
 Robert Vaccaro
 Rey Valdes
 Jesus Valdez
 Darla Van Mil Kime
 Geetha Vishwanathan
 Julieta Vital Garay
 Justin Von Stroh
 Daniel Wallace
 Lucas Wallis
 Andrea Walser
 Latoya Walter
 Jennifer Walter
 Katherine Walters
 Melanie Walther
 Donna Walthers
 Chun-Jui Wang
 Pei-Chen Wang
 Elsie Wang
 Kristine Washburn
 John Waugh
 James Wawrzaszek
 Gabriela Webber
 Daniel Weckesser
 Sharon Weiner
 Kimberly Wells
 Karen Werner
 Nicholas Werve
 Tanya White
 Sandra Whited
 Nicole Whitsel
 Brendan Whyte
 John Wiethorn
 Aaron Wilcutt
 Keum Woo
 Alexander Wozniak
 James Wrenn
 Jessie Xie
 Jinyan Yang
 Turgut Yasar
 Victoria Yeh
 Bryan York
 Stacey Zagata
 Kellyn Zamora
 Kevin Zeng
 Tao Zhang
 Nicole Ziober
 Stanley Zon

Francia

Elodie Anguissa

Laura Daudin-Antoine
 Loic Kervran
 Kristopher Poulton
 Ravinder Sachdeva

Ghana

Davis Adu Amponsah
 Clement Asiamah

Grecia

Tatiana Anastassiadi

Hong Kong

Priyanka Bordia
 Carlie Cheuk Ying Chan
 Shirley Chan
 Chee Ching Chan
 Tsz Yuen Chan
 Hong Chan
 Ivan Tsz Wun Chan
 Chi Ho Chan
 Ka Wo Kelvin Chan
 Surendra R. C. Nagavenkata
 Chung Yan Cheng
 Kenneth Cheng
 King Yu Cheung
 Ka Ming Chiang
 Sonny Chu
 Timothy Dang
 Boran Demirdag
 Mustafa Gungor
 Thomas Hill
 Wui Ho Howard Ho
 Yuk Yan Anthea Kan
 Kin Yip Kong
 Ching Yan Kwan
 Chak Long Kwok
 Hoi Yan Kwok
 Kit Wah Freda Lai
 Kiki Chun Wa Lam
 Chris Lam
 Sin Kin Lam
 Wing Yu Regina Lam
 Suet Ying Chelsey Lau
 Wai Ho River Lau
 Wilson Lee
 Man Wa Lee
 Ka Wing Carol Leung
 Tsui ShanTracy Li
 Hoi Chuen Li
 Ka Ying Li
 Ngung Lee Liew
 Kwan Liu
 Laura Liu
 Wai Man Luk
 Wing Pui Ma
 Ricky Ma
 Wing Ho Ma
 Kin Wai Mak
 Karen Wing Ka Mak
 Ka Wai Man
 Michael Mason
 Claire Massot
 Urszula McCormack
 Oonagh M. -Hutchinson
 Natalie Mok
 Yau Kit Eric Ng
 Kennix Ng Hau Ling
 Chi Pan
 Yu Grace Peng
 Wade Ryan Roos
 Julien Sery

Teariki Short
 Mei Ting Stephenie So
 Chung On Tam
 Li Ann Tan
 Vicki Tang
 Mémouna Traoré
 Chun Wai Tsang
 Michael Tse
 Tony Tse
 Maria Tsolaki
 Cheuk Man Ryan Tsui
 Nicholas Turner
 Ka Wing Wong
 Grace Tsai Wong
 Louis Wong
 Wun Man Mandy Wong
 Yu Ching Queenie Wong
 Yihua Wu
 Tsz Chun Wu
 Xin Xin
 Sin Man Yam
 Lu Yan
 Edwin Yau
 Wendy Yeung
 Yan Wing Yip
 Ko Chi Yuk

Hungría

András Bácsfalvi
 Eugene Kolesnichenko
 David Lewis
 Marton Szendrei
 Peter Toth
 Luke Van Boeschoten

India

Abhishek Abhishek
 Mitesh Agarwal
 Yogesh Agrawal
 Rohit Arora
 Sampath Balivada
 Vartika Bansal
 Nikhila Beju
 Anurag Bhargava
 Gaurav Bhoot
 Jain Bhuwan
 Krishnendu Biswas
 Paryant Buch
 Abraham Charles
 Kokila Damodaran
 Pawan Daryani
 Nagpal Falak
 Dhruvil Gaglani
 Shobhit Garg
 Manoj Gaur
 Nitha Geetha
 Sayan Ghosh
 Madhuri Gosai
 Veeren Gudhka
 Pinasree Halder
 Atharv Inamdar
 Sridevi Jayanti
 Ashish Jhaver
 Adarsh Kidiyoor
 R Kirubakaran
 Thulasi Kumar
 Yash Kumar
 Kundan Kumar
 Binay Kumar
 Shailendra Kumar
 Palangi Satish Kumar
 Neha Madan
 Meena Madhavan

Uma Maheswari V.
 Xavier Michael Raj
 Ramya Mudaliar
 Kingshuk Mukherjee
 Maheswaran Muthiah
 Naveen Nagamanickam
 Arun Navaneethan
 Sowmya Palayil Sivasadas
 Rohit Pandey
 Ameya Panse
 Vishal Parikh
 Ramaswamy Ponnappalli
 Panda Prakash
 Amitabh Prasad
 Arif Quraishi
 Ratna Kumar R.
 Sareen Rahul
 Venkatasubramanian Raja
 Senthil Rajasekaran
 Vallamchitti Srinivasa Rao
 Prankur Rastogi
 Prasenjit Roy
 Pornali Roy
 Tanuja Reddy Sadi
 Vardan Sharma
 Peeyush Sharma
 Vinutha Shivakumar
 Anshu Singh
 Sameeksha Sinha
 Srikanth Sirigidi
 Davidson Sirra
 Ranjan Dash Souravi
 Aditi Thakur
 Milind Tiwari
 Jagadish Upadrasta
 Sonali Vaidya
 Shwetaketu V. Jha
 Srinivas Vernula
 Vinay Vincent
 Vishwas Vishwas
 Suresh Voolala
 Rajendra Singh Wadhawa
 Sachin William

Iraq

Mustafa Abbas Abd Ali A. Ali
 Husham K. A. Al-Al-Dulaimi
 Mustafa Jawad Malk Alridha
 Mays Najm M. Al-Hasani
 Hayder Sabah M. Ridha

Irlanda

Federico Gaffney
 Michelle Guiney
 Shane Howe
 Gabby McMahan
 Deirdre Williams

Islas Caimán

Allain Forget
 Kendra Foster
 Regina Oliver
 Soraya Taylor

Islas Vírgenes Británicas

Nedy Ador Dionicio
 Alecia Brookes
 Pedro Castellanos
 Casey Gumbs
 Raven Kelly

Israel

Adam Shalov

Jamaica

Rushane Ellington
 Marcia Jackson
 Diana Sirila

Japón

Jonathan Ell
 Daisuke Fujiwara
 Jonathan Gallimore
 Tomohiko Hirano
 Yuichi Hirose
 Taeko Hori
 Koichi Imamura
 Maika Irie
 Shuji Ishida
 Yuhiko Kaji
 Shinjiro Kakihara
 Takashi Kato
 Hideki Koyanagi
 Nobuhiro Matsumoto
 Kanako Murata
 Ryo Nagao
 Yuki Nakano
 Yoshiyuki Nonomura
 Masashi Ono
 Jun Osumi
 Mikako Owaki
 Shinichi Sano
 Eiji Sato
 Hitomi Shimizu
 Kazuhisa Suzuki
 Koichi Takano
 Ryo Takebe
 Tomokazu Tanigawa
 Junko Tashiro
 Miki Yamagami
 Keigo Yasuda

Jordania

Mohammad J. A. El-Fattah
 Abdulla Foad Abdalamer
 Banan Ali Abu Shawareh
 Mohammad Issa A. Sheikha
 Rasha Ibrahim Abujabal
 Abdel Rahman A. Al Rbeihat
 Rawan M. A. Al-Amayreh
 Ali Adil Aidi Alhaggag
 Ehsan Nadeem Al-aref
 Rema Issa Albalbout
 Mohammed I. M. Al-Dabbas
 Zainab T. A. Almandalawi
 Walaa Zeyad Al-Madadha
 Hanan Hisham Al-Matlaq
 Alaa Atef Alshalaldah
 Haitham Rebhe Alyousef
 Ala Bashir Bqain
 Shereen Kamal Ghayada
 Shaden Khaleel Ghuneim
 Mohaned Zaki Hamdan
 Sami Juwinat
 Athraa Nadhim Khalaf Saedi
 Mohamad Khaled Alsmadi
 Ahmed Adnan Marie
 Odai Sameer Masoud
 Mohanad Farhan M. Alomari
 Abedalaziz N. Gharaibeh
 Jack Anis Neno
 Heba Mohammad Rababh
 Rania Rumman

Ali Saleh
Ala'a Ayman Shaban
Khalidoun Jaser Tadros
Mo'ath Abdel Wahab Alkurdi
Martha Khalil Zomut

Kazajstán

Nelly Adilshenova
Balnur Balkhozhayeva
Gulzhiiyan G. Aubakirova
Assel Iskuzhinova
Guldana Mukasheva
Vyacheslav Pak

Kenia

Evelyn Atsiambo
Nancy Wawasi Mrashui

Kuwait

Khaled Al-Foudari
Tamer Mohamed Hosny
Ibrahim Shahin Weza

Letonia

Natalja Buceniece
Mārtiņš Puķe

Libia

Aida Abdulla Dourda
Nezar Ben Naser M. AlBskine
Mahmud Ali ElAshgar
Ayad Hamouda
Omer Abdalla Magur
Mohamed AB. O. AlMahrouq
Faraq Mohamed Shamata

Lituania

Vilius Lukauskas

Luxemburgo

Jose Maria C. Donderis
Thomas Duche
Evelyn Holzeis
Florence Moreau
Stephen Zorn

Macao

Meng Kit Cheong
Hou Fai Chio
Wanting Huang
Keng Fai Lai
Meng Ying Li
Jiayi Li
San Sou
Xunzhou Wu

Malasia

Anita Soraya Adlan
Siti Nabilah Ahmad Azhar
Melvin Chew
Guan Ee Ling
Yi Mei Khoo
Lim Mei Lin
Nalini Sundaraj
Jose Thottungat

Malta

Anna Camilleri

México

Fernando Andres Lapajne
Luz María Villafuerte García

Montserrat

Michael Joseph

Morocco

Bouchra Naim

Namibia

Emmanuel Murwira

Nigeria

Akinjide Abegunde
Olanrewaju Adesomo
Oladele Asanmo
Frances Diribe
Samson Falade
Matilda Obigho
Nwamaka Obi-Obueze
Mobolaji Obisakin
Abdullahi Salami
Ijeoma Uzowuru

Nueva Zelanda

Dilawar Arbab
Jamil Guliyev
Benjamin Raggett
Christina Wang

Omán

Zainab Ali Malalah Al Lawati

Países Bajos

Marianne Scholtens
David Smit
Hilde van den Hoven
Aart-Jan Jacobus van Strien
Daphne Voorrips
Petronella Vriend

Pakistán

Rahim Rajab Ali
Qazi Furrukh Saleem
Saddam Hussain
Khalid Pervaiz
Shah Zeeshan Rafiq
Nida Shahbaz

Palestina

Rola Mansour
Rewa Taneeb

Polonia

Aleksandra Dana
Janina Galica
Dorota Gujska
Malgorzata Kabat
Alan Piechota
Artur Cezary Porowski
Agnieszka Stanczak
Aneta Szmids
Oleksii Vengerskyi
Krzysztof Wadynski
Iwona Wasilewska
Adrian Zurek
Iryna Ziyatyk

Puerto Rico

Rene Vazquez

Qatar

Hesham El Kurdy
Padmashree Ramachandran
Srikanth Srivatsavaya
Jharna Vaid

Reino Unido

Mudassar Abbasi
Daniel Omoniyei Afilaka
Olu Alli
Tina Amahson
Jose Arevalo
Himanshu Bajaj
Frederick Barber
Sam Cox
Harriet Denvir
Warren Deweltz
Olga Dias
Simon R. Dilloway
Susana D'Souza
Narasimha Eday
Pavel Esin
Cyril Esterhuysen
Muhammad Faisal
Carlo Gallo
Radiat Giwa
Andrea Gregory
Gary Holmes
Ivana Hostickova
Mary Ighekpe
Martin Jones
John Paul Jones
Frederic Jubin
Hee Jung
Hamad Khalid
Juelin Lee
Thomas Lee
Linda Siao C. Li Sheung Ying
Ran Ran Liang
Mark Marthinus
Nanda Mayampurath
Malachy Mcclelland
Ian McCormick
Kyle McMullan
Clive Mitchell
Olayinka Oluwasola
Lam Lam Janny Or
Nick Oskiewicz
Elaine O'Sullivan
Sharney Planner
Marc-Andre Poisson
Mariya Radeva-Gaye
Brian Rosner
Parminder Samrai
Marc Scarisbrick
Sho Suzuki
Margo Vakharia
Rosamaria Valentini
Yulia Vashchuk
Andrey Vatulin
Hugo Williamson
Malgorzata Williamson
Lyndsi Witsaman
Piotr Wojtowicz

Republica Democrática del Congo

Henri Faizi Auni

San Cristóbal y Nieves

Giselle Clarke-Theron
Kalindi Liburd
Suzy St. Brice
Marthford Thomas

Serbia

Milan Vlah

Seychelles

Deoraj Puddoo

Singapur

Alexchandar Anbalagan
Merion Anggerek
Marianne Azavedo Pereira
Ashwin Balaram
Neeraj Bansal
Raymond Bosker
Genevieve Sarah Brunner
Qing Hong Cai
Malgorzata Cegiela
Ee Chau Long
Fu Kwang Derek Chee
Yannick Cheral
Kryssa Chia
Zhen Wei Roy Chia
Kerry Chin
Su-Chian Chio
Andrew Choo
Si Wei Colin Chua
Sin Yee Diong
Seet Lai Ee
Lai Kuen Sherin Han
Mohit Handa
Richard Hanmer
Edwin Hoi
Kuok Hui Mei
Pitale Jay Vijay
June Khoo
Wang Kin
Yin Tin Koay
Tomoaki Kubo
Manoj Kumar
Arundas K. Bhuvanadasan
Anne Kynigos
Meryl Lau
Yan Ling Grace Lee
Kit Tzin Leong
Choy Yin Leong
Weiquan Li
Huiping Lim
Han Seong Ethan Lim
Ruiliang Lin
Keri Low
Robert Mahoney
David McGee
Rafe Mohamad
Sanjay Namasivayam Pillai
Kae Bin Eugene Ng
Wai Ling Ow
Rui Qin Poh
Tarini Ponniah
Wei Ming Edmund Poon
Hansel Quek
Muneeba Quraishi
Rika Sahara
Jayashree Satish Iyer
Shu Jie Seow
Jonathan Seror
Samira Shafiqi

Gyan Chandra Sharma
Pei Ru Soh
Vijayalakshmi Sundaram
Ikuko Takahashi
Jia Qi Tan
Chee Seong Tan
Sharon Ying En Teng
Sharath Mandara Vasudeva
Meera Vinodan
Liang Ern Milton Wong
Wong Ye Cheng
Kien Choong Yeong
Yessy
Zhang Yun

Sri Lanka

Nishan Jesudason

Sudáfrica

Jacques Mey

Suecia

Johanna Fagerström

Suiza

Karl-Leung Cheung
Emmanuel Eneme

Tailandia

Abigail Hope Serrano

Taiwán

Ya-Ting Chang
Wei-Hsuan Chen
Mei-Ju Chen
Wan-Ting Cheng
Chia Chi Cheng
Jung Lun Tomm Chiang
Shih Po Hsu
Yu-Fen Huang
Bob Huang
Aaron King
Wenchun Lin
Pei Je Luo
Winkie Wing Kun Ngan
See Inn Ong
Yuying Shang
Ivan Sun
Yuan Chi Wu

Trinidad y Tobago

Nikieshia De Bique
Nathalia Nasib-Cletus
Nicole Patrick

Turquía

Serkan Arslan
Ahmet Selim Demirtaş

Venezuela

Nahyr Gonzalez Quiroz

Vietnam

Thong Duong

Zimbabue

Shenjere Talent Zviedzo

YOUR AD HERE

Don't miss your opportunity
to reach a readership of over
38,000 AML professionals

TO ADVERTISE HERE CONTACT:

ANDREA WINTER

1.786.871.3030

AWINTER@ACAMS.ORG

