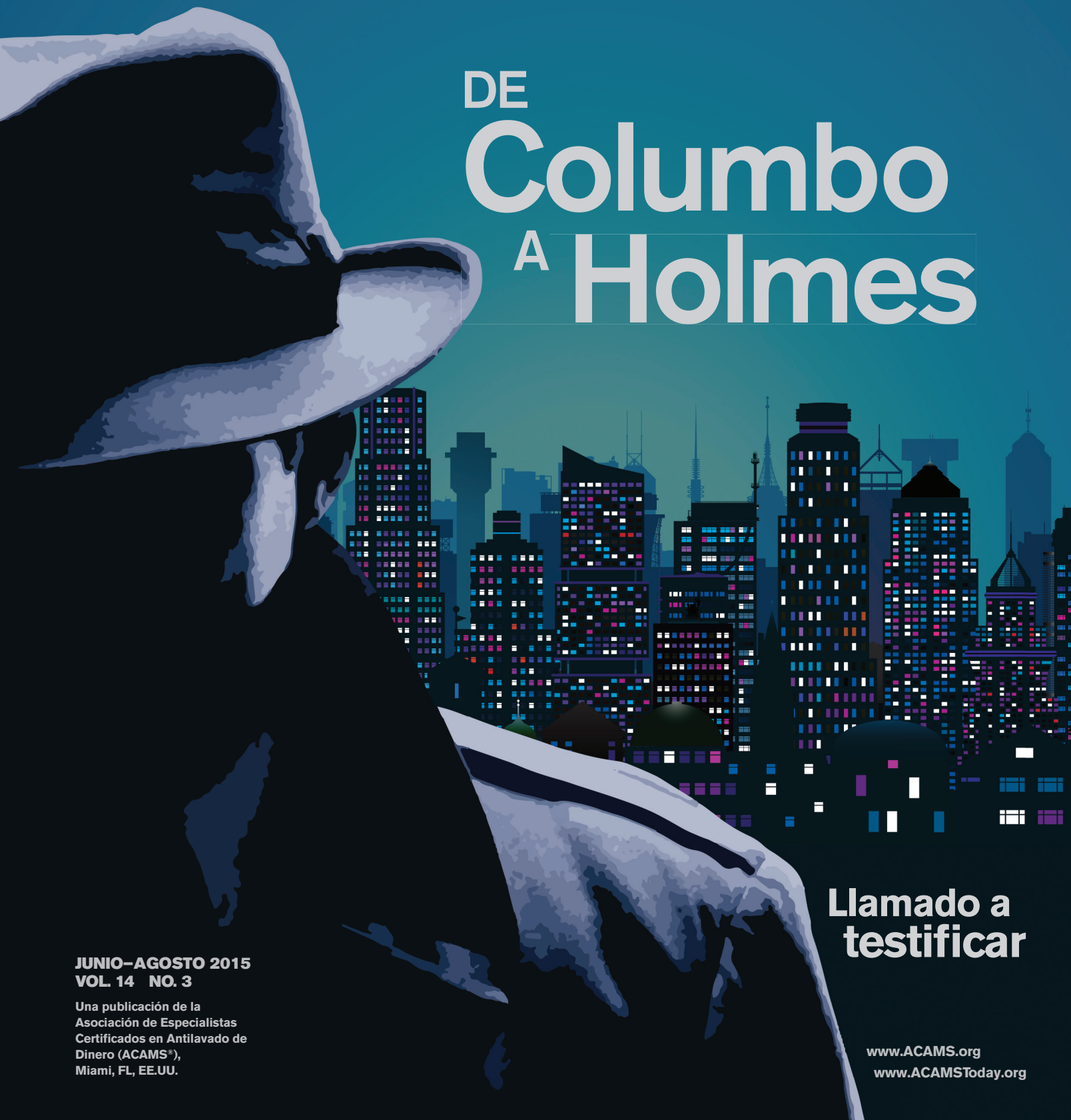
QUINTA EDICIÓN DE LA APLICACIÓN DE LA LEY

ACAMS® TODAY

La Revista Para los Profesionales en el Campo Antilavado de Dinero



DE Columbo A Holmes

Llamado a testificar

JUNIO–AGOSTO 2015
VOL. 14 NO. 3

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

www.ACAMS.org
www.ACAMSToday.org

ACAMS Advanced Certifications

Taking you beyond the Certified Anti-Money Laundering Specialist (CAMS) credential to an elevated level of education and practice.

ACAMS is certifying the advanced knowledge and skills of the CAMS community worldwide.

The Benefits of CAMS-Audit:

- Fulfill regulatory expectations.
- Safeguard your institution and prepare for examinations.
- Experience professional growth.

The Benefits of CAMS-FCI:

- Bridge the law enforcement communication gap.
- Improve the efficiency and effectiveness of your investigations.
- Reach new professional heights.

Email **advanced-cert@acams.org** for more information.

You must be CAMS certified in order to apply.

CAMS AUDIT

ACAMS® Advancing Financial Crime Professionals Worldwide®

CAMS FCI

DOW JONES

AVOID
RISK-INFESTED OPPORTUNITIES

In a sea of complex relationships and hidden dangers, Dow Jones Risk & Compliance helps you assess, investigate and monitor high-risk situations. We provide an exclusive content set, market-leading tools and due diligence reports to help keep your company in the clear. So you can dive right into business decisions—fearlessly.

dowjones.com/risk

RISK & COMPLIANCE
Know What You're Getting Into.

ACAMS® TODAY

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

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

Para asociarse o publicar anuncios publicitarios, contactar a:
ACAMS
Brickell City Tower
80 Southwest 8th Street, Suite 2350
Miami, FL, 33130

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

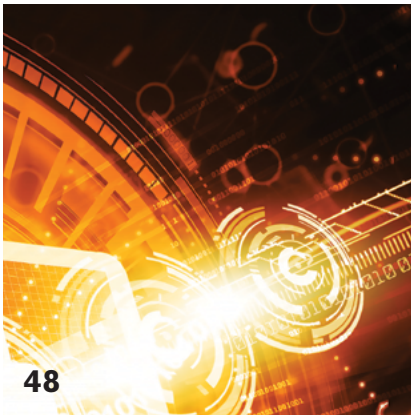
Fax 1-305-373-5229 ó
1-305-373-7788

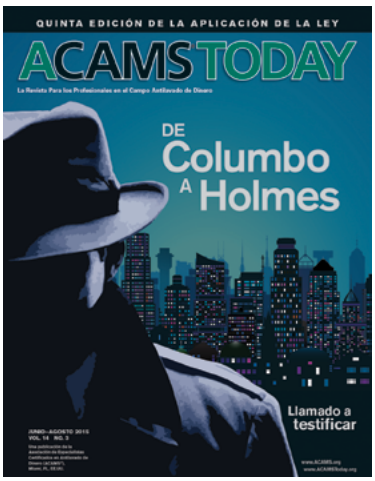
E-mail: info@acams.org

Internet:
www.ACAMS.org
www.ACAMSToday.org

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

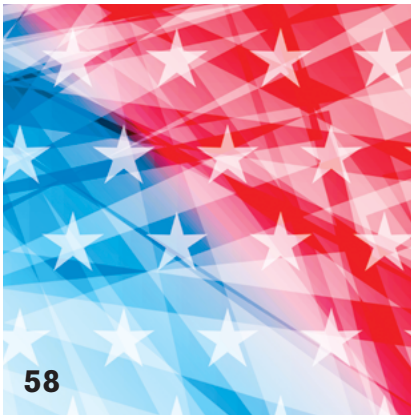
Contenido

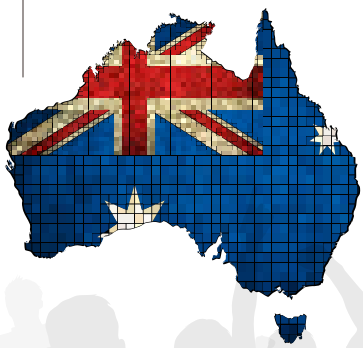




EN LA PORTADA

Ilustración de la portada por: Victoria Racine





Cómo se forma un gran investigador

¿Qué hace que un investigador sea genial? Si tuviéramos que crear un personaje, ¿qué rasgos tendría él o ella para acceder al panteón de los grandes detectives? O, para decirlo en términos más personales—para aquellos de ustedes que se esfuerzan por la grandeza en calidad investigativa—¿Qué rasgos se necesitan para lograr ese objetivo?

Para empezar, la definición de investigar se refiere a llevar a cabo una investigación sistemática o formal para descubrir y examinar los hechos de un incidente, denuncias, etc., a fin de establecer la verdad. Lo primero entonces para un investigador es ser sistemático. El objetivo final consiste en descubrir la verdad, y al seguir procedimientos el investigador puede estar más seguro de que no faltan detalles importantes, ya sean exculpatorios o inculpatorios. Una barra lateral de este primer requisito es que el investigador tiene que estar siempre vigilante en cuanto a los detalles. Los procedimientos y sistemas sólo funcionan en la medida en que el investigador presta atención a todos los hechos y a la información reunida y los mantiene en forma ordenada.

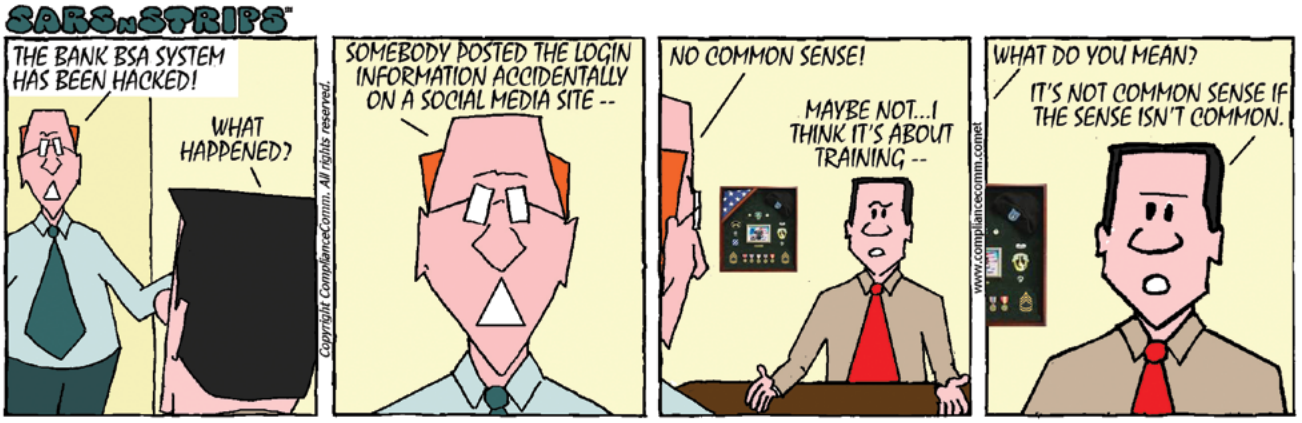
Lo segundo que necesita un investigador es la capacidad de descubrir los hechos pertinentes a su objetivo de descubrir la verdad. Los hechos y datos pueden reunirse en una variedad de maneras. Un investigador tiene que entender la utilidad y la eficacia de las herramientas individuales que se pueden emplear en la recopilación de estos datos. Con el fin de hacerlo, un investigador tiene que estar entrenándose constantemente con estas herramientas y en constante aprendizaje sobre los avances y desarrollos de otras herramientas.

Por último, a raíz de la definición anterior, el investigador tiene que examinar la evidencia. La recopilación de datos es relativamente fácil en el entorno electrónico en el que vivimos. El gran investigador es aquel que ha desarrollado la capacidad de examinar y entender lo que dicen los datos. El investigador tiene que eliminar los datos engañosos y centrarse en lo que es pertinente. El investigador tiene que tomar los pedazos de datos dispersos, contextualizarlos y darles significado. Nuestro artículo principal, *De Columbo a Holmes*, toma características diferentes de los detectives de ficción y da ejemplos de cómo estas características podrían resultar beneficiosas para el investigador de la vida real.

Lo que es más, esta es nuestra quinta edición sobre autoridades de control legal y me complace decir que hay una gran cantidad de artículos informativos y perspicaces que arrojan luz sobre el papel de las autoridades de control legal, las asociaciones importantes entre los sectores público y privado y mucho más.

Por último, me gustaría compartir con todos ustedes una buena noticia. En abril lanzamos nuestra nueva y mejorada página web ACAMSToday.org. Espero que todos ustedes se tomen el tiempo de leerla, ya sea en la edición impresa o la edición en línea en nuestro nuevo sitio web móvil amigable.

Karla Monterrosa-Yancey, CAMS
jefa de redacción



Producido por: ComplianceComm

With principles-based **SAFE Advanced Solutions®**, SBS closes gaps left by rules-driven anti-money laundering systems.

Rules are well-defined, predictable and orderly. The data they process is not. That's why real-world scale, scope and uncertainty — the Achilles' heel of traditional rules-based AML systems — are no match for SBS' patented risk-ranking methodology and powerful alert scoring model.

Using data-driven technologies that emulate human judgment, SAFE Advanced Solutions brings entity resolution to a new level. It provides a hierarchy of risk that identifies the most relevant and highly probable matches.

SAFE Advanced Solutions eliminates false negatives and greatly reduces false positives. All while delivering the lowest hit rates imaginable.

Learn how our principles-based approach to AML finds the bad guys that other systems miss. Contact **sales@safe-banking.com** or call us at **+1 631-547-5400.**

SBS®
SAFE BANKING SYSTEMS

www.safe-banking.com

Michael Amo, CAMS
Nueva York, NY, EE.UU.

Michael Amo se encuentra contratado por Promontory Financial Group cumpliendo una variedad de cargos relacionados con la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) en funciones de regulación y cumplimiento en instituciones financieras internacionales y nacionales con una especialización en control de las transacciones de la Oficina de Control de Activos Extranjeros (OFAC), la evaluación de riesgos, conozca a su cliente (KYC) y el entrenamiento.

Antes de ocupar su cargo actual, fue consultor de varios bancos internacionales en virtud de órdenes de consentimiento, y proporcionó una gama de servicios debido a su experiencia en el tema de ALD, con énfasis en las iniciativas de la banca corresponsal.

Amo ha adquirido una sólida base de servicios financieros y experiencia bancaria durante toda su carrera y ha alcanzado certificaciones sobre valores y seguros, siendo la más reciente, la designación de CAMS. También es miembro del comité de evaluación del contenido y clasificación del programa de la Certificación Avanzada de Investigaciones de Delitos Financieros de ACAMS (CAMS-FCI) y tiene una licenciatura en finanzas de la Universidad de Florida.

Zach Miller, CAMS-FCI
Harrisburg, PA, EE.UU.

Zach Miller es el gerente de operaciones (oficial adjunto de BSA) de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) de Metro Bank, una institución de banca minorista en el centro sur de Pensilvania. Miller se encarga de gestionar las investigaciones de ALD, la presentación de reportes de operaciones sospechosas (ROS), diligencia debida mejorada (EDD), el informe de transacciones en efectivo, las operaciones de la Oficina de Control de Activos Extranjeros (OFAC) y las áreas del sistema de negocios de ALD que incluyen la supervisión, dirección y orientación del equipo de ALD del banco y la interactuación con las autoridades de control legal, el personal regulatorio y de auditoría.

Miller también es responsable de los esfuerzos de entrenamiento de ALD del banco, que facilita a través de diversos tipos de métodos de entrega que alcanzan a toda la organización. Tiene seis años de experiencia en el área del ALD y ha servido como analista y especialista en control de calidad de ALD para el Metro Bank antes de asumir su cargo actual en noviembre de 2012.

Miller obtuvo su certificación de CAMS en junio de 2011 y la certificación avanzada de CAMS-FCI en agosto de 2014. Antes de comenzar su carrera en el sector de los delitos financieros, obtuvo su licenciatura de York College de Pensilvania. Además de ofrecer conferencias a nivel local, Miller participó recientemente como panelista en la *13ª Conferencia Anual de ALD y Delitos Financieros* en Las Vegas y en la *20ª Conferencia Internacional de ACAMS moneylaudering.com y de Delitos Financieros* en Hollywood, FL.

Samuel Chukwuka Onyeka, CAMS
Abuja, Nigeria

Samuel Chukwuka Onyeka lidera la Unidad de Antilavado de Dinero/Financiamiento del Contraterrorismo (ALD/CTF) de la Dirección de Inspección de la Comisión Nacional de Seguros de Nigeria. Con más de 20 años de experiencia en derecho, seguros y gestión de riesgos, Onyeka es, sin duda, uno de los principales referentes en el sector de seguros en Nigeria. Tiene tanto una Licenciatura como una Maestría en Derecho de Abia State University y una Maestría en Administración de Empresas (seguros y gestión de riesgos) de Enugu State University. Además, accedió al Colegio de Abogados de Nigeria en 1991.

Su carrera en el sector de seguros se inició en 1991 como oficial de reclamaciones del National Insurance Corporation de Nigeria (ahora NICON Insurance Limited). También trabajó para Unity Life & Fire Insurance Co. Ltd y más tarde, la Admiral Insurance Co. Ltd, donde llegó a ser director del Departamento de Motores en 1994. En 1995 abandonó el negocio de seguros temporalmente para involucrarse en la práctica jurídica activa y el mundo académico. Dictó clases sobre derecho y seguros en Imo State University hasta 2009 cuando pasó a la Comisión Nacional de Seguros.

Fue admitido como Miembro titular del Chartered Insurance Institute de Nigeria en 2011 y Miembro de la Asociación Nacional de Comisionados de Seguros (en los EE.UU.) en 2012. Se convirtió en asociado senior de la Asociación de Gerentes de Riesgo de Nigeria en 2013.

Con base en su experiencia y la calidad de sus contribuciones para mejorar la cultura del ALD/CTF en Nigeria, fue nominado, en 2010, miembro del Comité Presidencial de Nigeria del Grupo de Acción Financiera. Actualmente es copresidente de la Secretaría de la Evaluación Nacional de Riesgos (NRA) de lavado de dinero/financiación del terrorismo (ML/FT) de Nigeria.

Viajero consumado, Onyeka ha asistido a varios seminarios, talleres y conferencias regionales e internacionales sobre seguros, gestión de riesgos, ALD y delitos financieros. Onyeka ha publicado más de una docena de libros sobre seguros y otras disciplinas, el último de ellos titulado *Anti-Money Laundering and Combating the Financing of Terrorism in Nigeria* (*El Antilavado de Dinero y el Combate de la Financiación del Terrorismo en Nigeria*, en español). También ha contribuido con innumerables artículos a muchas revistas de especialidad locales, entre ellas la *Journal of Insurance Law* and *Practice* de la que funge como asesor editorial.

Greg Ruppert
San Francisco, CA, EE.UU.

Greg Ruppert es el jefe del grupo de Investigaciones de Delitos Financieros (FCI) de Charles Schwab Corporation, que abarca los programas de antilavado de dinero (ALD), la Oficina de Control de Activos Extranjeros (OFAC), la prevención del fraude y de investigación de toda la empresa.

Antes de unirse a Schwab en 2014, Ruppert pasó más de 17 años en el FBI. Más recientemente, fue un alto ejecutivo en la sede de Washington, D.C. del FBI, donde supervisó los esfuerzos de la División Cibernética para combatir las amenazas cibernéticas de mayor prioridad.

Ruppert comenzó su carrera en el FBI en la Oficina Local de Boston especializándose en fraude complejo corporativo y de valores, lavado de dinero, delitos financieros y fraude cibernético. También sirvió en el Grupo de Tareas de Enron como investigador principal asignado a investigar al director financiero de Enron y a otros funcionarios corporativos de alto nivel.

Ruppert también tiene experiencia en los esfuerzos antiterroristas del FBI. Dirigió un equipo, como parte de la investigación del FBI del 9/11, que dejó al descubierto las actividades financieras y fuentes de financiación del secuestrador. Posteriormente se incorporó a la Sección de Operaciones de Financiación del Terrorismo (TFOS) donde creó una unidad encargada de la investigación del terrorismo relacionada con el lavado de dinero y la recaudación ilegal de fondos basada en la caridad.

Ruppert también trabajó internacionalmente en La Haya, los Países Bajos y luego en Berlín, Alemania, donde dirigió una de las mayores oficinas internacionales de la FBI. Es también un miembro del Colegio de Abogados de California.

Se sigue reconociendo lo esencial que resultan las autoridades de control legal para el ALD efectivo

ACAMS se enorgullece de publicar la quinta edición de *ACAMS Today* dedicada a las autoridades de control legal. Para mí, la tercera de las tres patas del taburete del ALD (las instituciones financieras, los reguladores y las autoridades de control legal) es la clave para tener éxito en disuadir, presentar informes e identificar el lavado de dinero y delitos financieros. ¿Por qué tenemos estas leyes y reglamentos que se ocupan del lavado de dinero? Desde mi punto de vista, es para poner la información en manos de los hombres y mujeres que son autoridades legales, para que las investigaciones y procesos judiciales puedan proceder. La comunidad de ACAMS entiende este hecho y también reconoce los muchos desafíos que enfrentan las autoridades de control legal y esta edición cubre sólo una parte de esas áreas.

Por ejemplo, el abuso de los mayores es tristemente un problema para muchas familias a medida que la sociedad envejece y sigue frustrándonos a todos nosotros que los individuos se aprovechan de esa parte de la población. Hemos incluido un artículo sobre cómo responder a esta actividad en curso.

Con todo el caos en Oriente Medio y en el mundo, los practicantes del antilavado de dinero (ALD) ahora necesitan entender mejor la motivación y las acciones de los terroristas y esta edición contiene información sobre los llamados "terroristas nacionales".

Tenemos la suerte de tener un tipo de funcionarios de control legal comprometidos tan dispuestos a compartir consejos y orientación. Esta edición cuenta con un importante artículo sobre cómo realizar una entrevista y su importancia en las investigaciones de ALD. Otra parte de la historia del lavado de dinero es el uso de las leyes fiscales en el procesamiento de delincuentes. Paul Camacho nos remonta a la década de 1920 y explica cómo el infame gánster Al Capone fue aprehendido por la Oficina de Impuestos Internos (IRS) y sus agentes valientes.

Como todos hemos llegado a apreciar, los profesionales de ALD ahora tienen que estar bien versados en una variedad de áreas que van más allá del lavado de dinero tradicional. *ACAMS Today* se ocupa de ese desafío con artículos adicionales sobre la corrupción, las apuestas en el deporte y el problema abrumador de la seguridad cibernética.

No hay duda de que para tener éxito en el ALD en 2015, todos tenemos que ampliar nuestros horizontes legales y de cumplimiento—¡una meta hacia la cual nos esforzamos en cada edición de *ACAMS Today*!

Otra llamada a la razón con la "eliminación del riesgo"

Acabo de leer un anuncio de la Autoridad de Conducta Financiera (FCA) del Reino Unido que sin duda sugiere que puede haber acciones contra los bancos que salen de o se niegan a aceptar cuentas, debido a las preocupaciones del ALD. Mi primera, segunda y tercera reacción fue—"¿Hablan en serio?" Esta posición, junto con declaraciones similares (pero no tan potencialmente perjudiciales) de los reguladores de los EE.UU. confirma mi punto de vista de larga data sobre este tema: Las partes están hablando sin oírse y necesitan tener un diálogo informado sobre la manera de garantizar la "inclusión financiera" y deferencia a las instituciones financieras para que realmente puedan utilizar el "enfoque basado en el riesgo". El statu quo no puede permanecer. Nunca funcionarán las amenazas a las instituciones financieras que siguen afrontando las críticas reglamentarias más formales según las cuales deben aceptar todas las cuentas.

Recordemos que el ALD es sólo tan eficaz como la calidad de la información compartida o enviada a las autoridades de control legal. Los profesionales de cumplimiento necesitan orientación y asesoramiento. Si los que hacen las políticas quieren que las instituciones financieras tradicionales acepten depósitos de entidades de mayor riesgo, tienen que confiar en el proceso y los sistemas que se desarrollan, siempre y cuando las instituciones hagan lo mismo.

ACAMS Today recibe elogios

Finalmente, estoy orgulloso de anunciar que la Academy of Interactive and Visual Arts ha adjudicado *ACAMS Today* ocho Premios del Comunicador en el diseño y la escritura. Felicidades a Karla, su equipo y la fuerza de tarea editorial para este reconocimiento de 2015 de *ACAMS Today*.

John J. Byrne, Esq., CAMS
vicepresidente ejecutivo

Richard Weber:

Comprometido en la lucha contra la delincuencia financiera

ACAMS Today tuvo la oportunidad de entrevistar a Richard Weber, Jefe de Investigación Delictiva (CI), de la División de Servicio de Impuestos Internos (IRS), para hablar de lo que las instituciones financieras pueden hacer en la lucha contra las sanciones, la corrupción, el delito cibernético y mucho más.

Weber es responsable de investigar violaciones penales del código fiscal y delitos financieros relacionados. Con sede en Washington, D.C., Weber supervisa un personal a nivel mundial de casi 3.500 empleados del IRS-CI, incluyendo aproximadamente a 2.500 agentes especiales, responsables de la investigación de delitos relacionados con impuestos, lavado de dinero, corrupción pública, cibernética, robo de identidad, narcóticos y financiación del terrorismo.

Antes de emplearse en IRS-CI, Weber fue Jefe Adjunto de la División de Investigación y Director de la Oficina de Delitos Económicos Mayores en la oficina del Fiscal del Distrito de Manhattan. En este cargo era responsable de la gestión de fiscales, investigadores, analistas y asistentes legales que manejaban investigaciones de fraude de valores y productos, hipotecas y seguros de fraude a gran escala, esquemas de Ponzi, lavado internacional de dinero, financiación del terrorismo, evasión de sanciones, decomiso de activos y delitos fiscales.

Weber antes se desempeñó como Jefe de la Sección de Confiscación de Bienes y Lavado de Dinero del Departamento de Justicia, y como Fiscal Federal Auxiliar en el Distrito Este de Nueva York. Weber realizó numerosas grandes investigaciones y enjuiciamientos de lavado de dinero, entre ellos algunos de los mayores decomisos de instituciones financieras por violaciones de sanciones.

Además, Weber ha sido recipiendario, en dos ocasiones, del *John Marshall Award* (Premio John Marshall, en español) de la Procuraduría General, el más alto honor para abogados del Departamento de Justicia.

ACAMS Today: Al graduarse de la facultad de derecho, ¿sabía que quería tomar el camino de la prevención de los delitos financieros o fue más bien un crecimiento orgánico y por qué?

Richard Weber: Desde muy joven quería ser detective. Siempre me han gustado los programas de policías y fingir ser un agente. Así que me matriculé en la facultad de derecho para ser un Agente Especial. El camino me llevó a convertirme en fiscal y al principio de mi carrera empecé a trabajar en casos que involucraban seguir el rastro del dinero y los delitos financieros. Me gustó mucho el trabajo y me pareció muy gratificante y desafiante. Me encantó trabajar con agentes especiales y perseguir a los malos que cometen delitos de cuello blanco y quitarles las ganancias y bienes mal habidos. Respeto mucho a los agentes especiales que hacen este trabajo—son tan increíblemente hábiles y dedicados en buscar entre documentos voluminosos y armar un rompecabezas gigante con el fin de resolver el delito y conectar puntos. Un sueño mío cuando era fiscal era dirigir una agencia de autoridades legales y no puedo ser más feliz como Jefe de la mejor agencia de investigación financiera del mundo. Sinceramente ha sido un gran honor y privilegio servir como Jefe del IRS-CI durante estos últimos tres años.

AT: ¿Cómo hacen las instituciones financieras para detectar y reportar sobre delitos financieros y qué pueden hacer para mejorar?

RW: En su mayor parte, las instituciones financieras están haciéndolo muy bien en cuanto a la detección y denuncia de delitos y trabajando en colaboración con el gobierno. IRS-CI goza de una gran relación con muchas instituciones y rutinariamente tenemos foros de acciones bancarias donde se discuten las tendencias y las investigaciones realizadas. Los reportes de operaciones sospechosas (ROS) de los bancos son un valor añadido y una de las herramientas de aplicación de la ley más importantes que tenemos en nuestro arsenal.

Es claro para todos los que investigan delitos financieros que el mundo del fraude está en constante evolución para generar nuevas ganancias mal habidas y para evitar la detección por las autoridades de control legal. Las instituciones financieras desempeñan un papel fundamental en la detección precoz de nuevos esquemas diseñados para estafar y lavar dinero. Se han hecho grandes avances en la detección de estas actividades con una programa de Ley de Secreto Bancario y antilavado de dinero (BSA/ALD) fuerte y con la ayuda de tecnología muy compleja.

La herramienta más eficaz de una institución financiera es un "programa de diligencia debida del cliente" integral. Este programa no debe terminar con la solicitud de cuenta, sino que continuará hasta que la cuenta se cierre. Un programa eficaz de diligencia debida del cliente (DDC) asistirá a las instituciones financieras en gran medida en la detección de nuevos esquemas y asegurará que las instituciones financieras no están siendo utilizadas, sin saberlo, para el lavado de dinero proveniente de actividades ilícitas.

La facilidad con la que los ciberdelincuentes pueden ocultar, anonimizar o disfrazar sus senderos electrónicos en la Internet es probablemente el mayor desafío para los investigadores

Y, por último, me gustaría dar las gracias a las instituciones financieras que trabajan tan duro en la prevención de lavado de dinero y otros delitos financieros, que realmente sirven como primera línea de defensa y el IRS-CI aprecia su trabajo y compromiso con el ALD.

AT: ¿Ha aumentado la corrupción pública en los últimos cinco años y qué tendencias ha visto que las IF deben tener en cuenta?

RW: Durante los últimos cinco años, el IRS-CI ha iniciado cientos de investigaciones de corrupción pública al año. Si bien no hemos visto un aumento en las investigaciones de corrupción en los últimos cinco años, hemos visto recortes significativos en nuestro presupuesto que afectan drásticamente nuestra capacidad de trabajar este tipo de casos. IRS-CI está comprometido con la lucha contra la corrupción pública y vamos a usar nuestra experiencia financiera para que los funcionarios públicos corruptos se hagan responsables.

AT: ¿Cuáles son los principales desafíos que enfrentan los investigadores al investigar el delito cibernético?

RW: La facilidad con la que los ciberdelincuentes pueden ocultar, anonimizar o disfrazar sus senderos electrónicos en la Internet es probablemente el mayor desafío para los investigadores. Un informe del año pasado estimaba que casi un tercio de todos los equipos pueden estar infectados con algún tipo de malware. Cada equipo infectado tiene el potencial de ser un punto de entrada para los delincuentes desde donde rebotan su conexión a la Internet por lo que resulta difícil para las autoridades de control legal identificar la verdadera fuente de una transacción fraudulenta. Además, la Darknet (Internet oscura, en español) se ha convertido en una fuerza impulsora en la evolución del ciberdelito debido a su enorme tamaño (Darknet tiene 500 veces el tamaño de la Internet visible) y la falta de indexación por los motores de búsqueda. Servicios delictivos, herramientas y tácticas se anuncian y se comparten en la Darknet con regularidad. Su tamaño abrumador les hace difícil a las autoridades de control legal identificar, y mucho menos controlar, toda la actividad delincuencial que ocurre.

AT: ¿Qué consejo puede darles a las IF sobre cómo abordar la ciberdelincuencia?

RW: Asegúrese de que las políticas y los procedimientos de diligencia debida mejorada (EDD) y conozca a su cliente (KYC) son sólidos y se cumplen en toda la organización. Reportar todas las actividades sospechosas a las autoridades de control legal por medio de los documentos ROS presentados y asegúrese de incluir toda la información electrónica (dirección IP, agente de usuario, URL de referencia) recogida por sus sistemas. Utilizar autenticación de múltiples factores para verificar la identidad de un cliente al acceder a la información de cuenta. Mientras que parte de esta información puede parecer trivial, a menudo es el tipo de información que puede guiar a las autoridades de control legal en la dirección correcta a través de un patrón de actividad o actividad vista por múltiples instituciones financieras.

AT: ¿Qué medidas deben tomar las IF para identificar sanciones evasiones?

RW: Una vez más, un programa de CDD dinámico y un programa de cumplimiento de la Oficina de Control de Activos Extranjeros (OFAC) son críticos en la identificación temprana de los clientes que tienen las sanciones impuestas en su contra. La Ley Patriota aborda varios aspectos de la debida diligencia, incluyendo, la verificación de la identificación y la debida diligencia especial de corresponsales y cuentas de banca privada. La debida diligencia requiere de una institución financiera que esté alerta a las transacciones inusuales y compare el titular de la(s) cuenta(s) y las transacciones relacionadas (transferencias bancarias, cartas de operaciones de crédito y transacciones de quienes no son clientes, tales como transferencias de fondos) a una lista de la OFAC actualizada.

A continuación se presentan algunos de los métodos que los individuos estadounidenses pueden utilizar para evadir las sanciones estadounidenses.

Los clientes de los EE.UU. que crean empresas simuladas:

- Corporaciones simuladas utilizadas con este fin se forman a menudo en un país distinto del propietario y del banco
- La corporación/entidad está formada en un país distinto de donde se está haciendo negocios
- El presidente o la junta de una corporación pueden mostrar la verdadera propiedad de los EE.UU.
- Una revisión de los estatutos de la sociedad puede ayudar en la identificación de la verdadera identidad de los titulares de cuentas

Clientes estadounidenses enmascarando la verdadera identidad de los titulares de cuentas de los EE.UU. mediante la creación de fideicomisos:

- El beneficiario de los fideicomisos puede indicar el interés de los EE.UU.
- Revisión de la fuente de los fondos

Apertura de cuentas bancarias suizas “numeradas” para blindar las identidades, incluso de los empleados del banco suizo:

- Asegúrese de que la documentación se mantiene cuando se arman las cuentas
- KYC

Permanece siempre fiel a ti mismo y sigue tu instinto

AT: Durante su estadía en el IRS, ¿qué ha visto como violaciones comunes del código de impuestos de los EE.UU.?

RW: El robo de identidad relacionado con los impuestos ha sido el tema más prolífico durante mi mandato. Desde 2010, el IRS ha visto un crecimiento epidémico en el robo de identidad. En respuesta, el IRS dedicó gran cantidad de recursos para luchar contra esta prioridad y, en consecuencia, a partir de 2011 hasta octubre de 2014, el IRS detuvo 19 millones de declaraciones de sospechosos y protegió más de $63 mil millones en reembolsos fraudulentos. IRS-CI permanece al frente luchando contra el robo de identidad. En los últimos tres años fiscales del IRS-CI inició más de 3.400 investigaciones de robo de identidad y más de 1.400 personas fueron condenadas a procesamientos adicionales en espera de la adjudicación definitiva. Profundizando nuestro compromiso, IRS-CI patrocinó el programa de Asistencia de Autoridades de Control Legal en todo el país, que prevé la divulgación de información federal de declaración de impuestos para su uso en los procesos estatales y locales de control legal. En la actualidad hay más de 860 agencias de control legal estatales/locales de 48 estados participando. En el año fiscal 2014, se recibieron más de 6.776 solicitudes de asistencia de agencias de control legal estatales y locales. En enero de 2012, el IRS-CI estableció una centralizada Cámara de Compensación de Robo de Identidad (ITC) para evaluar y plantear esquemas de reembolso de fraudes de robo de identidad a las Oficinas de campo de IRS-CI para su investigación. Desde su creación, el ITC ha recibido más de 7.600 pistas individuales potenciales de robo de identidad en las que participaron más de 1,47 millón declaraciones de sospechosos y más de $6,8 mil millones en reembolsos. IRS-CI también mantiene un papel de liderazgo y/o papel activo en más de 75 grupos de trabajo multiregionales o grupos de tareas, incluyendo las agencias de control legal estatales/locales y federales exclusivamente centradas en el robo de identidad también.

AT: Hubo un reciente, primero de su tipo, arreglo de BSI SA anunciado a principios de este año, ¿cuáles son algunos puntos clave que deben tomar las IF de la investigación?

RW: El gobierno de los EE.UU. continuará sus esfuerzos de erradicar la evasión fiscal offshore. Vamos a seguir persiguiendo a aquellos que ayudan a facilitar la evasión de impuestos y los que utilizan cuentas secretas en el extranjero para evadir impuestos. Con BSI, el gobierno de los EE.UU. acordó no enjuiciarlos por delitos relacionados con los impuestos de los títulos 18 o 26, Código de los EE.UU., ni de los delitos de transacciones monetarias bajo el Título 31, Código de los EE.UU., Secciones 5314 y 5322. A cambio de llevarlos a juicio, el banco acordó los siguientes términos:

- Hacer una divulgación completa de sus actividades transfronterizas;
- Proporcionar información detallada sobre una base de cuenta por cuenta de las cuentas en las que los contribuyentes estadounidenses tienen un interés directo o indirecto;
- Cooperar en las solicitudes de tratados para información de cuentas;
- Proporcionar información detallada sobre otros bancos que transfieren fondos en cuentas secretas o que aceptaron fondos cuando las cuentas secretas se cerraron;
- Estar de acuerdo en cerrar las cuentas de los titulares de cuentas que no cumplen con las obligaciones de información de los EE.UU.; y
- Pagar penas adecuadas (en el caso del BSI fue de $211 millones).

AT: ¿Anticipa usted arreglos adicionales este año?

RW: Sí.

AT: ¿Cuál es el mejor consejo de carrera que ha recibido?

RW: He sido muy afortunado en mi carrera en haber tenido algunos grandes mentores. Un mentor me dijo desde el principio "permanece siempre fiel a ti mismo y sigue tu instinto". También he aprendido a rodearme de grandes colegas que forman parte de mi equipo. Trato de trabajar tan duro como pueda y mantenerme centrado en la misión, sin importar cuán significativo sea el desafío. Soy muy dedicado a IRS-CI y apasionado por el trabajo y los empleados. Si haces algo que te gusta, es más fácil ir a trabajar todos los días. Y, por último, creo que es muy importante equilibrar el trabajo y la vida familiar. Tengo un hijo de 4 años de edad, que es la parte más importante de mi vida y trato de asegurarme de pasar tanto tiempo con él como pueda.

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

ACAMS Chapter Development Program

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.

Join an ACAMS Chapter today!

For more information on ACAMS Chapters please visit: http://acams.org/acams-chapters

ACAMS® | Advancing Financial Crime Professionals Worldwide®

MERCADO NEGRO DE CAMBIO DE PESOS: EL comienzo

Los mercados negros han operado siempre desde que han existido fronteras, civilizaciones y gobiernos. Se desarrollan con el fin de aprovechar las diferencias políticas y/o económicas entre dos o más jurisdicciones: países, estados y provincias, condados y distritos o ciudades. Los mercados negros generalmente se forman y florecen como una respuesta a la prohibición o restricción de acceso a los bienes.

Este artículo comentará el Mercado Negro de Cambio de Pesos (BMPE, por sus siglas en inglés), lo que facilita el blanqueo del producto de la venta de drogas ilícitas en los EE.UU., y se centrará en los dos puntos siguientes: 1) sus participantes, estructura y funcionamiento; y 2) las respuestas penales y civiles a través de las leyes de lavado de dinero de los EE.UU., la Ley de Secreto Bancario (BSA) y las regulaciones de informes de divisas asociadas, y el decomiso de activos y otros estatutos federales relacionados.[1] Además, Colombia y México serán el foco principal de esta discusión.

En el mercado negro de bienes de otro modo legales, las diferencias suelen ser económicas: la mayor disponibilidad o menores costos de adquisición (por ejemplo, las materias primas, los costes de fabricación y precios de compra) en la fuente o de la jurisdicción "de salida" y mayores precios de venta en el destino o "jurisdicción de entrada". Las diferencias en los derechos, aranceles, los impuestos y las tasas de cambio de divisas también pueden jugar un papel. Las sanciones civiles o penales relacionadas con la actividad económica del mercado negro en general sólo se encuentran en la jurisdicción de destino.

Para las mercancías de contrabando así designadas por decisión política (por ejemplo, alcohol, armas de fuego, equipo militar/municiones, materiales nucleares) o bienes ilegales—principalmente drogas ilícitas—las recompensas financieras son mayores. Sin embargo, existen riesgos en ambos lados de la(s) frontera(s), debido a la criminalización y la ejecución conjunta de las jurisdicciones afectadas. Al igual que con el tráfico de drogas, los efectos colaterales de la actividad del mercado negro y el BMPE incluyen la evasión fiscal nacional y extranjera, la corrupción, el debilitamiento de la actividad económica local y la violencia.

Los EE.UU. sigue siendo el mayor mercado de consumo de drogas ilícitas: cocaína, marihuana, heroína, metanfetamina y MDMA (éxtasis). Los principales productores de cocaína son Colombia, Perú y Bolivia. México es el segundo mayor productor de amapolas del mundo (detrás de Afganistán); 95 por ciento de la cocaína que entra en los EE.UU. transita a través de México y México es el mayor proveedor extranjero de marihuana y metanfetamina a los EE.UU.[2]

[1] Se supone que el lector está familiarizado con el narcotráfico, los estatutos federales estadounidenses de lavado de dinero, la Ley de Secreto Bancario (BSA) y normas relacionadas; la 'visión' del contenido y ejemplos será desde la perspectiva estadounidense (es decir, usando términos tales como nacional, hacia el exterior, exportar, etc.) a menos que se diga lo contrario.

[2] The CIA World Factbook, Field Listing: Illicit Drugs (2011).

GRÁFICO 1

Comercio de los EE.UU. con Colombia en 2014

**En millones de dólares estadounidenses*

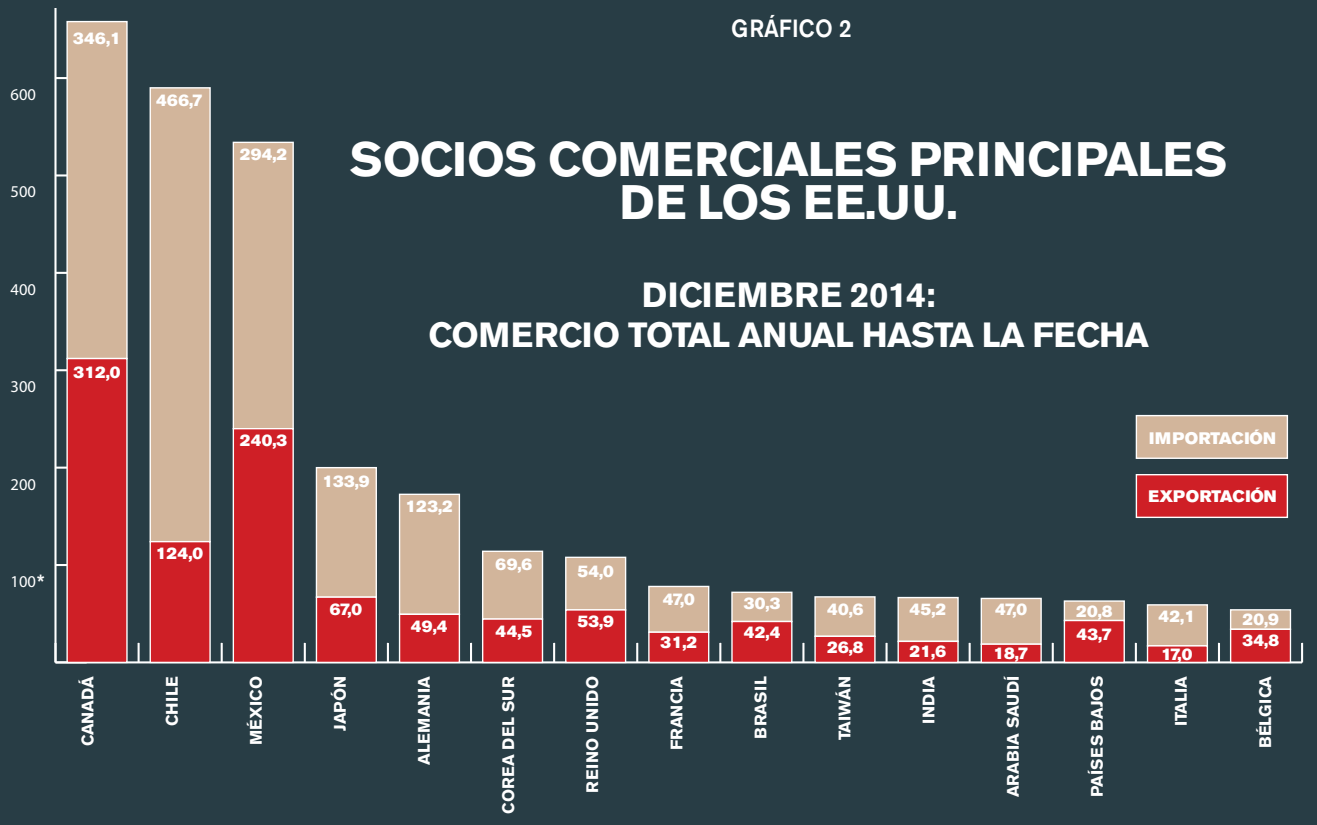
México es nuestro tercer socio comercial, representa el 13,5 por ciento del total del comercio estadounidense de mercancías (vea el gráfico 2). El país ocupa el segundo lugar en las exportaciones ($240,3 mil millones, 14,8 por ciento del total) y la tercera de las importaciones ($294,2 mil millones, 12,5 por ciento del total).[3] La frontera entre los EE.UU. y México se extiende por unas 1.933 millas a través de los estados de Texas (1.241 millas), Arizona (373 millas), Nuevo México (179 millas), California (140 millas) y a través de seis estados mexicanos.[4] El comercio anual con Colombia para el 2014 representó exportaciones de $20,3 millón e importaciones de $18,2 millón (vea el gráfico 1).[5]

La venta de drogas ilícitas genera millones de dólares para las organizaciones de tráfico de drogas (DTO) o los carteles de Colombia y México. Estos dólares se encuentran físicamente en los EE.UU., mientras que los líderes de DTO residen principalmente fuera de los EE.UU. Las DTO quieren la mayor parte de sus ganancias lavadas y devueltas, o de otra manera accesible a ellos, en su moneda local: pesos colombianos o pesos mexicanos. El BMPE logra varios objetivos importantes:

- La "colocación" de las divisas de los EE.UU.—ganancias de las drogas—en el sistema financiero nacional (y en última instancia internacional); convirtiendo así el dinero en forma "digital",

[3] The U.S. Census Bureau, Foreign Trade Statistics, Year-To-Date (diciembre de 2014).
[4] Report, "U.S. International Borders: Brief Facts," Congressional Research Service, 9 de noviembre del 2006.
[5] The U.S. Census Bureau, Foreign Trade Statistics, U.S. Trade in Goods With Colombia, diciembre de 2014.

GRÁFICO 2



**Los datos son sólo para mercancía, sobre la base de un censo, en miles de millones de dólares*

- La superación de la vasta geografía involucrada,
- La limitación del riesgo de detección de las autoridades de control legal/interrupción y enjuiciamiento de los EE.UU. (ya que la "responsabilidad" de los fondos es del lavador), y
- La conversión de los narcodólares a pesos (y otros activos)—se entrega a los traficantes y sus asociados en cualquier parte del mundo.

Un componente importante del BMPE implica la compra y exportación de bienes y materias primas de los EE.UU. a los países de origen de la droga: Colombia, Perú, Bolivia, México y otros lugares. El término en espanol de "money laundering" es "lavado de dinero" y el BMPE se conoce comúnmente por los participantes locales como "el dólar negro" o "el dólar de la calle". El término "mercado informal" es utilizado por profesionales de las finanzas y de negocios y la élite social cuando se refiere a dinero en efectivo de los "narcotraficantes". El término "lavado de dinero basado en el comercio" (TBML) se utiliza a veces por la policía para describir el BMPE.

El BMPE es un sistema complicado, con muchos participantes; opera simultáneamente en todo el mundo. Cada participante tiene un papel específico. Estos son los cinco pilares del BMPE:

1. La DTO del exterior y su personal que reside en los EE.UU.
2. Las empresas "legítimas" e importadoras de bienes/materias primas en Colombia y México que compran estos productos de los fabricantes estadounidenses para la exportación/reventa en sus mercados
3. Los "corredores de pesos" que operan entre ambos y facilitan a las DTO y negocios de Colombia y México
4. Los fabricantes y empresas de los EE.UU.
5. Las instituciones financieras estadounidenses y extranjeras

Las DTO poseen grandes sumas de dólares ubicadas en los EE.UU. y las empresas extranjeras tienen pesos, pero necesitan dólares para comprar y exportar productos y materiales estadounidenses. Los corredores de pesos ofrecen un proceso eficiente y discreto para resolver los respectivos dilemas de ambos grupos de "clientes". El BMPE resulta menos costoso para las empresas extranjeras que convertir sus pesos al tipo de cambio oficial a través de sus sistemas bancarios locales y las organizaciones de narcotraficantes pueden recibir sus ganancias lavadas en la moneda local y evitar los riesgos y costos del contrabando de dinero y la conversión.

Los fabricantes estadounidenses, las empresas al por mayor o menor y los exportadores parecerían no estar involucrados en el BMPE; sin embargo, varias leyes estadounidenses obligan a las empresas a informar (y pagar impuestos sobre) las transacciones monetarias.[6]

[6] Código de los Estados Unidos: Título 31, la BSA y regulaciones asociadas (crímenes informes moneda); y Título 26 (Fiscal Penal y delitos relacionados).

Los estatutos de lavado de dinero criminalizan las transacciones financieras "al saber que los fondos involucrados son el producto de la *actividad ilegal especificada*" (SUA, por sus siglas en inglés), un subconjunto de los delitos de tráfico de drogas.[7] Por otra parte, las leyes de los EE.UU. permiten el decomiso de activos y de los fondos "que participan en o pueden trazarse a" violaciones de lavado de dinero o de informes de divisas. La carga judicial de la prueba en los casos de decomiso de activos civil (preponderancia de la evidencia) en los EE.UU. es significativamente inferior a la norma penal de "más allá de una duda razonable".

Los corredores de pesos están generalmente ubicados en el mismo país de los líderes de las organizaciones narcotraficantes. Pueden llevar a cabo una combinación de actividades financieras legítimas e ilícitas a nivel local, con el fin de reducir al mínimo sus propios riesgos de descubrimiento y persecución por parte de sus respectivos gobiernos. También pueden trabajar en el BMPE como un negocio secundario, además de su comercio habitual/legítimo. La DTO llama al corredor de pesos para avisar de una cantidad de dólares y su ubicación, se alcanza un acuerdo en cuanto al precio (de pago) para el corredor para "comprar" los dólares (y aceptar la responsabilidad por el dinero en efectivo) y se acuerda un plazo de ejecución. Este acuerdo es aceptado por ambas partes como un contrato ejecutable, aunque las ejecuciones sean extrajudiciales.

El pago (por lo general una tasa de cambio) dependerá de la relación entre el corredor de pesos y la DTO, la cantidad y la ubicación de los dólares disponibles para ser lavados, si el corredor de pesos ya tiene un cliente de negocios locales que necesita dólares (o una fuente disponible de pesos) y cualquier petición especial por parte de la organización narcotraficante. El plazo habitual de "asentamiento" es de 10 a 14 días, dependiendo de la complejidad de la organización para efectuar la transferencia de dinero en efectivo, en los EE.UU., de los empleados de la DTO a los agentes del corredor del peso y de la sofisticación de la organización interna de lavado de dinero del corredor de pesos de los EE.UU.

A la vez, las empresas legítimas colombianas o mexicanas que buscan comprar dólares llaman a su corredor de pesos. El corredor de peso ofrece "vender" sus dólares al cliente de negocios de pesos a un tipo de cambio que es más favorable (más dólares por peso) que el tipo de cambio oficial/del gobierno. Una vez que se alcanza un acuerdo, el cliente empresario arregla para entregar/transferir pesos al corredor de pesos y proporciona la cantidad y dirección o número de cuenta bancaria al(os) proveedor(es) de los EE.UU. del(os) que se ordenó la mercancía. El corredor de pesos se encargará de pagar al proveedor de los EE.UU., ya sea a través de transferencia bancaria o entrega física de dinero en efectivo o instrumentos negociables (cheques, giros postales, cheques de cajero u oficiales). El cliente de negocios suele ser responsable de organizar el transporte de lo comprado/pagado por los bienes a su propio país, que puede implicar medios legales e/o ilegales.

Las ganancias del corredor de pesos se hacen sobre la diferencia en las tasas (tipos de cambio) entre los clientes de las DTO y los de negocios. El beneficio para ambos clientes es una transacción "privada", llevada a cabo con poco o ningún conocimiento, participación o escrutinio del gobierno. Además, los bienes adquiridos por los clientes o empresarios de las DTO colombianas o mexicanas pueden ser introducidos de contrabando en sus respectivos países de destino, para evadir los derechos de importación, impuestos o por otras razones.

Una vez que se finaliza el contrato entre el corredor de peso y la DTO, el dinero debe transferirse; por lo general, ocurre a través de un intercambio de mano a mano. Esto se logra mediante una serie de llamadas telefónicas, faxes, mensajes de texto, o BlackBerry Messenger (BBM) entre cada parte a sus respectivos empleados en los EE.UU. (por lo general en lenguaje cifrado) que proporciona el acuerdo sobre la ubicación, el tiempo, las descripciones y "nombres de calle" de los actores locales. Se prefieren los mensajes de BBM "instantáneos" porque se mueven en un sistema de comunicación de propiedad, cuyos servidores de archivos se encuentran fuera de los EE.UU.

Estas reuniones y transferencias pueden estar en un lugar público o en una residencia o negocio, de preferencia con un garaje para evitar/minimizar la detección y vigilancia por parte de las autoridades de control legal. Después de la transferencia de dinero en efectivo de la organización de narcotráfico a la gente del corredor de pesos, ambas partes notificarán a sus respectivos jefes, lo que sirve para trasladar la responsabilidad de los fondos (de riesgo) y empezar el reloj del arreglo.

El beneficio para ambos clientes es una transacción"privada", llevada a cabo con poco o ningún conocimiento, participación o escrutinio del gobierno

En posesión de una gran cantidad de billetes de los EE.UU. de pequeña denominación,[8] el dinero debe ser "colocado" en el sistema bancario nacional a través de uno de dos métodos. Múltiples depósitos de menos de $10.000 cada uno se pueden hacer en docenas de cuentas personales o de empresas en múltiples sucursales de una o más instituciones financieras, lo que se conoce como estructuración.[9] En algunos casos, los depósitos en efectivo de más de $10.000 pueden hacerse en una o más cuentas de las empresas, posiblemente mezclándose con

[7] Código de los Estados Unidos: Título 18 § 1956, 1957 y 1960 (estatutos de lavado de dinero); y Título 21 (violaciones de tráfico de sustancias controladas o drogas).

[8] Hay alrededor de 441 billetes en una "libra" de moneda estadounidense; un millón de dólares en billetes de $20 pesa aproximadamente 113 lbs. Ejemplo: $700.000 dividido equitativamente entre billetes de $10 y $5, consiste en 105.000 billetes individuales y pesa 238 lbs.

[9] En un intento de evadir la presentación del informe de transacción en efectivo (CTR) de la BSA, disparado por depósitos (o retiros) en efectivo que superan los $10.000; ahora el promedio del depósito estructurado es de entre $2.500 a $4.000.

unos negocios legítimos, con una explicación por el volumen de actividad de efectivo y la cooperación en, o sin aparente resistencia a la presentación del informe de transacción en efectivo (CTR) para evitar el aumento de la sospecha de la entidad financiera en cuestión.

Los depósitos en efectivo estructurados se hacen en varios, a menudo docenas, de cuentas bancarias personales.[10] Esos saldos de primer nivel son luego transferidos a algunas cuentas de "estratificación". De estas cuentas de segundo nivel, las transferencias y transacciones se efectivizan para devolver los fondos lavados a los traficantes; por lo tanto hay "integración" de los narcodólares a la economía. Las transacciones del corredor de pesos se llevan a cabo a través de un representante o una cuenta de DTO controlada, de lo contrario, para la compra de otros activos. Los pagos en efectivo también se les hacen a otros proveedores y fabricantes de productos/materias primas solicitados por el negocio del corredor de pesos o clientes de la DTO.

El fenómeno de BMPE fue identificado por primera vez por la policía de los EE.UU. en la década de 1980

El fenómeno de BMPE fue identificado por primera vez por la policía de los EE.UU. en la década de 1980, asociado casi exclusivamente con las actividades de tráfico de cocaína de los cárteles colombianos de Medellín y Cali. Fue citado como una defensa a una incautación de una serie de cuentas bancarias efectuada al concluir la Operación Polar Cap, una investigación internacional estadounidense a gran escala de lavado de dinero[11] que se hizo pública en febrero de 1989. Los propietarios de varias de las cuentas incautadas (y sus abogados) argumentaron, a principios de 1990, que el BMPE era un sistema económico legítimo "paralelo"—si técnicamente ilegal en Colombia—y los fondos que se habían trasladado a través de su(s) cuenta(s) bancaria(s) estaban relacionadas con actividades comerciales legítimas entre las empresas en Colombia y los EE.UU.[12]

Tal vez la primera investigación del Congreso sobre BMPE se debió al 106º Caucus del Congreso del Senado sobre el Control Internacional de Narcóticos, copresidido por el senador Charles Grassley y el senador (ahora vicepresidente) Joseph Biden. Durante una audiencia del 21 de junio del 1999 ("El Mercado Negro del Cambio del Peso: Cómo las Empresas Estadounidenses son Utilizadas para Lavar Dinero") los funcionarios de los EE.UU. y colombianos describieron los procesos y principios económicos subyacentes que dieron origen a esta actividad económica paralela. También testificaba un corredor de pesos colombiano, quien describió sus actividades y experiencias. Al testificar de forma anónima, con un seudónimo, "Carlos" dijo que "El nacimiento del mercado negro fue hace unos 30 a 35 años [principios de 1960]. Cuando llegué a los negocios en Colombia, Colombia tenía y aún tiene altos aranceles de importación e impuestos altos. Debido a los altos impuestos y tarifas combinadas con el hecho de que en realidad era ilegal poseer moneda de los EE.UU. en Colombia, se creó el mercado negro. En aquel entonces si a uno lo pillaban con dólares, podría ir a la cárcel, dependiendo de la cantidad de dólares que tenía".[13] "Carlos" pasó a describir cómo funciona el BMPE, su transición a una herramienta para el lavado de los narcotraficantes colombianos y sus impactos en la vida de los colombianos.

Durante los años 1990 y 2000, ya que la actividad anti-narcótica coordinada presionó las rutas aéreas y de distribución marítima de los carteles, México surgió como una alternativa de ruta terrestre; y, con el tiempo, se convirtió en un conducto para las drogas colombianas y una fuente de suministro de "cosecha propia". Los carteles mexicanos se formaron y prosperaron, con los impactos adversos penales, económicos y sociales resultantes—en especial la corrupción y la violencia. La diferencia más significativa entre los cárteles colombianos y mexicanos es la proximidad geográfica (ventaja) de la que gozan los cárteles mexicanos. El comercio transfronterizo y el tráfico entre México y los EE.UU. sirve como una tapa eficaz para enmascarar ambas actividades de contrabando y lavado de dinero BMPE, dentro de la corriente de comercio entre los dos países. Durante décadas, ya que la economía mexicana se desarrolló y el comercio aumentó, la necesidad de servicios de cambio de divisas creció, particularmente en las zonas fronterizas; las casas de cambios y los cambistas (corredores de pesos) se desarrollaron para proporcionar dichos servicios. Actualmente, sin embargo, una gran parte del volumen total de las transacciones financieras—incluyendo la moneda estadounidense—es generada por las actividades de tráfico de drogas de México y lavada por el BMPE.

Las medidas de investigación y recursos dependerán de dónde (o de quienes) las transacciones de BMPE uno encuentre, ya sea como un agente de la banca o de la ley. Las alertas rojas en la actividad bancaria incluirían las siguientes:

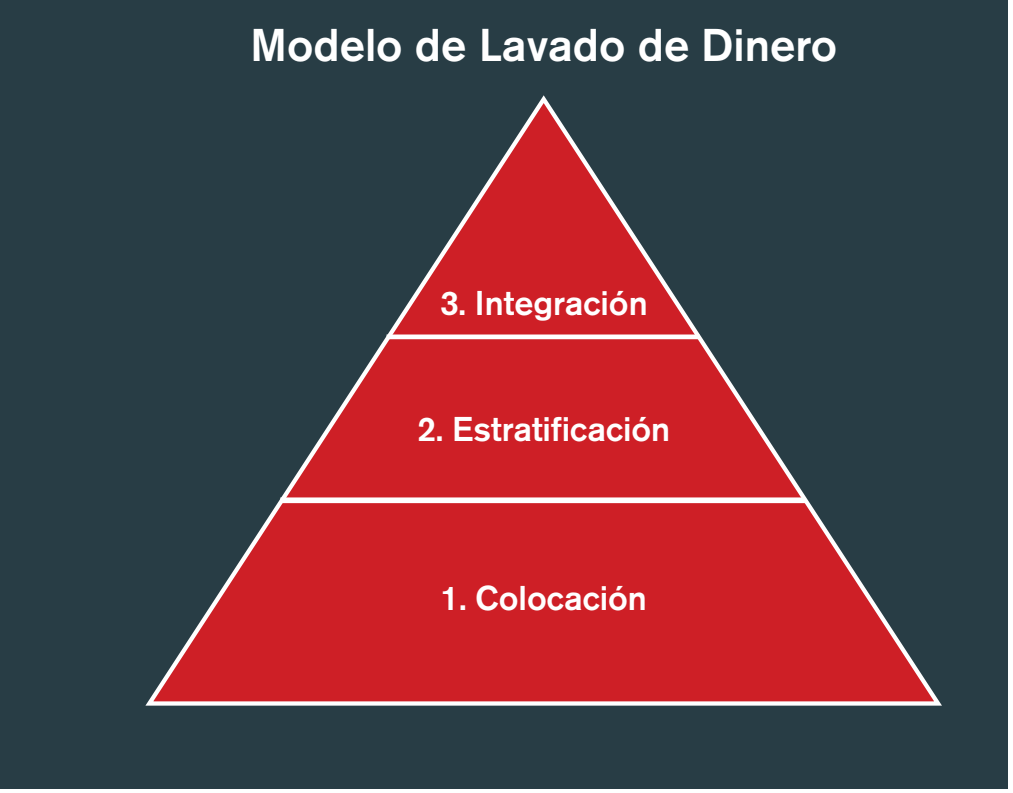
- Depósitos en efectivo frecuentes, en cuentas por lo general de cheques personales (las más fáciles de abrir).

[10] Porque resulta de lo más fácil abrir una cuenta corriente personal, las organizaciones de lavado de dinero (MLO) insistentemente trabajan para mantener un inventario de cuentas bancarias de los EE.UU.

[11] A finales de febrero de 1989, el Fiscal General Dick Thornburgh and el Secretario del Tesoro Nicholas Brady anunciaron la "culminación de la mayor investigación de de lavado de dinero jamás hecha por las autoridades de control legal de los Estados Unidos". El Fiscal General Thornburgh dijo que la Operación Polar Cap fue "una operación de lavado de dinero que manejó más de mil millones de dólares en ganancias ilícitas que pertenecían al cartel de Medellín. Cubrió… nueve ciudades por todos los Estados Unidos… 27 personas fueron enjuiciadas y se incautó más de media tonelada de cocaína y $45 millones en efectivo, alhajas y bienes inmuebles".

[12] Vea los EE.UU. v. los Ochenta y Ocho (88) Cuentas Designadas que Contienen Sumas Detectables A Cambios Para Sustancias Controladas, 740 F.Supp. 842 (S.D. Fla. 1990)

[13] Transcripción de la audiencia ante del caucus del Senado sobre Control Internacional de Narcóticos, Congreso 106º [S. Hrg. 106-198], "The Black Market Peso Exchange: How U.S. Companies are Used to Launder Money", 21 de junio del 1999, Declaración de Testigo Anónimo, "Carlos", un corredor de peso, Pg. 35, U.S. Government Printing Office.



- Cantidades de transacción de entre $2.000 y $7.500, pero por lo general menos de $5.000.
- Depósitos en efectivo realizados en las sucursales geográficamente distantes de la rama donde está domiciliada la cuenta o la dirección física del titular de la cuenta, sobre todo si los depósitos están llegando de manera rutinaria de fuera del estado y/o de múltiples estados.
- Volúmenes de transacciones altos, pero saldos finales bajos (el dinero no permanece mucho tiempo).
- Frecuentes débitos de grandes transacciones: cheques o transferencias entre cuentas dentro de la misma institución, o en cuentas en otras instituciones—transacciones de "estratificación"—probables también en las cuentas personales, pero posiblemente en cuentas empresariales o corporativas.
- La escritura a mano en los cheques depositados puede parecer diferente de la firma; los números de los cheques pueden ser sin número (cheques de inicio), de baja numeración o secuencialmente numerados.
- Compras con cheques de alta denominación o cheques oficiales; o iniciación de las transferencias grandes, pero con saldos bajos al final.
- La actividad de transacción puede ser significativamente más alta de lo esperado o excesivamente alta para el tipo de negocio de la cuenta.

Por parte de las autoridades de control legal, las personas o negocios que vale la pena tomar en cuenta son aquellos cuyas cuentas tienen actividad como se describe arriba, pero con poco empleo o ninguno, sin fuente legítima de ingresos, o tráfico de clientes; o sin lugares reales de actividad. Las empresas reales que están involucradas en BMPE estarán recibiendo entregas recurrentes por individuos que son probablemente no clientes (un cliente sube con una caja o bolsa, pero el individuo sale con las manos vacías poco tiempo después). Esos negocios al por menor o al por mayor también tendrán correos electrónicos o faxes de sus clientes mexicanos o colombianos "legítimos", asesorando al vendedor/proveedor del "paquete" pronto por llegar o que la entrega [monto en lenguaje cifrado] acabada de recibir era por sus facturas. Los registros de los clientes internos de negocio de siempre son representativos de estos pagos, o pueden ser falsificados para ocultar las grandes entregas de efectivo para evitar/evadir el Formulario 8300, requisito de presentación resultante. Otra actividad sospechosa puede incluir individuos reunidos en estacionamientos, con transferencias de bolsas o cajas entre los participantes, o el canje de vehículos.

El BMPE ha estado funcionando y evolucionando durante casi 60 años y sigue siendo uno de los métodos de lavado más eficientes y exitosos. En los últimos años, las instituciones financieras mejoraron sus sistemas de detección de antilavado de dinero (ALD) y las autoridades de control legal lograron enjuiciamientos exitosos en casos de estructuración y de lavado de dinero. Como respuesta, grandes cantidades de narcodinero en efectivo pasaron a los comercios al por menor y por mayor transferidas o dejadas a los propietarios de negocios dispuestos a aceptar las entregas anónimas de dinero en efectivo, para pagar por las ventas a sus clientes extranjeros. Estos dueños de negocios, a continuación, depositaron el efectivo en sus cuentas, como si se tratara de "recibos diarios".

En septiembre de 2014, el derribo de varias agencias de la Operación "Fashion Police" en Los Ángeles dio como resultado la incautación de cerca de $100 millones en moneda estadounidense y una Orden de Selección Geográfica (GTO) emitida por la Red Contra los Delitos Financieros (FinCEN) del Tesoro de los EE.UU. En abril de 2015, la FinCEN emitió una GTO similar para abordar actividades de lavado de dinero basadas en el comercio en Miami, Florida. Las GTO necesitan mayor transacción en moneda que reportan obligaciones de 2.000 empresas de Los Ángeles y 700 empresas en Miami, respectivamente y, como resultado, nuestro trabajo continúa.

Stephan Robinson, CAMS, agente especial, Investigación Penal del IRS, West Palm Beach, FL, EE.UU., stephan.robinson@ci.irs.gov

Hable el idioma del ALD

Un detective me alcanza tímidamente un archivo mientras su otra mano se eleva inconscientemente en un gesto como para protegerse los ojos del horror que se encuentra dentro de la carpeta. Su lenguaje corporal inconfundible habla tan fuerte como sus palabras. Quiere, sin ambages, escapar de la entrevista de investigación asociada al aspecto de lavado de dinero de este caso.

Escenas similares se dan con regularidad a las autoridades de control legal que optaron por especializarse en las investigaciones relacionadas con lo financiero y también los de las instituciones financieras que trabajan en el departamento de cumplimiento. Una vez que usted se instale más cómodamente en el mundo de antilavado de dinero (ALD) encontrará que muchos de los que están dispuestos a asumir las obligaciones dentro de esa carpeta no están necesariamente tan dispuestos a hacer las entrevistas de investigación asociadas a ella.

"Una entrevista de ALD productiva es mucho más compleja que la contabilidad forense más extrema. A menudo es el arte menos practicada del profesional de ALD",[1] escribí en un artículo anterior de *ACAMS Today*. La entrevista de investigación también sigue siendo un temor infundado, que impide que muchos investigadores alcancen plenamente la excelencia en ALD. Es hora de tener una buena charla sobre eso.

¿Alguien puede señalar un enjuiciamiento exitoso de ALD en el que las anomalías numéricas por sí solas hicieron ganar el juicio? Ya se trate de una confesión, contradicción o mentiras descaradas, serán las palabras que salieron de la boca de testigos las que al final llevarán un caso a una conclusión.

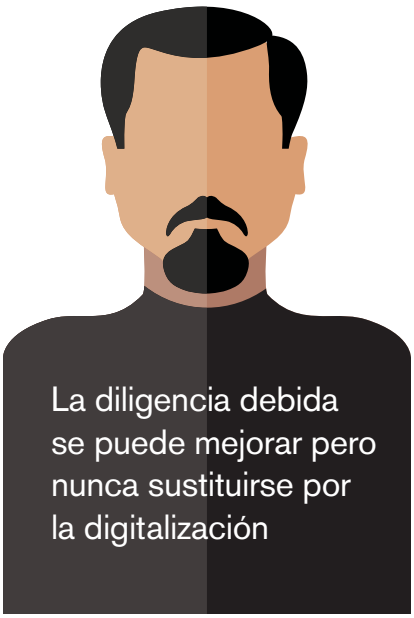
Todas las horas y los esfuerzos que usted ha realizado en una investigación de ALD pueden hacerse inútiles sin un testigo productivo y entrevistas sospechosas. Los fiscales legítimamente darán escasa atención a todos sus coloridos gráficos y análisis de enlaces a menos que usted les ofrezca confesiones, admisiones o declaraciones de testigos directamente relacionados con las personas que aparecen en ellos. Sus documentos corroboran o contradicen las declaraciones. Cualquier cosa ilícita en ellos necesita que alguien en una posición creíble diga por qué esto es así. Fuera de los casos en firme de fraude, la naturaleza individual de las transacciones relacionadas con el ALD no son inherentemente ilegales. Fuera de contexto, el depósito de una maleta llena de dinero en efectivo es simplemente un depósito bancario. Una conversación le agrega contexto.

Ese no es mi trabajo

Demasiados investigadores y profesionales de los sectores público y privado de ALD parecen demasiado ansiosos por señalar que las entrevistas no son parte de su descripción de trabajo específico y que es el trabajo de las autoridades de control legal o de otra persona. Todos ellos están demasiado cómodos detrás de una pantalla de computadora o una carpeta de archivos. Es sorprendente cómo tratando de digitalizar esta parte esencial de una estrategia global de investigación de ALD llegó tan lejos y se hizo tan frecuente. La diligencia debida se puede mejorar pero nunca sustituirse por la digitalización.

La pregunta mayor, a la que no hay una respuesta definitiva, es: ¿Cuándo es el momento más ventajoso para iniciar el proceso de entrevistas para una investigación de ALD? La mayor parte del tiempo los investigadores esperan demasiado tiempo. Por el lado de la institución financiera, la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD), la reducción de números y las anomalías de software ahora pueden resultar en cerrar cuentas deliberadamente, evitando toda posibilidad de que el cliente explique las anomalías. Se necesita una conversación para ver si los números caen en su lugar, o pueden ocupar ya su lugar. Ya sea un buen lugar, como un comportamiento inocente malinterpretado, o un mal lugar, como un esquema de lavado de dinero. Los números por sí solos nunca estarán en un lugar verdaderamente definitivo por sí mismos. Como resultado, la especulación se convierte en el juego final de cualquier estrategia de investigación de ALD que ignora deliberadamente la necesidad de una conversación relevante y de investigación.

Por el lado de las autoridades de control legal, datos al parecer interminables y la acumulación y análisis de documentos ha llevado a demasiados casos a estancarse. Incluso las posibles entrevistas de testigos no afectados, tales como cajeros o empleados de instituciones financieras son resistentes a los temores de comprometerse en una investigación. Las entrevistas con sospechosos directos se evitan debido a la especulación



[1] Steve Gurdak, "La Lógica de la Pizza", *ACAMS Today*, marzo-mayo 2012.[1]

infundada de que el sospechoso no accede a hablar. Los investigadores experimentados saben que su silencio es extremadamente raro en investigaciones de ALD. Por desgracia, dudar y dilatarse en hacer esas entrevistas no es tan raro.

Más charla, menos acción

La conversación investigadora nunca debe quedar en segundo plano respecto de otras prioridades en una estrategia de investigación de ALD. Es un elemento esencial de una conclusión exitosa. Lo que los investigadores de de ALD necesitan preguntar es por qué no han realizado entrevistas desde el inicio de una investigación. Si usted no puede expresar con claridad las consecuencias perjudiciales para una estrategia de investigación de hacer una entrevista de investigación, entonces usted necesita salir y hacer la entrevista.

Cuando se trata de las investigaciones, los investigadores de ALD comienzan normalmente en una posición mucho más fuerte que los investigadores de muchos otros delitos. Los "quién" normalmente se identifican hasta los números de Seguro Social. Los "qué" son transacciones financieras sujetas a verificación, junto con el "cuándo" y "dónde". "¿Por qué?" es el elemento que falta que sólo se puede responder si alguien es entrevistado. Reducir números adicionalmente y el análisis aumentará la especulación pero nunca responderá plenamente al por qué.

No se espera que usted pueda saltar de estar frente a una pantalla de computadora a enfrentar a Bernie Madoff. No hay, sin embargo, ninguna excusa para no llevar a cabo algún tipo de formación y práctica para alcanzar un nivel de competencia en lo que las entrevistas de investigación de ALD podrían implicar o cómo llevarlas a cabo. Las alertas de BSA/ALD más comunes o reportes de actividades sospechosas (ROS) se encuentran a nivel de sucursal o de la comunidad. Al igual que las anomalías entresacadas del ciberespacio en los datos de un punto de recogida centralizado. Son los cajeros y gerentes de sucursales los que notan las interrupciones o anomalías en el flujo normal de la línea de caja. Conseguir su perspectiva sobre las actividades es un punto ideal para iniciar la comunicación de investigación.

Tener conversaciones pertinentes es mucho mejor que no tener ninguna

Esto es por supuesto un arte que hay que practicar. Sin embargo, no deje usted que el hecho de que no ha asistido a uno de esos cursos de formación de alta especialización en las entrevistas e interrogatorios lo intimide. Los investigadores de ALD están normalmente en una buena posición para hacer preguntas pertinentes. Tener conversaciones pertinentes es mucho mejor que no tener ninguna.

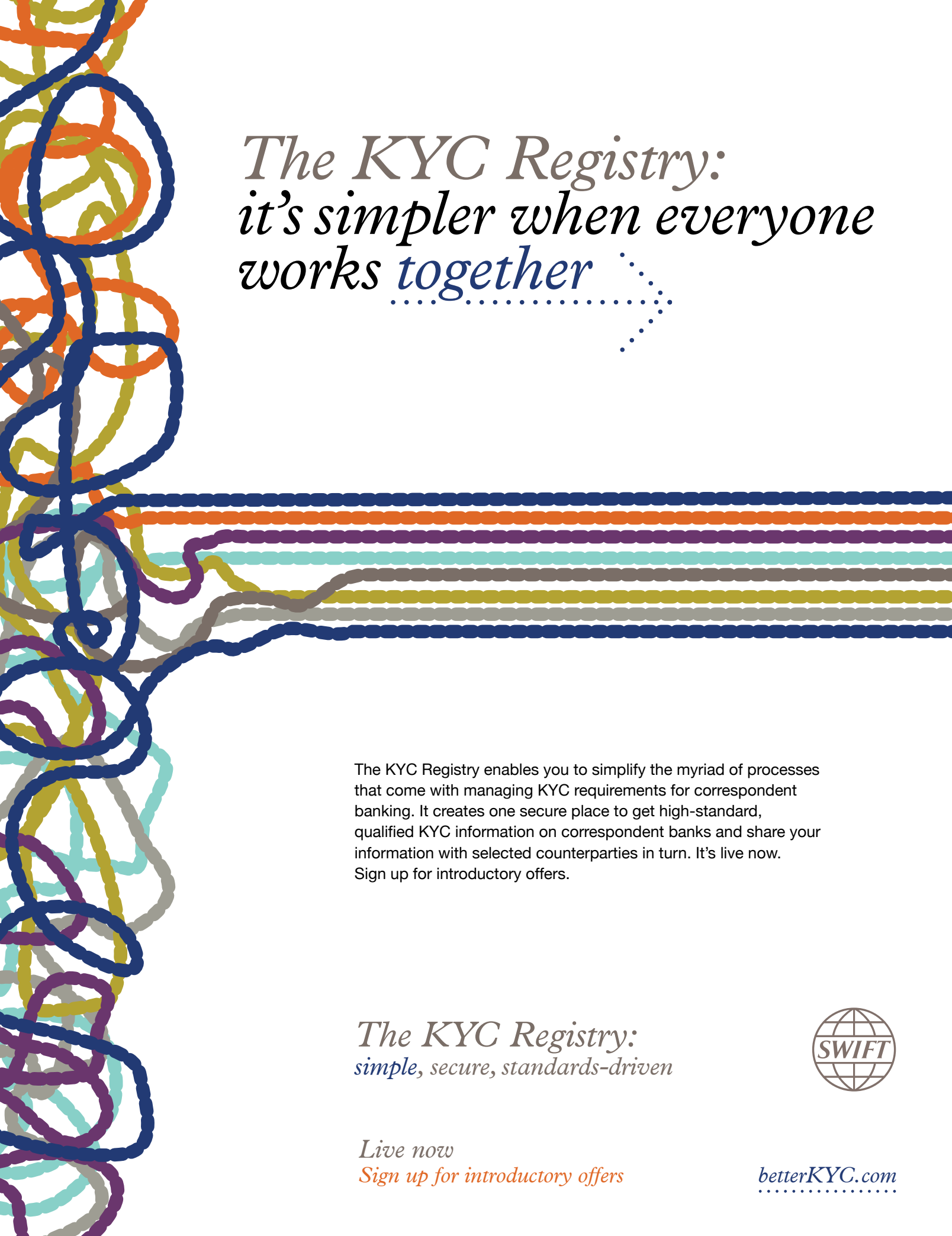
Y en cuanto a las respuestas, recuerde siempre que las mentiras, contradicciones, incoherencias y explicaciones incoherentes a menudo tienen más valor de investigación que la verdad. Los investigadores experimentados esperan y abrazan la mentira y el engaño, mientras que los inexpertos se ofenden o molestan personalmente por ellos. La BSA/ALD es acerca de las finanzas; en la vida real, las mentiras sobre las finanzas excederán las mentiras acerca de la fidelidad. La única salvedad a esto es que cuando usted llega a la verdad, a menudo es más extraña que la ficción.

Las especulaciones a menudo siniestras formadas por mirar los registros y documentos pueden alterarse por la verdad. A veces es una píldora difícil de tragar cuando todo su tiempo de investigación y los esfuerzos puestos en la investigación de los depósitos en efectivo sospechosos por medio de varias cuentas resulta ser un plan para evitar una estructura de comisiones bancarias y no una estructuración real. No se trata de hablar de todos aquellos ROS acerca de los patrones de abstinencia estructurados que parecen coincidir casualmente con el efectivo retirado al límite en varias sucursales. Preguntas simples hechas desde el principio protegen de citaciones desperdiciadas, producción de registros, el tiempo de investigación y otros costos relacionados.

Las preguntas tempranas podrían causar interrupciones o cambios en los más elaborados planes de lavado de dinero que se manifiestan en aún más anomalías transaccionales sospechosas y reconocibles. El fraude de los mayores puede ser eliminado antes de que se agoten los ahorros de toda la vida. Los lazos de la servidumbre por deudas también pueden romperse mucho antes. Preguntas simples hechas pronto también pueden descubrir aún más la torpeza de tratar de financiar a lobos solitarios o grupos terroristas de células pequeñas. Estos son sólo algunos ejemplos de los crímenes expuestos a través de la BSA, pero resueltos sólo porque un investigador en algún lugar del camino se bajó y habló con alguien acerca de ello.

Si el lavado de dinero tiene tres etapas—colocación, estratificación e integración—también lo tienen las investigaciones: identificado, investigado y resuelto. El dinero no habla realmente, pero sin duda puede actuar como el dial de volumen de los que hablan de ello. La conversación no puede ser programada de una investigación exhaustiva de ALD. Guardar silencio no es la opción correcta para las investigaciones de ALD—aprenda a hablar el idioma ALD.

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



The KYC Registry: it's simpler when everyone works together

The KYC Registry enables you to simplify the myriad of processes that come with managing KYC requirements for correspondent banking. It creates one secure place to get high-standard, qualified KYC information on correspondent banks and share your information with selected counterparties in turn. It's live now. Sign up for introductory offers.

The KYC Registry:
simple, secure, standards-driven

SWIFT

Live now
Sign up for introductory offers

betterKYC.com


Llamado a
testificar

Ser testigo en un proceso legal no es un paseo. Es asunto serio. Como testigo, su primer encuentro será muy probablemente con un abogado amistoso cuyo objetivo es ayudarlo en presentarse como un testigo creíble. Desafortunadamente, en la mayoría de los foros, probablemente encontrará un abogado acusatorio que querrá impugnar su credibilidad. Créame, ser testigo en una situación de confrontación puede ser muy estresante.

Las autoridades de control legal están entrenadas para prestar testimonio en los procesos judiciales. ¿Cuántos profesionales de antilavado de dinero (ALD) y/o de cumplimiento antifraude están capacitados para lo mismo? A menos que tengan experiencia previa en la aplicación de la ley, muy pocos profesionales de ALD y de cumplimiento antifraude han sido capacitados para testificar. De hecho, no muchos—si alguno—de estos profesionales creen que se les obligará testificar en un proceso legal acerca del desempeño de sus responsabilidades. Animo a todos los profesionales de cumplimiento a considerar la posibilidad de que se los llame a declarar sobre decisiones tomadas en el desempeño de sus funciones y las posibles consecuencias de las decisiones y acciones tomadas para apoyar esas decisiones. Me refiero a esto como su momento de "si/entonces".

If/Then (Si/Entonces, en español) es un musical de Broadway. Es la historia de Elizabeth, una divorciada de 38 años de edad, quien regresa a la ciudad de Nueva York para volver a empezar después de su divorcio. Poco después de llegar a Nueva York, Elizabeth se enfrenta a una decisión acerca de las posibilidades y realidades de la vida y las relaciones. Hay dos líneas distintas en la historia basadas en su decisión. Una decisión lleva a "Liz" en cierta dirección en la vida, mientras que la otra decisión lleva a "Beth" en una dirección alternativa. La decisión de Elizabeth era su momento de "si/entonces". La decisión y líneas argumentales distintas resultan con consecuencias significativas. La pregunta es, ¿tomó Elizabeth la decisión correcta?

Los profesionales de ALD y de cumplimiento antifraude viven la historia de la vida real de llevar a cabo sus responsabilidades de cumplimiento, de investigación y/o analíticas sobre una base del día a día. ¿Toman decisiones informadas? ¿Documentan adecuadamente y ejecutan sus funciones al máximo grado o no? Aquí es donde el momento de "si/entonces" comienza para los analistas e investigadores de instituciones financieras.

Como investigador de cumplimiento de ALD y/o analista de fraude, ¿cree usted que alguna vez estará obligado a testificar en un proceso legal? Si no, reconsidérelo. Sucede. Cuando usted se da cuenta de que podrían llamarlo a testificar acerca de su desempeño profesional su decisión de "si/entonces" estará mucho mejor pensada y ejecutada. El trabajo diligente que hace de cara al público, sobre todo en la documentación de sus decisiones y la labor que lleva a este tipo de decisiones, tendrá un impacto significativo y minimizará el estrés que experimenta en la parte final de su labor cuando se enfrenta a la perspectiva de testificar en un proceso legal. Mientras más completo, coherente y objetivo sea, menos "margen de maniobra" les dará a los abogados que traten de desacreditarlo. Del mismo modo, asegúrese de documentar, documentar y documentar completamente, su proceso de trabajo y la toma de decisiones.

Un abogado de la oposición no es su amigo. Quiere desacreditarlo. Para lograrlo, tratará de "no dejar que los hechos se interpongan en el camino", a la vez que atacará su credibilidad. Mientras mejor informadas y documentadas sus decisiones, más difícil le será impugnar su credibilidad y confundir los hechos. Piense "si/entonces" y limite las posibles consecuencias estresantes.

De encontrarse usted en el lugar poco envidiable de ser testigo, hay una serie de situaciones testimoniales que podría tener que enfrentar. Van desde el tipo de testigo que usted podría ser, hasta al foro testimonial en el que se podría encontrar. Como testigo, dependiendo de la situación, usted podría ser un testigo amistoso o adverso. Se lo podría llamar a testificar como experto en la materia, testigo de hecho, testigo de corroboración o testigo hostil. Los foros testimoniales potenciales incluyen entrevistas, acciones regulatorias, audiencias del Congreso, deposiciones, gran jurado o juicio. Los profesionales de cumplimiento de las instituciones financieras han estado involucrados en todos estos foros. Las entrevistas suelen ser las situaciones testimoniales más informales que pueden surgir y las menos estresantes. Algunos procedimientos en que podría estar usted involucrado serían los de tema de derecho civil, mientras que otros podrían ser de índole penal. Independientemente del foro, todos son estresantes. Cuanto más se puede hacer para minimizar el estrés, mejor estará usted. Por eso su momento de "si/entonces" es tan importante.

En caso de que usted tenga que ser testigo en un procedimiento judicial, los abogados que representan sus intereses lo prepararán para la experiencia. Deben trabajar con usted para reducir al mínimo la posibilidad de que el abogado contrario lo desacredite. En el caso de que sea testigo, aquí hay algunos consejos útiles básicos:

> Asegúrese de documentar, documentar y documentar completamente, su proceso de trabajo y la toma de decisiones

- Conozca el tema y las dificultades
- Su apariencia es importante
- Hable con sus propias palabras
- Sea responsable y veraz
- Escuche las preguntas y las instrucciones con atención
- Piense antes de hablar
- Si usted no entiende una pregunta o no sabe la respuesta, dígalo y no arme una respuesta cualquiera
- Corrija los errores
- Sea positivo y confiado

En realidad, la mayoría de los profesionales de ALD y de cumplimiento antifraude nunca se encontrarán en una posición que los obligue a testificar; sin embargo, algunos sí. No nos equivoquemos al respecto, cuando se produzca esa realidad, las consecuencias de su momento de "si/entonces" cobrará gran importancia.

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

Política, criminalidad y terrorismo en América Latina

En América Latina, las actividades de los cárteles de la droga, los grupos terroristas y estados canallas han aumentado a medida que los regímenes revolucionarios como Venezuela y sus aliados en Ecuador, Bolivia y Nicaragua tomaron las riendas del poder en la última década.

La guerra contra los cárteles mexicanos de la droga es a menudo descrita como una guerra contra una operación delictiva que tiene lugar en México. Además, también se presenta como un problema entre los EE.UU. y México.

Sin embargo, se puede argüir convincentemente que los cárteles de la droga también constituyen parte de una guerra asimétrica no sólo contra los EE.UU. sino contra muchos países de la región, también. Según el Dr. Max G. Manwaring, profesor y experto en estrategia militar en el Instituto de Estudios Estratégicos (Strategic Studies Intitute, en inglés) en Washington D.C., una guerra asimétrica incluye no sólo la guerra no convencional, como la guerra nuclear y los ataques terroristas de la guerrilla, sino que se compone de actos de gran complejidad política. En este sentido, Hugo Chávez, líder de la Revolución Bolivariana, entendía que el "proceso que lleva al fracaso es el más peligroso reto de seguridad a largo plazo", ya que un "estado fallido o en vías de serlo es el caldo de cultivo para la inestabilidad, la delincuencia, la insurrección, el conflicto regional y el terrorismo".[1] Por lo tanto, la erosión de la estabilidad, la seguridad y la soberanía efectiva del Estado-nación causada principalmente por las actividades delictivas de los cárteles de la droga, da paso a la anarquía. Los cárteles de la droga pueden comprar funcionarios electos, jueces, policías y otros elementos de la burocracia estatal. Por lo tanto, la sociedad misma se deteriora hasta el punto de convertirse en vulnerable a medida que la ley se convierte en cenizas. Este vacío de poder puede ser utilizado por un líder pro-Chávez para tomar las riendas del poder. Los cárteles de la droga estarían interesados en esta situación ya que el nuevo régimen los protegería autorizándoles la libre circulación.

Del mismo modo, los cárteles de la droga tienen una función secundaria a los ojos de estos países. Los cárteles de drogas

[1] Max G. Manwaring, "Venezuela's Hugo Chávez, Bolivarian Socialism, and Asymmetric Warfare," Carlisle, PA: The Strategic Studies Institute, U.S Army War College, octubre de 2005, p. 22.

envenenan la sociedad occidental y los EE.UU., causando daño. Como el erudito Ari Chaplin señala acertadamente, Fidel Castro utilizó el narcotráfico como medio para dañar a los EE.UU. Del mismo modo, Chaplin nos recuerda que Irán, que al igual que Castro es un aliado de Venezuela, señaló que "el narcotráfico es un medio para destruir a los hijos e hijas de Occidente".[2]

El narcotráfico es también una importante fuente de ingresos que sigue alimentando la revolución y recompensando a aquellos que lideran la misma. En Venezuela, un país que ha dado lugar a una nueva revolución socialista en América Latina y ha declarado hostilidad abierta hacia los EE.UU., el narcotráfico involucra los niveles más altos. El verano pasado, el general Hugo Carvajal—quien se desempeñó como jefe de inteligencia de Venezuela entre 2004 y 2011 y fue reelegido por el presidente venezolano, Nicolás Maduro, durante un breve período el año pasado—fue detenido en Aruba, a petición de los EE.UU. por su participación en el narcotráfico. Carvajal fue supuestamente el encargado de recoger cargamentos de droga de la organización narcoterrorista colombiano conocida como las Fuerzas Armadas Revolucionarias de Colombia (FARC). Carvajal presuntamente controlaba toda la distribución de drogas a los EE.UU. y Europa, y estuvo a cargo del lavado del dinero de la droga a través de la gigante petrolera venezolana, PDVSA. Desafortunadamente, debido a las amenazas del gobierno de Venezuela, Aruba envió a Carvajal de nuevo a Venezuela en lugar de responder a la solicitud de los EE.UU. para ponerlo bajo custodia estadounidense.

El difunto Hugo Chávez ofreció puertos y aeropuertos venezolanos a los cárteles de la droga. De acuerdo con un informe de la Oficina de Responsabilidad Gubernamental de los EE.UU. en 2009,[3] Venezuela les dio una mano a los grupos ilegales y armados colombianos, proporcionándoles un apoyo significativo y refugio seguro a lo largo de la frontera. Como resultado, estos grupos siguen siendo amenazas viables a la seguridad de Colombia y los esfuerzos antinarcóticos de los EE.UU. y Colombia. El informe proporciona evidencia de las actividades y la cooperación entre el gobierno venezolano con cárteles de la droga y las FARC.

El informe también reveló que el flujo de cocaína de los puertos y aeropuertos venezolanos a los EE.UU., África Occidental y Europa aumentó más de cuatro veces de 2004 a 2007 y sigue aumentando. Del mismo modo, la cocaína con destino a los EE.UU. desde Venezuela transita por Centroamérica, México, República Dominicana, Haití y otras islas del Caribe. Entre enero y julio de 2008, se incautaron numerosas embarcaciones con banderas venezolanas que llevaban grandes cantidades de cocaína.[4]

Tal cooperación con cárteles de la droga se amplió a los países aliados del régimen venezolano. Según un informe de WikiLeaks, Daniel Ortega, presidente de Nicaragua, es un aliado incondicional de Venezuela y recibió fondos de cárteles de la droga.En Bolivia, las actividades de los cárteles de la droga se han extendido desde que el aliado de Venezuela, Evo Morales, llegó al poder. El presidente ecuatoriano, Rafael Correa, recibió fondos para su campaña electoral de parte de las FARC, de acuerdo con uno de los líderes de las FARC. Además, Ecuador es un punto de transbordo importante para gran parte del polvo derivado de la coca producido en Bolivia y Perú. Venezuela, Bolivia y Ecuador expulsaron a los agentes de la Drug Enforcement Administration (DEA) hace dos años, proporcionando un ambiente más libre para los cárteles de la droga. La lucha contra las drogas es vista por estos países como un esfuerzo imperialista, de los EE.UU.

Esto agrava la situación en otros países de la región. En América Central, la actividad delictiva de la droga en países como Honduras, Guatemala y El Salvador, ha dado lugar a la anarquía y la debilidad del estado.

Tal crisis crea problemas tales como la emigración de los niños a la frontera norte. En palabras del presidente Juan Orlando Hernández, de Honduras, estos menores son "personas desplazadas", como resultado de una guerra provocada por el narcotráfico y las peleas afines entre bandas para tomar el control de la delincuencia y reclutar a niños y adolescentes con fines delictivos. Hernández denunció que el gobierno de los EE.UU. está haciendo un esfuerzo mínimo para luchar contra las organizaciones delictivas que les suministran drogas a los EE.UU. El Presidente Salvador Sánchez Cerén de El Salvador, hizo un llamado de redoblar esfuerzos para combatir el narcotráfico y el delito.

La presencia del terrorismo presenta otro problema agravado por los regímenes revolucionarios y la anarquía creada en la región. Irán y su apoderado, la organización terrorista Hezbolá, tienen una fuerte presencia en América Latina. Irán ha utilizado el sistema bancario venezolano (con la cooperación del gobierno de Venezuela) para evitar las sanciones impuestas por la comunidad internacional sobre su programa nuclear. Un acuerdo entre los gobiernos de Venezuela e Irán creó un banco de desarrollo binacional iraní-venezolano, es decir, de hecho, una alianza entre el Banco Industrial de Venezuela y el Banco de Desarrollo de Exportaciones de Irán. Esta asociación creó una nueva entidad, el Banco Internacional de Desarrollo, y se embarcó en otras ofertas, como la apertura de oficinas de instituciones comerciales de Irán en Venezuela. Sus sucursales se han expandido al Ecuador con el claro propósito de evitar sanciones financieras contra Irán.

Por otra parte, los iraníes y otros ciudadanos de Oriente Medio han recibido pasaportes de Venezuela o los adquiridos en otros países de la región asociados con la Alianza Bolivariana para los Pueblos de Nuestra América (ALBA) países. Del mismo modo, se cree que Irán ha comprado uranio de Venezuela y Bolivia para ayudar a desarrollar su capacidad nuclear.

La cooperación entre Hezbolá, el apoderado de Irán, y los cárteles de la droga también se está llevando a cabo. Hezbolá ha ayudado a construir túneles sofisticados para introducir drogas en los EE.UU. desde México. Estos túneles están equipados con electricidad, ventilación y un sistema ferroviario. Cientos de toneladas de cocaína fueron transferidos a través de estos túneles. Estos túneles se conectan entre almacenes o entre dos casas comunes a ambos lados de la frontera. De hecho, lo que hizo Hezbolá en la frontera libanesa/israelí no es diferente de lo que hemos

[2] Ari Chaplin, *Chávez' Legacy: The Transformation from Democracy to a Mafia State*, University Press of America, 2014, p. 173.
[3] EE.UU., Government Accountability Office, "Drug Control: U.S Counter-Narcotics Cooperation with Venezuela Has Declined," 20 de julio del 2009, http://www.gao.gov/assets/300/292722.pdf
[4] Ibid.

visto en la frontera México/EE.UU. Según los informes, Hezbolá ayudó a los cárteles a construir esos túneles a imagen de los mismos túneles que había construido en el sur de Líbano. Para ser claros, los túneles en el sur de los EE.UU. son más difíciles de detectar que los de Gaza. Hezbolá podría utilizar estos túneles para llevar a cabo ataques terroristas en los EE.UU. De hecho, en octubre de 2011 hubo un intento de matar al embajador saudí en Washington, D.C., con la ayuda del cártel de los Zetas. Esto demuestra la afinidad de los cárteles de la droga con grupos terroristas.

Asimismo, el grupo guerrillero colombiano FARC, que opera tanto como un cártel de la droga y como una organización terrorista, produce el 70 por ciento del total de cocaína refinada colombiana y controla los envíos de drogas de Colombia. Desde Colombia la mayor parte de la cocaína pasa por Venezuela, a través de América Central y a México, donde los cárteles de la droga mexicanos venden y transportan el producto a los EE.UU.

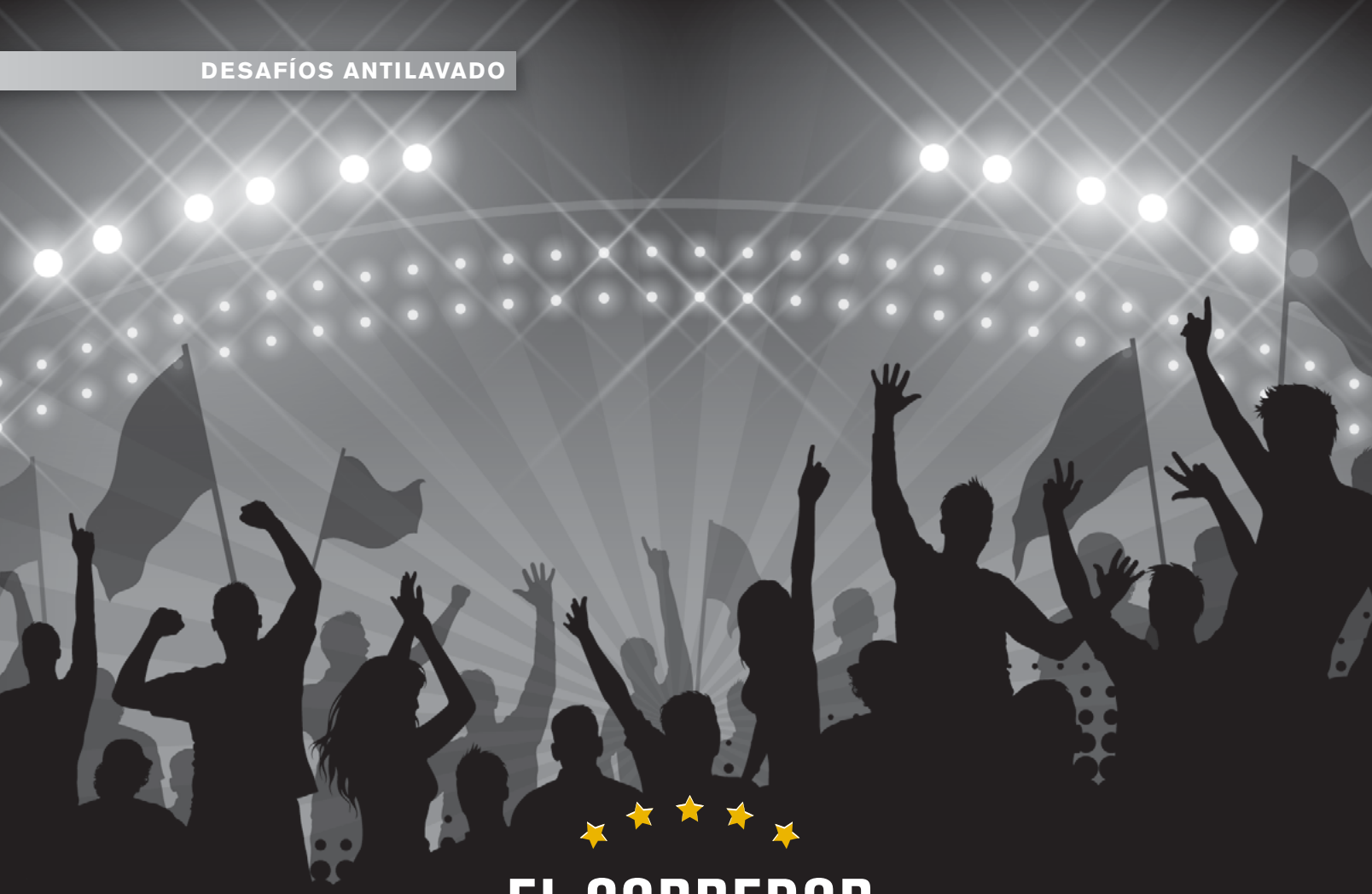
Además de las FARC y Hezbolá, la anarquía que ahora caracteriza una buena parte de América Central podría ser una atractiva para otros grupos terroristas. A continuación, bien podría ser el Estado Islámico de Irak y el Levante conocido como ISIL o ISIS. Su estilo al-Qaeda de amenazar a los EE.UU., su crueldad con respecto a la vida humana y la búsqueda de recursos financieros podría hacer de América Latina un blanco fácil para su marca de terrorismo. El negocio de la droga y la anarquía en expansión proporciona una especie de refugio seguro y un lugar estratégico desde donde podrían llevar a cabo una serie de actividades.

En primer lugar, ISIL estaría en un área geográficamente cerca de los EE.UU. Como tal, podría secuestrar y extorsionar a los estadounidenses con facilidad por dinero. En segundo lugar, podría obtener la documentación que les permita la libre circulación en el continente que podría hacer que las embajadas estadounidenses y otras instituciones sean vulnerables a los ataques terroristas. Por último, ISIL podría profundizar su participación en el narcotráfico y las actividades delictivas en América Latina para ayudar a proporcionar recursos financieros a su organización delictiva.

Como se ha señalado, Hezbolá, por supuesto, ha estado haciendo todo lo anterior durante largo tiempo. Los profesionales del antilavado de dinero (ALD), así como otros profesionales de la prevención de delitos financieros deben ser conscientes de los peligros de entender lo multidimensional de esta compleja coalición delictiva y política. Las transacciones financieras procedentes de los países del ALBA, en la medida que provienen de gobiernos o individuos, deben ser monitoreadas cuidadosamente. Ciertamente es crucial cuestionar el dinero en movimiento de estos países o de cualquier país de América Latina al Oriente Medio o viceversa. Ninguno de estos temas tiene estrategias adecuadas como debería y ha llegado el momento de hacerlo.

Luis Fleischman,[5] asesor principal, Menges Hemispheric Project, Center for Security Policy, Washington, D.C., EE.UU., lfleisch@hotmail.com

[5] Autor también de *Latin America in the Post-Chávez Era: The Security Threat to the United States*.



EL CORREDOR DE APUESTAS

¿Quieres apostar o hacer que un evento deportivo sea más interesante apostando en el resultado? Llama a un corredor de apuestas para ver qué pasa.

March Madness terminó hace unos meses y la gente de todo el mundo comprobó que no había ganado. Hay una persona que sí va a ganar: el corredor de apuestas. Entonces, ¿quién es el corredor de apuestas? Es la persona o personas que acepta/n apuestas, recibe el dinero y les paga a los ganadores. "¿Esto es legal?" uno se pregunta. En los EE.UU., sólo en Viva Las Vegas.

Una persona puede entrar en un casino de Las Vegas, ir a una casa de apuestas y apostar a cualquier evento deportivo, pero hay que pagar por esa apuesta de entrada. El corredor de apuestas hoy utiliza un sitio de apuestas offshore. No depositar dinero por adelantado resulta atractivo y conveniente cuando se lo puede hacer desde un dispositivo móvil, tableta, computadora del hogar o trabajo e incluso ahora desde el reloj.

El juego ha existido desde hace miles de años. Diferentes formas de juego se descubrieron en escritos del antiguo Egipto, China y Roma. Por ejemplo, los emperadores apostaban sobre los resultados de las carreras de carruajes; aunque apostar era ilegal, era una práctica común.

En la década de 1800, el béisbol comenzó y así comenzó la era del corredor de apuestas. En 1919, los White Sox de Chicago perdieron la Serie Mundial frente a los Cincinnati Reds. Lo que se conoce hoy en día como el escándalo de las Medias Negras (Black Sox scandal, en inglés) involucraba a jugadores que intencionalmente perdían la serie para recibir sobornos de los jugadores que colocaban apuestas con corredores.

En 1920 se formó la Asociación de Fútbol Americano (American Football Association, en inglés), que más tarde se llamaría la National Football League (NFL). Esta competencia de hombres y un balón de fútbol de cuero cambiaría drásticamente los deportes del mundo de apuestas como lo conocemos hoy. La NFL también catapultaría el mundo de apuestas de los deportes en un frenesí. Cada año se hacía un estimado de $80 a $100 mil millones en apuestas deportivas ilegales.

Juegos de azar: ¿Delito sin víctimas?

Los medios masivos de comunicación informan de manera habitual que la policía no debería perder el tiempo focalizando delitos inofensivos y sin víctimas. Además, los medios también afirman que es legal hacer una apuesta deportiva en Las Vegas y lugares de todo el mundo, así que se siga haciendo. Algunos de los que leen este artículo saben tan bien como yo que el juego puede ser adictivo, cosa que también sabe el corredor de apuestas.

¡Es hora de pagar! Tu equipo o equipos han perdido y le debes al corredor de apuestas. En mi profesión, me he encontrado con personas que le deben cientos de miles de dólares a su corredor de apuestas. Hablemos de este delito "sin víctimas". Una investigación reveló que un corredor de apuestas a través de instituciones financieras legítimas realizó segundas hipotecas sobre viviendas de sus apostadores que estaban profundamente endeudados debido al juego ilegal. Los apostantes continuaron apostando y perdiendo, y el corredor ejecutaba la hipoteca de la casa y de hecho utilizaba el Departamento del Sheriff de la localidad para desalojar a la familia de su casa. Cuando veo a niños sin hogar porque un esposo y/o esposa han destruido sus vidas por el juego, veo víctimas.

En los casos en los que he trabajado, he visto a apostadores que les debían a sus corredores dinero de pérdidas por apuestas deportivas. En un caso, el apostador no podía pagar y recibió una llamada telefónica del ejecutor del corredor de apuestas. Al apostador se le dijo "o pagas o me pongo enfrente de la casa de tu mamá y ella va a sufrir mucho". En otro, al marido se le dijo que a su esposa la golpearían y violarían si no pagaba. Historias como esta y peores existen en todo el país y el mundo. Las instituciones financieras sufren también: Las casas de apuestas, como los traficantes de drogas, depositan grandes sumas de dinero ilegal en los bancos, realizan transferencias ilegales por cable y ponen en peligro la integridad del sistema bancario.

La temporada alta para las apuestas

Los traficantes de drogas y los corredores de apuestas son organizaciones que operan en efectivo 24/7. Una institución financiera puede distinguirlos por la época del año. Un cliente bancario que recibe grandes depósitos en efectivo entre septiembre y diciembre podría estar involucrado en el juego ilegal, ya que es la temporada de la NFL. Como la temporada final comienza en enero y el Super Bowl se inicia en febrero, se puede detectar más dinero en la cuenta de un corredor de apuestas durante esta temporada. Entonces, de repente, hay un período de calma, pero la actividad recomienza en marzo, justo cuando comienzan los torneos de baloncesto universitarios de la NCAA, y una vez más hay un momento de calma en abril. No existe un método exacto en la detección de los fondos ilegales que entran o salen de las instituciones financieras. A las instituciones financieras no se las puede obligar a saber cuándo la cosecha de marihuana o amapola comienza o termina. Las instituciones financieras pueden protegerse a sí mismas a través de su diligencia debida del cliente (DDC) y al conocer a sus clientes. Por ejemplo, si el cliente dice que es una empresa de mudanza de muebles y está depositando millones de dólares al año. La pregunta que viene a la mente es: ¿Una empresa de mudanza de muebles realmente gana un millón de dólares al año?

El juego en línea

Un corredor de apuestas establecerá su registro, por lo general a través de Internet, con una compañía que muy probablemente se encuentra fuera de los EE.UU. El corredor crea una cuenta con TakesBets.com (una compañía falsa) y paga una cuota basada en el número de clientes. El corredor está provisto de una contraseña de Agente, esto le permite ver todas las cuentas de sus clientes. A medida que el corredor adquiere jugadores, a cada uno se le da el sitio web TakesBets.com y se le asigna una contraseña de cliente. Quien apuesta sólo puede ver las apuestas que él o ella haya colocado. El apostador puede ahora realizar apuestas en cualquier cosa del sitio web del corredor.

Los sitios web les ofrecen a los corredores un negocio anónimo delictivo, sin registrar, y la capacidad de comprobar las cuentas de los jugadores desde un dispositivo móvil. Esto facilita que el corredor no sea detectado por las autoridades de control legal. En la época en la que se usaba el papel de flash, se tiraba el papel en un cubo de agua, y se disolvía. Ahora basta con ponerse en contacto con su compañía de teléfono celular para limpiar la memoria del teléfono antes de que la policía extraiga la información de la misma.

Las autoridades de control legal por lo general descubren estas operaciones ilegales por medio de un apostador detenido bajo la acusación delictiva no relacionada con la operación del juego ilegal. Un buen agente de control legal que entrevista a un sospechoso le preguntará sobre todos los crímenes en que él o ella está involucrado/a o de los que tiene referencia y no sólo del delito bajo examen, lo que vale su peso en oro. A los corredores se les suele capturar por su base de clientes.

Un corredor que utiliza un sitio web puede ampliar su negocio delictivo ilícito. Además, los subcorredores de apuestas pueden ser contratados, lo que permite la expansión del cliente y permite al corredor salir de su territorio habitual, hacerse multiestatal e incluso internacional. Por ejemplo, un caso reciente reveló que nueve subcorredores abarcaban cuatro estados diferentes.

El dinero

El dinero intercambiado entre el cliente y el corredor se hace de maneras diversas. Las transferencias electrónicas parecen ser lo más común seguido por depósitos directamente en las cuentas. La DDC y políticas y procedimientos de conozca a su cliente (KYC) pueden ayudar en la detección de las instituciones financieras. Por ejemplo, un corredor de la costa oeste comienza a recibir depósitos en efectivo en su cuenta de individuos en la costa este. Se detecta que esta actividad se produce entre los meses de septiembre y febrero. ¿Puedes adivinar por qué? La temporada de fútbol americano de la NFL.

Otra forma popular para cambiar dinero es a través de giros postales enviados por correo al corredor. Los subcorredores y los clientes irán a numerosas negocios para comprar giros postales y permanecer por debajo de los requisitos de presentación de informes. Por ejemplo, en un caso investigado, un

subcorredor compró más de $70.000 en órdenes de pago de varias oficinas de correos y luego los envió al corredor en la costa oeste.

En otro caso investigado, el corredor depositó múltiples órdenes de pago en una cuenta de jubilación de una institución financiera. Un empleado empezó a notar que en las órdenes de pago figuraban nombres diferentes con sus firmas correspondientes, pero que las firmas parecían hechas por una sola persona. Estas transacciones se prolongaron durante más de un año y sólo se presentó un reporte de operaciones sospechosas (ROS).

Las apuestas deportivas tienen lugar en todas partes y siempre encontrarás un corredor de apuestas, si quieres hacer una apuesta

Por otra parte, los corredores utilizaban diferentes métodos para disfrazar sus ganancias mal habidas. Los trabajos ficticios son un tema común. Un corredor se centrará en el propietario de un negocio, lo endeudará y le dará una alternativa. El corredor hará que el dueño del negocio lo ponga en su nómina y nunca trabajará. El corredor recibe un cheque de nómina, que de hecho es la deuda contraída con el corredor de apuestas por el dueño del negocio y el cheque se puede depositar como dinero limpio.

Los corredores de apuestas a veces no viven sólo según las reglas; hay delitos conexos cometidos por empresas criminales ilegales, como usura, extorsión, fraude fiscal, tráfico de drogas, lavado de dinero, fraude por cable, por nombrar unos pocos. La Cosa Nostra (la mafia siciliana) ha estado involucrada en actividades delictivas en los EE.UU. desde la década de 1800. Uno de los mayores ingresos de dinero de la mafia a través de los años es el juego ilegal. A través de los años el delito organizado siempre ha buscado influir en el resultado de un evento.

La mafia no se encuentra sola cuando se trata de infiltrarse en el deporte profesional y en el deporte de apuestas ilegales para influir en el resultado. En 2007, el árbitro de la NBA Tim Donaghy utilizó su conocimiento del juego y su posición en la cancha para influir en el resultado del juego. Se declaró culpable de cargos federales de conspiración. Aquí, en el condado de Fairfax, Virginia, algunas de nuestras investigaciones mayores y de largo plazo han involucrado las apuestas deportivas ilegales, casos de corredores de apuestas.

Éstos son sólo algunos ejemplos de estos casos de corredores:

- *La familia Bansal*—Un padre y sus dos hijos tomaron las empresas y las casas y utilizaron el Departamento del Sheriff por medio de órdenes judiciales para desalojar a las familias de sus hogares residenciales y los dueños de negocios, que habían participado en las apuestas deportivas ilegales y habían quedado endeudados. Se les conocía como un grupo de delito organizado de Chicago de 1920 y se los llamó los Soprano de Fairfax.
- *La investigación Wu*—Una familia local que amasó millones por medio de una operación ilícita de apuestas deportivas. Los y las cónyuges se ayudaron entre sí mediante la adopción de apuestas deportivas ilegales por teléfono. Cada llamada se registró en micro casetes. La investigación Wu llevó a una incautación de $10 millones y se encontró que era una organización internacional.
- *Los Peters*—Un ex candidato de política tenía un sistema telefónico sofisticado y más de 400 clientes por todos los EE.UU. La investigación de los Peters condujo a una incautación de $500.000 de varias cajas de seguridad y cuentas bancarias ubicadas en Washington D.C., Florida, Ohio, Indiana y Texas. Este caso tuvo un giro interesante: El Servicio de Impuestos Internos (IRS) clasificó a Peters como muerto por no presentar una declaración de impuestos federales durante nueve años. Peters, que no había trabajado durante más de 10 años, fue depositando grandes sumas de dinero en cuentas bancarias por todos los EE.UU.
- *La investigación Yau*—La detención de vehículos en la vía pública hecha de manera rutinaria conduce al descubrimiento de miles de dólares estadounidenses. La investigación puso al descubierto una enorme operación internacional de apuestas deportivas ilegales. La investigación Yau identificó a 10 subcorredores en el condado de Fairfax, Virginia del Norte y en todos los EE.UU. que canalizaban fondos a Yau, que residía en Las Vegas, Nevada. Yau enviaba esos fondos ilegales a China donde se depositaban. Tarjetas de crédito y compras en los EE.UU. a través de bancos corresponsales se utilizaban para gastar los fondos ilegales.

La Unidad de Delito Organizado y División de Narcóticos de Lavado de Dinero del Departamento de Policía del Condado de Fairfax atribuye una gran cantidad de sus historias de éxito a la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS). Lo que hemos aprendido de las conferencias de ACAMS, los contactos realizados en los últimos años, las asociaciones formadas con las instituciones financieras en los EE.UU. y en el mundo, tienen un valor incalculable. Sin las asociaciones formadas con nuestros hermanos y hermanas en las autoridades de control legal locales y federales a lo largo de los EE.UU. y en el extranjero, nunca se habría logrado nuestro éxito.

El Condado de Fairfax no está solo en los EE.UU. o en el mundo. Las apuestas deportivas tienen lugar en todas partes y siempre encontrarás un corredor de apuestas, si quieres hacer una apuesta.

Alguien que lee este artículo comprenderá términos como por encima y por debajo, valerse de las apuestas, la línea, las burlas de la línea, la línea de dinero, el jugo, el vig, y así sucesivamente. En nuestra profesión, tienes que conocer tu objetivo y cómo operar, con el fin de desmantelar y arrestar. Una institución financiera puede proteger su industria por medio de buenas políticas y procedimientos de DDC y KYC para reducir su riesgo. Los corredores de apuestas utilizan varios métodos para colocar sus ganancias mal habidas en bancos, cuentas de jubilación, seguros de vida, fraudes de seguros, productos, transferencias bancarias, acciones, bonos y mucho más. Por medio de la formación y el reconocimiento de los modus operandi, los empleados de las instituciones financieras y las autoridades de control legal pueden derrotar este problema cada vez mayor.

Con los juegos de azar en línea cada vez más populares (y en algunos casos legales), ambas profesiones necesitan hacer sus tareas con el fin de proteger a nuestras comunidades, instituciones, nuestra economía y a veces a nuestros seres queridos.

James A. Cox III, CAMS, sub teniente, Departamento de Policía del Condado de Fairfax, Fairfax, VA, EE.UU., james.cox@fairfaxcounty.gov

Dun & Bradstreet grows the most valuable relationships in business by uncovering truth and meaning from data.

Visit us at dnb.co.uk/compliance to learn more.

dun & bradstreet

GROWING RELATIONSHIPS THROUGH DATA

EL REGISTRO DE ABONADO MÓVIL:

Una herramienta eficaz en la lucha contra el terrorismo

En mi artículo anterior "Dinero móvil: Equilibrar la integridad financiera con la conveniencia comercial",[1] examiné la génesis y el crecimiento del dinero móvil en África Oriental, con especial referencia a la importante contribución de inclusión financiera hecha por M-Pesa en Kenia.

El artículo también destacó varias vulnerabilidades del lavado de dinero móvil y la financiación del terrorismo o factores de riesgo y tipologías comunes, y formuló recomendaciones sobre los controles de mitigación apropiados que pueden adoptar los proveedores de dinero móvil para protegerse de la cristalización de estos riesgos.

Este artículo examina el papel del registro de abonados a la red móvil como una clave control de antilavado de dinero y la lucha contra el financiamiento del terrorism (ALD/CTF) y una herramienta para las autoridades de control legal, y pone de relieve las formas en que los datos de un abonado a la red pueden jugar un papel fundamental en la lucha contra el terrorismo a nivel mundial.

Estadísticas mundiales de terrorismo

El terrorismo es un flagelo que sigue amenazando y devastando vidas inocentes en todo el mundo. En este sentido, la Base de Datos del Terrorismo Mundial (GTD) ha codificado más de 125.000 incidentes terroristas que se han producido desde 1970 hasta la fecha.[2] Las estadísticas terroristas globales indican además que los incidentes terroristas han aumentado en los últimos 15 años y que ha habido "un aumento de cinco veces en el número de muertes por terrorismo, pasando de 3.361 en 2000 a 17.958 en 2013".[3]

África es uno de los tres principales continentes afectados por el terrorismo, con el África del Este y el Cuerno de África identificados como "la región de África subsahariana más amenazada por el terrorismo autóctono e internacional".[4] A través de los años, diversas iniciativas de países y globales se han implementado para contrarrestar el terrorismo y la financiación del terrorismo, incluida la promulgación de legislación pertinente para criminalizar el terrorismo, el lavado de dinero y la financiación del terrorismo; el establecimiento de programas de ALD/CTF en el ámbito institucional regulatorio y del sector privado; la creación de unidades de control legal específicas de lucha contra el terrorismo y los centros de denuncia de delitos financieros para hacer cumplir la legislación de ALD/CTF; y la cooperación mutua entre los estados en el intercambio de información y la captura y enjuiciamiento de sospechosos de terrorismo.

Las redes móviles y los riesgos del terrorismo

Los operadores de redes móviles (MNO) que también son proveedores de dinero móvil, normalmente se incluyen en la definición de "instituciones financieras" en la legislación ALD/CTF, y por lo tanto serían obligados a reportar operaciones sospechosas en sus redes móviles de dinero a la unidad financiera de reporte del crimen relevante.

Debido a su velocidad y portabilidad, que no son cara a cara y a la naturaleza de dinero no en efectivo, el dinero móvil tiene diversos riesgos que lo hacen vulnerable al lavado de dinero y al financiamiento

[1] Mercy W. Buku, "Dinero móvil: Equilibrar la integridad financiera con la conveniencia comercial", *ACAMS Today*, Vol. 11, No. 4, septiembre-noviembre 2012

[2] *Global Terrorism Index: Measuring and Understanding the Impact of Terrorism*, Institute for Economics and Peace, 2014, http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf

[3] *Global Terrorism Index: Measuring and Understanding the Impact of Terrorism*, Institute for Economics and Peace, 2014, http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf

[4] David H. Shinn, "Terrorism in East Africa and the Horn: An Overview," *The Journal of Conflict Studies*, 2003, http://journals.hil.unb.ca/index.php/jcs/article/view/218/376

del terrorismo como se ha dicho. Sin embargo, como la mayoría de los proveedores de dinero móvil han puesto en marcha sistemas automatizados de transacciones, que pueden realizar un seguimiento de las transacciones en sus plataformas, los terroristas en muchos casos prefieren financiar sus actividades en efectivo a través de canales tradicionales como *hawalas*,[5] u otros agentes informales de transferencia de dinero, en vez de por la corriente principal de dinero móvil y otros canales de remesas. Esta preferencia ha dado lugar cierres de agencias de transferencia de dinero de tipo *hawala* en países como Kenia, donde el Banco Central clausuró recientemente varios agentes informales de transferencia de dinero a raíz de un incidente terrorista contra una universidad local.[6]

Si bien los terroristas no usarían necesariamente sus plataformas de dinero móvil para remitir ganancias de la financiación del terrorismo, los operadores de redes móviles todavía estarán en riesgo, ya que los terroristas usarán invariablemente los teléfonos móviles como su principal medio de comunicación en la planificación y ejecución de actos terroristas.

En varios países se requiere por ley que las tarjetas SIM de estos teléfonos estén anotados bajo el nombre del usuario. En este sentido, el registro de abonado a la red y la integridad de los datos del titular asumen importancia crítica y por lo tanto se hace imperativo que operadores de redes móviles pongan en marcha los procesos de registro de abonado adecuados para garantizar la integridad de sus datos de suscriptor y que les permita detectar las operaciones terroristas en sus redes.

La legislación de registro del suscriptor

En los países donde no existen regulaciones obligatorias de suscripción de red o cuando dichos reglamentos no se cumplen, las redes móviles serán vulnerables a que los terroristas y otros delincuentes los usen para facilitar la planificación y ejecución de sus actividades delictivas.

En consecuencia, como una medida de salvaguardia, los reguladores de telecomunicaciones en varios países han adoptado una legislación según la cual es obligatorio que los operadores de redes móviles lleven a cabo la diligencia debida del cliente (DDC) de sus suscriptores

[5] George Ngigi, "CBK rules outlaw 'hawala' money transfer system," *Business Daily*, 2 de abril del 2013, http://www.businessdailyafrica.com/CBK-rules-outlaw-hawala-money-transfer-system/-/539552/1761942/-/fdtuja/-/index.html

[6] Allan Odhiambo and Ouma Wanzala, "Remittances to Kenyans are 'most at risk," Somalia warns," *Business Daily*, 8 de abril del 2015, http://www.businessdailyafrica.com/Kenya-shuts-down-Somali-remittance-firms/-/539546/2679402/-/14qhgkiz/-/index.html

mediante la adopción de medidas necesarias para verificar la identidad del suscriptor, antes de la activación de las tarjetas SIM en sus redes.

Estas medidas incluyen cumplimentar una solicitud por parte del suscriptor y la presentación de la documentación de identidad prescrita tales como documentos de identidad nacional, pasaportes, licencias de conducir, tarjetas de empleo y documentos de identidad estudiantil al agente del MNO, quien luego verifica la identidad del cliente contra la cédula de identidad y los detalles del formulario, antes de registrar la tarjeta de línea o SIM. La inscripción puede ser realizada por el agente directamente o por el MNO al recibir las solicitudes del agente.

La legislación también establece sanciones por incumplir la ley, que incluye multas y cárcel. En Kenia, por ejemplo, la legislación de abonado impone duras sanciones por incumplir la ley, que se aplican proporcionalmente a la MNO, al agente y al suscriptor.[7]

Actividad sospechosa/ indicadores de alertas rojas— Actividad terrorista

Los siguientes son ejemplos de operaciones sospechosas de redes móviles, incluyendo transferencias de dinero móvil, que podrían estar vinculadas a la actividad terrorista y por lo tanto requerirían una mayor investigación (la lista no es exhaustiva):

- Actividad del agente fuera de lo normal (por ejemplo, el aumento repentino de las irregularidades de registro dentro de una zona de alto riesgo)
- Registros sospechosos en los sistemas de la red del abonado y de MMT (por ejemplo, múltiples registros de los sospechosos y registros de terroristas en lugares de reclusión como cárceles, registros que utilizan documentos de identidad falsos, robos de identidad/fraudes de suplantación)
- Registros que incumplen los controles de detección de sanciones
- Registros sospechosos o frecuentes por parte de los agentes en zonas de alto riesgo

Es imperativo que los operadores de redes móviles garanticen la integridad y la eficiencia de sus procesos de registro de abonados

- Llamadas/mensajes de texto/transferencias de dinero frecuentes entre conocidos sospechosos de fraude/terrorismo y sus asociados (por ejemplo, antes o después de un incidente terrorista)
- Textos que incitan al odio étnico o religioso en contra de los que no son de la misma religión o raza
- Textos que buscan nuevos reclutas terroristas
- Llamadas sospechosas y amenazas hechas a los centros de llamadas de la MNO, o lo informado por los suscriptores
- Mucho tráfico de red próximo a un incidente terrorista, antes o después
- Retiros a distancia y depósitos directos (transacciones por mostrador) en zonas de alto riesgo
- Retiros de cajeros automáticos a distancia en zonas de alto riesgo
- Agentes informales internacionales agentes de transferencia de dinero no registrados que usan redes móviles de dinero para afectar las transferencias internacionales en nombre de sospechosos de terrorismo
- Frecuentes intercambios de SIM/cambios de autorización que permiten el acceso no autorizado a cuentas de banca móvil que lleva a la transferencia fraudulenta de fondos a través de la red de dinero móvil que puede utilizarse para financiar el terrorismo
- Uso elevado del volumen de los servicios de datos en lugares de alto riesgo

Datos de registro del suscriptor como una herramienta de control legal

En el caso de actividades sospechosas en la red, como se ha indicado anteriormente, o donde hay una investigación criminal terrorista en curso, los datos del abonado y los registros de llamadas/transacciones de dinero móvil pueden proporcionar información vital en la financiación del terrorismo o el terrorismo y otras investigaciones penales. Por medio de un software de análisis de enlace correspondiente, los datos pueden ser utilizados para proporcionar detalles de los sospechosos y sus asociados, su ubicación en determinados puntos en el tiempo, sus transacciones financieras y otras pruebas que pueden utilizarse para apoyar la acusación contra el sospechoso. En consecuencia, es imperativo que los operadores de redes móviles garanticen la integridad y la eficiencia de sus procesos de registro de abonados y que los datos de abonados y los registros de transacciones se actualicen con regularidad. También es imperativo que los operadores de telefonía móvil tengan sistemas automatizados de detección y sanción de transacciones y herramientas de análisis de enlace de monitoreo para vigilar y detectar inscripciones sospechosas y operaciones sospechosas en sus redes.

Los operadores de redes móviles también deben estar en condiciones de proporcionar el apoyo necesario a los organismos de control legal por medio de la presentación de los datos de abonado y registros para su uso en investigaciones de terrorismo u otras penales, de conformidad con la normativa aplicable para la presentación de tales pruebas.

Conozca a su suscriptor: Las mejores prácticas

A continuación se presentan unas mejores prácticas recomendadas que los reguladores y operadores de redes móviles en zonas de alto riesgo de terrorismo necesitan tener respecto de los datos de suscriptores:

[7] The Kenya Information and Communications (Amendment) Act, 2013, http://africanmediainitiative.org/content/2014/01/26/KICA-Act-2013.pdf

Reguladores

- Promulgar leyes que hace que el registro de abonados, su verificación y la sanción de detección sean obligatorios con sanciones por incumplimiento
- Establecer la documentación prescrita para la verificación de abonados (documentos de identidad aprobados, licencia de conducir, pasaporte, etc.)
- Establecer regulaciones que promuevan el intercambio mutuo de reportes de operaciones sospechosas (ROS) entre operadores de redes móviles y garanticen la cooperación obligatoria con las autoridades de control legal contra el terrorismo y otras investigaciones penales
- Asociarse con los ministerios pertinentes para poner en marcha sistemas de registro digitales, como los que se están implementando actualmente en Kenia,[8] Nigeria[9] y Egipto,[10] y establecer las bases de datos de registro centralizados, como el Sistema Integrado de Registro de Población en Kenia, que se puede utilizar para validar los datos de los abonados.[11]

MNO

Las MNO deberían poner en marcha las siguientes medidas con el fin de cumplir con la legislación de abonado y para detectar y prevenir actividades sospechosas en sus redes:

- Los registros electrónicos de suscriptores con funcionalidad biométrica y captura de fotos
- Validación automática de las bases de datos de clientes en relación con las bases de datos del gobierno aprobadas y contrastadas con listas de vigilancia, antes de la activación del servicio
- Establecimiento de la base de datos de suscriptores como la principal base de datos de clientes de dinero móvil como una opción de servicio
- Examen de sanciones en curso para identificar sospechosos de terrorismo registrados en sus redes
- Invertir en sistemas de monitoreo de transacciones automatizadas con alertas oportunas para detectar actividades sospechosas del suscriptor
- Invertir en herramientas de análisis de enlace para identificar las transacciones financieras y registros de llamadas de sospechosos de terrorismo y sus colaboradores cercanos
- Hacer uso eficaz de los datos de localización para facilitar el seguimiento de la actividad terrorista
- La acción apropiada de registro de irregularidades—actualización de los registros y la supresión de todas las tarjetas SIM con registros fraudulentos/sospechosos
- Programas amplios de capacitación de agentes en los procesos de registro de abonados
- Ejecución de cumplimiento de agentes por medio de encuestas de cliente desconocido (mystery shopper, en inglés), comprobaciones del sistema, sanciones a agentes, etc.
- Asegurar que los procesos de archivado automático y recuperación de documentos funcionan
- Cooperar con las autoridades de control legal para hacer cumplir la ley a través de la provisión de información necesaria que facilite la rápida conclusión de las investigaciones relacionadas con el terrorismo.

Conclusión

El terrorismo sigue siendo una gran amenaza para la paz mundial, y en estas circunstancias, los operadores de redes móviles seguirán siendo claves en las iniciativas mundiales de la lucha contra el terrorismo.

La legislación de ALD/CTF en la mayoría de las jurisdicciones da amplios poderes a las autoridades de control legal, que les permite cumplir la ley, lo que permite inspecciones sorpresa, investigaciones exhaustivas de pruebas que toman, la detención y el enjuiciamiento, seguimiento, embargo y decomiso de bienes y demás activos del delito.

En este caso, no hay necesidad de probar la comisión de un delito real; la sospecha razonable de que un delito se ha cometido es suficiente.

Sin embargo, en muchos casos, la pronta investigación y resolución de los casos se ve obstaculizada por la falta de leyes eficaces de ALD/CTF, la falta de capacidad regulatoria y judicial para poner en marcha las leyes pertinentes y adjudicar casos bajo la ley, la aplicación ineficaz de las leyes donde las hay, y las instituciones que carecen de infraestructura adecuada y la capacidad técnica para monitorear y detectar el lavado de dinero o financiamiento de la sospecha del terrorismo/actividad terrorista.

Tomando nota del papel fundamental que desempeñan los operadores de redes móviles en la guerra contra el terrorismo, es de suma importancia que se pongan en marcha los mecanismos adecuados para garantizar la integridad de los datos del suscriptor, en cumplimiento de la legislación vigente y para facilitar la vigilancia y detección de actividades sospechosas en sus redes. Por la misma razón, los reguladores deben introducir una legislación que hará que el registro de abonados sea obligatorio y facilite la aceptación de los registros de abonados como prueba en los juicios relacionados con el terrorismo.

Mercy W. Buku, CAMS, consultora de ALD/CFT de pagos móviles, CGAP, Nairobi, Kenia, mwbuku@gmail.com

[8] Mwende Gatabaki, "National Digital Service," http://www.cofek.co.ke/National%20Digital%20Registry%20Service.pdf

[9] Megan Geuss, "MasterCard-backed biometric ID system launched in Nigeria,"*ArsTechnica*, 2 de septiembre del 2014, http://arstechnica.com/business/2014/09/02/mastercard-backed-biometric-id-system-launched-in-nigeria/

[10] Cyrus Farivar, "Egypt wants digital ID cards for 85 million people," *ArsTechnica*, 7 de junio del 2012, http://arstechnica.com/business/2012/06/07/egypt-wants-digital-id-cards-for-85-million-people/

[11] Mugambi Mutegi, "New digital registry to limit identity theft, catch aliens (Kenya)," Asoko Insight, 12 de marzo del 2015, http://asokoinsight.com/news/new-digital-registry-limit-identity-theft-catch-aliens-kenya/

John Riggi:

"¿Estamos avanzando lo suficientemente rápido?"

ACAMS Today tuvo el privilegio de hablar con John Riggi, un veterano del FBI condecorado, con 27 años de experiencia, y quien actualmente se desempeña como Jefe de Sección de la División de la Sección de Extensión Cibernética donde lidera el desarrollo de la misión de asociaciones críticas con el sector privado.

Anteriormente, Riggi sirvió como Agente Especial Adjunto a Cargo de la División de Inteligencia de la Oficina de Campo de Washington. En 2013 Riggi fue seleccionado para liderar el desarrollo del Equipo Cibernético de Seguimiento Financiero del FBI. Anteriormente, Riggi sirvió durante cuatro años como gerente nacional de operaciones para la Sección de Operaciones de Financiación del Terrorismo (TFOS) del FBI y dos años en el Centro de Contraterrorismo (CTC) de la CIA.

Antes de emplearse como gerente nacional de operaciones, Riggi sirvió durante 16 años en la Oficina de Campo del FBI de Nueva York como Agente de Caso, Supervisor del Grupo de Tareas del Área de Criminalidad Financiera de Alta Intensidad (HIFCA) y Supervisor del Escuadrón de Financiamiento del Terrorismo. En Nueva York, desarrolló y dirigió la primera operación encubierta del FBI contra el delito organizado ruso, fue el primero en utilizar una operación encubierta en transacciones de lavado de dinero en casos de financiamiento del terrorismo e inició el caso de financiación del terrorismo de la Alavi Foundation, que resultó en la mayor incautación de activos de contraterrorismo en la historia de los EE.UU. Riggi también actuó en calidad de agente encubierto haciéndose pasar por un lavador de dinero de delito organizado para penetrar y exponer la industria del cheque comercial de cobro de miles de millones de dólares en la ciudad de Nueva York y su conexión con la delincuencia organizada, el lavado de dinero y la corrupción bancaria. Además, Riggi sirvió como operador en el equipo SWAT del FBI de Nueva York durante ocho años. Riggi comenzó su carrera como un Agente Especial del FBI en la oficina de Birmingham en 1988.

Por otra parte, Riggi es recipiendario del Premio del Director del FBI, por dirigir un programa reservado de interdicción del financiamiento terrorista con gran éxito, que fue responsable de la prevención de varios ataques terroristas a un aliado extranjero. Riggi es también recipiendario del *Premio George H.W. Bush a la Excelencia en Contraterrorismo* de la CIA, el premio más alto de contraterrorismo de la CIA, por expandir en gran medida las operaciones antiterroristas conjuntas y la cooperación del FBI/CIA.

ACAMS Today: Usted ha tenido una impresionante carrera en el sector público, ¿cuándo supo que quería formar parte del FBI?

John Riggi: Bueno, supongo que tuve suerte en ese aspecto. Desde niño, me parecía tener un interés innato en el control legal. Crecí en una ciudad obrera sólida, pero dura, la de Lynn, Massachusetts, que se encontraba en medio de una tremenda transición en ese momento. Había una gran interacción entre la policía y la comunidad. Vi a la gente del lado correcto de la ley y del lado equivocado. Algunos de los papás de mis amigos eran agentes de policía y los héroes del barrio. Al entrar a la escuela secundaria, me di cuenta de que quería hacer algo más: participar en el control legal a nivel nacional y hacerles frente a los problemas de la delincuencia más importantes para el país. El FBI parecía la elección lógica para mí. Fui realmente afortunado en poder hacer realidad ese objetivo, y después de 27 años en el FBI, todavía estoy agradecido por el privilegio que tengo de servir.

AT: ¿Cuál caso ha sido el más memorable y por qué?

JR: Si no le importa, me gustaría destacar dos casos, que ilustran la importancia de "seguir el dinero" en casos de delincuencia y de terrorismo. A mediados de la década de 1990, mientras investigaba las conexiones internacionales entre los grupos del delito organizado italiano y ruso, desarrollé y conduje la primera operación encubierta del FBI contra el delito organizado ruso. Al trabajar con un gran equipo de agentes encubiertos del FBI, pudimos infiltrarnos en una vasta red de lavado de dinero operada por delincuentes rusos, haciéndonos pasar por miembros de la delincuencia organizada italiana que buscaban la ayuda del grupo del delito organizado ruso para el lavado de dinero del narcotráfico. La operación duró tres años, en los que se utilizó la provisión de operación encubierta de la ley de lavado de dinero para permitir que millones de dólares de los fondos del gobierno, presentados como ganancias de la droga, "pasearan" y se lavaran por medio de la red rusa. Con la estrecha colaboración de las instituciones financieras, pudimos rastrear el movimiento de los fondos del gobierno a través de la red delictiva, lo que llevó a la identificación de los métodos de lavado de dinero, los co-conspiradores, la interconexión entre los grupos del delito organizado y el fraude de atención médica, y la complicidad de empleados bancarios corruptos. Todos los acusados fueron enjuiciados con éxito y millones de dólares de activos de origen delictivo fueron incautados por el gobierno.

Diez años más tarde, cuando era gerente nacional de operaciones para la TFOS del FBI, tuve la oportunidad, de nuevo, con un gran equipo, incluidos socios del sector financiero, de liderar el desarrollo de una operación altamente reservada de financiación del terrorismo. Lo que puedo decir sobre el caso es que mediante el uso de técnicas de investigación financieros estándar, combinadas con técnicas y autoridades de inteligencia, fuimos capaces de rastrear e interceptar los fondos destinados a una organización terrorista. Los fondos iban a ser utilizados para atacar un país aliado. Como resultado de la operación y la inteligencia obtenida de ella, se identificó y se interrumpió la red, lo cual dio lugar a una marcada disminución de los ataques terroristas en el país aliado.

AT: ¿Qué alianzas ha ayudado a crear entre los sectores público y privado?

JR: De las investigaciones de lavado de dinero a las investigaciones de financiamiento del terrorismo, siempre entendí que nosotros, el FBI, no podríamos hacer nuestro trabajo con éxito sin la ayuda y la colaboración del sector financiero. Si se trataba de un reporte de operaciones sospechosas (ROS) de un grupo de revisión en Nueva York, el establecimiento de grupos de trabajo de delitos financieros reservados o no a nivel nacional, o de personal de confianza en las principales instituciones financieras, todos han demostrado ser muy valiosos para la misión del FBI. Así que, cuando llegué a mi nuevo rol de jefe de la Sección de Extensión Cibernética del FBI, tenía un profundo conocimiento y apreciación del valor de las relaciones efectivas del sector privado.

Las asociaciones eficaces y de confianza con el sector privado, a través de todos los sectores de infraestructuras críticas no sólo se valoran en cibernética, sino que resultan fundamentales y esenciales para nuestra misión crítica en la lucha contra las amenazas cada vez mayores y complejas a la seguridad nacionales y por parte de ciberdelincuentes que enfrenta nuestro país. Uno de los programas que tengo el privilegio de supervisar es el programa InfraGard, una organización tipo 501(c)(3) sin fines de lucro con 36.000 oficiales, patrocinada por la División Cibernética del FBI. InfraGard es una organización donde ciudadanos voluntarios individuales ("Patriotas", como me gusta llamarlos), se reúnen en 83 capítulos en todo el país con el objetivo común de intercambiar información sobre amenazas entre sí y con el FBI, para ayudarnos a defendernos mutuamente y a la nación contra todo tipo de amenazas.

Además del programa de InfraGard, nosotros en la División Cibernética realizamos rutinariamente extensiones a socios clave del sector privado para establecer relaciones de confianza, ofrecemos sesiones de información de amenazas de anuncios cuando resulta apropiado y facilitamos el intercambio de información sobre amenazas cibernéticas.

AT: ¿Qué recomendaciones tiene sobre cómo construir y mantener relaciones público-privadas?

JR: Yo realmente creo que el gobierno debe entender y apreciar el valor de las asociaciones con el sector privado y de lo fundamental que esas relaciones resultan para la misión central de la defensa del país. Entonces, la institucionalización de esa filosofía a través de programas de divulgación formales y centralmente coordinados y seleccionando individuos con habilidades interpersonales excepcionales para desarrollar y mantener las relaciones del sector privado resultan críticos para defender el país de la amenaza cibernética. Creo que en el gobierno nos estamos moviendo en la dirección correcta, especialmente en términos de la amenaza cibernética, donde se encuentran en marcha grandes esfuerzos para crear un entorno estructural y legal propicio para el intercambio de información entre el sector privado y el gobierno. La pregunta, que sólo el futuro puede responder, es "¿Estamos avanzando lo suficientemente rápido?"

AT: ¿Cómo se ha incrementado el riesgo cibernético en los últimos dos años?

JR: Tanto la seguridad nacional como las amenazas cibernéticas delictivas a los EE.UU. han aumentado de forma exponencial en los últimos dos años, e incluso en los últimos seis meses. La gama de actores que amenazan nuestros intereses es tan compleja como variada. Nos enfrentamos a ciberterroristas, que pretenden utilizar nuestra dependencia y uso de sistemas digitales para promover sus objetivos políticos o ideológicos. Nos enfrentamos a estados nacionales, que tienen como objetivo utilizar el mundo cibernético para realizar espionaje, para hacer preparativos de guerra y que incluso pueden llevar a cabo actos de guerra a través de medios cibernéticos. Nos enfrentamos a delincuentes impulsados ideológicamente, que pueden utilizar métodos tales como ataques de denegación de servicio, conocidos como ataques DDoS, para promover su propia ideología o causa social. Nos enfrentamos a amenazas internas, cuyo acceso legítimo a la información sensible puede ser utilizado para diversos fines ilícitos. Por último, nos enfrentamos a grupos e individuos motivados financieramente, que utilizan una variedad de métodos para enriquecerse a costa de los demás.

La amenaza de los actores cibernéticos sigue cosechando una parte creciente de la atención de los medios y sigue avanzando en sofisticación, basta con ver los titulares. Recientes ataques de alto perfil, tales como los de los sectores minorista, financiero, de entretenimiento y de la salud, destacan las vulnerabilidades en algunas de las compañías más grandes de nuestro país. Seguimos trabajando en estrecha colaboración con el Servicio Secreto, el DHS y otros asociados de todo el gobierno. Robos de puntos de venta, también conocidos como estafas de puntos de venta, por ejemplo, no son nuevos, pero siguen planteando serias amenazas para la industria de servicios financieros. Según el informe de 2014 de investigaciones de la violación de datos de Verizon, la instalación física de un "skimmer" en un cajero automático, estación de servicio, o terminal de POS para leer los datos de tarjetas de crédito se ha centrado en los cajeros automáticos con una abrumadora especificidad: el 87 por ciento de los ataques de skimming en 2013, por ejemplo, fueron en cajeros automáticos. Estafas de punto de venta al por menor, donde los atacantes comprometen las computadoras y servidores que ejecutan aplicaciones de punto de venta con la intención de capturar los datos de pago, comprenden un nivel adicional de sofisticación y pueden tardar semanas o incluso meses en ser descubiertos, y mucho menos mitigado.

Las botnets, que pueden aprovechar el poder de una enorme red de computadoras con fines maliciosos, continúan evolucionando también. Mientras hablo, las estimaciones sitúan el total de daños causados por botnets en más de $9 mil millones en pérdidas a los estadounidenses víctimas y más de $110 mil millones en pérdidas en todo el mundo. Aproximadamente 500 millones de computadoras están infectados por año en todo el mundo, lo que se traduce en 18 víctimas por segundo. Como las botnets se vuelven más sofisticadas, nuestras técnicas deben evolucionar para mantener el ritmo. El FBI y nuestros socios pueden acabar con una botnet, por ejemplo, pero los programadores pueden alterar el código y reconstruir sus bots en un plazo bastante corto. El poder y la escala de las botnets es particularmente digno de mención, ya que las botnets se han utilizado para atacar el sector financiero a través de ataques DDoS y el FBI ha estado profundamente involucrado en la prevención de este

tipo de ataques y en impedir que este tipo de ataques inflijan un daño duradero. A partir de septiembre de 2012, por ejemplo, hubo agentes que lanzaron potentes ataques DDoS desde una botnet, que combinaba el ancho de banda de numerosos servidores para alcanzar las principales instituciones bancarias estadounidenses. El FBI trabajó en estrecha colaboración con el Departamento de Seguridad Nacional (DHS) para emitir Boletines Indicadores Conjuntos (JIB) a los bancos de los EE.UU., que incluyeron miles de direcciones de IP que participaron en los ataques. Los bancos estadounidenses utilizaron las direcciones de IP para mitigar mejor los incidentes futuros, lo que ayuda a garantizar que sus operaciones comerciales podrían proceder con menos interrupciones de servicio a sus clientes. Los JIB ayudaron a reducir los recursos disponibles para que los actores de amenazas lleven a cabo futuras operaciones DDoS y demostraron la eficacia de la divulgación del FBI a la industria. A lo largo de esta campaña, el FBI llevó a cabo importantes esfuerzos de difusión para informarles a los defensores de redes de bancos por medio de una serie de informes reservados. Estos informes, realizados por el FBI, DHS, y representantes del Tesoro, le dieron al personal de seguridad del banco el contexto de la amenaza del DDoS y permitieron a los bancos compartir las mejores prácticas con sus compañeros en tiempo real.

AT: ¿Qué pueden hacer los profesionales de la prevención del delito financieros para prepararse frente a ataques cibernéticos?

JR: Voy a responderlo en el contexto de lo que los profesionales pueden hacer para "prevenir y prepararse" contra un ataque cibernético. En primer lugar, ser muy conscientes de que personalmente podrían estar específicamente elegidos para un ataque cibernético, o pueden ser usados, sin saberlo, como un vector para entregar el malware en la institución financiera, en base a su posición y nivel de acceso a los datos críticos. Minimizar su perfil de redes sociales en línea, que puede dar pistas a los "chicos malos" en cuanto a su acceso a los datos. Creo que la estrecha adhesión a las políticas de seguridad de la información de las instituciones, que tienen buenas prácticas de seguridad cibernética en los dispositivos informáticos personales, y por supuesto, aseguran que los datos críticos estén siempre en copia de seguridad en los sistemas o dispositivos independientes son componentes clave para la prevención y la preparación para un ataque cibernético. Además, reportar siempre la actividad del equipo sospechoso y correos electrónicos a los departamentos de seguridad y nunca hacer clic en cualquier enlace sospechoso incrustado en un correo electrónico o visitar sitios web sospechosos.

AT: ¿Cuáles son las más importantes alertas rojas que una institución financiera debe tener en cuenta cuando se trata del riesgo cibernético?

JR: El riesgo es en realidad doble: existe el riesgo a la institución y el riesgo para sus clientes. En términos de riesgo cibernético institucional, los departamentos de seguridad de las principales instituciones financieras son muy eficaces en el trato con los aspectos técnicos del riesgo. Correos electrónicos de "spear phishing" siguen siendo el método de entrega más común de malware en cualquier tipo de institución, financiera o de otro tipo. Correos electrónicos sospechosos, la actividad del equipo inusual, una disminución en el rendimiento y la velocidad en los sistemas o dispositivos individuales, exfiltración de datos sin explicación, la progresividad no autorizada de los privilegios del sistema para los usuarios, o anomalías de sitios web pueden ser indicadores de una amenaza cibernética institucional.

En términos de riesgo cibernético a los clientes hay cuentas de las que se apoderan, skimming de cajeros automáticos y fraudes relacionados con robos de identidad que son comunes y siguen aumentando. Algunos indicadores consisten en la transferencia de varias cuentas a una cuenta interna común, seguidas por o bien retiros inmediatos o bien transferencias bancarias extranjeras; transferencias inusuales de una cuenta interna a una de Europa del Este, Rusia o China; disminución de una cuenta a través de múltiples retiros en cajeros automáticos o retiros en cajeros automáticos extranjeros; una cuenta que recibe la devolución de impuestos de varios individuos; varias cuentas que se registran en la misma dirección IP o inicios de sesión de la dirección IP externa inusuales. Estas son sólo algunas de las cosas por las que los clientes y las entidades financieras deben estar en alerta.

AT: En su experiencia, ¿cuál ha sido el hilo conductor para frustrar planes criminales?

JR: Los ingredientes comunes que he visto en los casos de éxito en mis más de 27 años en el FBI han incluido una gran alianza y el intercambio de información con el sector privado, la transparencia y la cooperación entre los organismos gubernamentales, la incorporación de técnicas de inteligencia y la aplicación de técnicas de investigación financiera, independientemente de la violación.

AT: ¿Cómo ha evolucionado la lucha contra el terrorismo en los últimos cinco años?

JR: Eso podría ser objeto de una entrevista o de un libro totalmente diferente, en realidad. En general, hemos visto disminuir la amenaza estratégica al país planteada por el núcleo de al-Qaeda como resultado de su destrucción por las operaciones de contraterrorismo altamente eficaces del gobierno de los EE.UU. Esa es la noticia buena. La mala es que hemos visto el surgimiento de otras organizaciones terroristas con base regional, tales como ISIS, inspirar a occidentales a través de la Internet para unirse a ellos en Siria o llevar a cabo ataques en sus países de origen. El uso de la Internet para reclutar, radicalizar y difundir técnicas terroristas, tácticas y procedimientos ha crecido enormemente. Hemos visto que organizaciones como ISIS demuestran cierta capacidad para conducir desfiguraciones de sitio web. Pero hasta ahora, no han demostrado poder llevar a cabo intrusiones informáticas.

AT: ¿Hay algún otro consejo que le gustaría compartir con los lectores de *ACAMS Today?*

JR: El gobierno solo no puede defenderse contra la multitud de amenazas cibernéticas, el terrorismo, la seguridad nacional y las amenazas delincuenciales que enfrenta la nación. La colaboración, la cooperación y el intercambio de información es clave entre el gobierno y el sector privado y entre los diversos componentes internos de las instituciones financieras (especialmente con los profesionales de seguridad de la información). Al participar en la colaboración y el intercambio de información vertical y horizontal, que no sólo ayuda en la defensa de su institución y de los clientes, usted nos ayuda a defender la nación.

Gracias por la oportunidad de hablar con ustedes hoy, y ustedes, mis amigos y colegas, gracias, por todo lo que hacen.

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

DETECTANDO AL ENEMIGO INTERNO

Los titulares de los periódicos y los noticieros nocturnos están llenos de historias que relatan los recientes ataques o ataques evitados de lobos solitarios, células terroristas y combatientes terroristas extranjeros. Todos son parte de la creciente amenaza del terrorismo de cosecha propia en los EE.UU. y la detección de estos terroristas antes de que ataquen presenta desafíos únicos. Para identificar con éxito a un terrorista de cosecha propia y ser capaz de detener un ataque antes de que suceda, los profesionales de cumplimiento y autoridades de control legal deben trabajar juntos.

Lobos solitarios y manadas de lobos

Si bien los ataques de un lobo solitario o de una manada—generalmente consisten en un grupo de seis o menos—se llevan a cabo por pocas personas con relativamente pequeñas cantidades de dinero, el daño que causan puede ser masivo. El tiroteo de octubre 2014 de un soldado canadiense delante del edificio del Parlamento en Ottawa; el asesinato de marzo de 2011 de dos miembros de las fuerzas armadas estadounidenses en el Aeropuerto de Frankfurt por un hombre que fue empujado a la acción por la propaganda terrorista; y la matanza de noviembre de 2009 de 13 personas y las heridas a otras 32 personas en Fort Hood en Texas son sólo algunos ejemplos de la devastación causada por un solo individuo. Los atentados de julio de 2005 de los subterráneos en Londres, que dejaron 56 muertos y 700 heridos y las 17 personas que murieron durante los ataques de enero de 2015 en París son claros ejemplos de lo que los grupos pequeños pueden hacer.

La razón por la que es difícil identificar a los terroristas de cosecha propia se resumía en un discurso de junio de 2006 del entonces director de la Oficina Federal de Investigaciones, Robert S. Mueller, III, en relación con un atentado terrorista frustrado en Toronto. "Al igual que los terroristas responsables de tanto el atentado de Londres como de los atentados de Madrid, los sospechosos de Toronto vivían en la zona en la que tenían la intención de atacar", dijo Mueller. "No eran agentes durmientes enviados a misiones suicidas; eran estudiantes y gente de negocios y miembros de la comunidad. Eran personas que, por cualquier razón, vinieron a ver su país de origen como el enemigo".[1]

Además de ser capaces de mezclarse con la comunidad en la que viven, las alertas rojas habituales que apuntan a una posible actividad terrorista no se encuentran en un escenario de lobo solitario. Este tipo de terrorismo puede ser autosostenido y no busca una fuente de financiamiento externo, de acuerdo con Mike Loughnane, un consultor de financiación del terrorismo y el instructor senior de Innovative Analytics and Training LLC., donde capacita a estudiantes del gobierno, de defensa y del sector privado en financiación de antiamenazas. Loughnane aprovecha sus 27 años de experiencia en la investigación de delitos financieros con la Oficina del Inspector General del Departamento de Transporte y la Agencia de Protección Ambiental para proporcionarles a sus alumnos las herramientas necesarias para encontrar patrones de financiación de amenazas o, en otras palabras, "una aguja en un pajar de agujas".

"Desde una perspectiva de identificación ellos [los terroristas lobo solitario] son difíciles de detectar porque saben que para lograr lo que quieren tienen que permanecer fuera del radar", dijo Loughnane. "Viven en general en un ambiente tan tranquilo, que se hace difícil encontrar cualquier cosa que los distinga. Si están en un grupo, es generalmente pequeño. No necesitan redes sociales para comunicarse, pueden reunirse personalmente".

Debido a que no dependen de las redes sociales para la comunicación o la recaudación de fondos, los terroristas lobo solitario a menudo no dejan una huella en línea rastreable por la policía. En lugar de ver las alertas rojas tradicionales, los profesionales de cumplimiento de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) y las autoridades de control legal deben trabajar en estrecha colaboración con una amplia gama de partes interesadas para detectar esta amenaza. El trabajo comienza con el personal de cumplimiento que debe detectar la actividad inusual y reportarla a la policía para su investigación. "Las autoridades de control legal occidentales tienen una estructura reactiva que se basa en los derechos constitucionales y el derecho a la privacidad", dijo Loughnane. "Las instituciones financieras son las primeras en responder tanto por negocios como por razones regulatorias. Deben ser el actor y entonces la ley responde".

La colaboración no termina con la detección de la posible actividad terrorista. Durante la investigación, las autoridades de control legal pueden obtener información valiosa al trabajar en estrecha colaboración con la entidad financiera. En cuanto a las transacciones financieras de un sospechoso al ver no sólo lo que compró, sino dónde lo compró y cómo encaja en el área en la que el potencial terrorista vive y trabaja puede descubrir alertas rojas ocultas. "Esa es una de las lecciones aprendidas de [el terrorista de Oklahoma City] Timothy McVeigh", dijo Loughnane. "Busque la anomalía. Tendría que haber sido detectada, no sólo por la cantidad de fertilizante que compró, sino también por su compra de fertilizantes de calidad comercial".

Las instituciones financieras son las primeras en responder tanto por negocios como por razones regulatorias

Producto nacional y educado en el extranjero

Los combatientes terroristas extranjeros (FTF) son individuos que se radicalizaron en los EE.UU. por la propaganda en línea, por lo general a través de las redes sociales, que viajan al extranjero para entrenarse y pelear. Luego regresan a los EE.UU., con el objetivo de llevar a cabo atentados terroristas en el país. "Vuelven con nuevos conjuntos de habilidades y con las preocupaciones ideológicas [del grupo yihadista]", dijo Loughnane. "Han crecido en el grupo y pueden actuar de manera más agresiva en casa".

Diferente del lobo solitario, los FTF suelen dejar una huella muy grande en línea a medida que se adoctrinan y recogen información sobre cómo unirse a los campos de entrenamiento del grupo terrorista. Los FTF también tienen patrones financieros comunes que pueden servir como alertas rojas para las instituciones financieras y las autoridades de control legal.

[1] Robert S. Mueller, Discurso sobre la amenaza de terrorismo de cosecha propia, la Oficina Federal de Investigación, 23 de junio del 2006, http://www.fbi.gov/news/speeches/the-threat-of-homegrown-terrorism

Las alertas por buscar son:

- Actividades inusuales de recaudación de fondos, especialmente con adolescentes y adultos jóvenes. "ISIL les da instrucciones muy específicas—depende de ti financiarte y llegar hasta aquí", dijo Loughnane. "Se puede ver un patrón en el que están poniendo o recibiendo dinero de una manera diferente del pasado. Hay que preguntarse si la actividad es coherente con la persona que se dice ser";
- La compra de billetes de avión a Siria u otras áreas que rodean el territorio controlado por el Estado Islámico de Irak y el Levante (ISIL);
- Una reciente solicitud de pasaporte; y
- Llamadas o excursiones a puntos de comunicación centralizados conocidos de la banda terrorista en los EE.UU.

Incluso si no levantan alertas rojas antes de salir de los EE.UU., los FTF pueden detectarse por su financiación y gasto, mientras que en el extranjero o una vez que regresan a los EE.UU. De acuerdo con Jeff Ross, vicepresidente senior, BSA/ALD de la Oficina de Control de Activos Extranjeros (OFAC) y oficial de Green Dot Corporation/Green Dot Bank, otras alertas rojas que se deben buscar son:

- Las aberraciones en cualquier gasto extranjero o patrones de carga de tarjetas de prepago o cuentas que puedan tener.
- El lugar donde las tarjetas de prepago se compran, cargan y utilizan. Hay que fijarse, tanto en cuanto a las tarjetas adquiridas y cargadas en los EE.UU. como con retiros en lugares del extranjero y también las tarjetas de prepago Discover/Mastercard/Visa emitidas por bancos extranjeros y cargadas a través de transferencias del exterior pero que realizan transacciones en los EE.UU. Ross se muestra particularmente enfático en que las autoridades de control legal estadounidenses tienen que tener una firme comprensión de todas las tarjetas recargables emitidas en el exterior y con los programas de tarjetas de prepago que podrían estar haciendo negocios en los EE.UU.
- El dinero transferido a una cuenta de tarjeta de prepago o cuenta bancaria o emitida o establecida en los EE.UU. desde una ubicación externa.

De acuerdo con Steve Gurdak, supervisor de un equipo de revisión de reportes de operaciones sospechosas (ROS) en Virginia y ex detective de la policía con 30 años de experiencia especializado en delitos financieros, otras alertas rojas incluyen:

- Actividades de cuenta que no coinciden con el cargo del titular de la cuenta, por ejemplo, un estudiante con numerosas transferencias electrónicas en y retiros de efectivo, pero no los gastos de educación;
- Empleo no verificable dentro de una comunidad étnica; y
- Titulares de cuentas apoyados por otro sin razón obvia. "Si no es familiar, la motivación debe ser considerada o investigada", dijo Gurdak. "Una vez más, necesita investigarse los detalles de quién, cómo y por qué los gastos de subsistencia se están pagando".

Para ayudar a reconocer al terrorista potencial de cosecha propia, Gurdak recomienda que las instituciones financieras construyan una relación con las autoridades de control legal para lograr capacitación. "El coentrenamiento con las autoridades de control legal para reconocer esta actividad ofrece la oportunidad a cada parte (aplicación de la ley y el cumplimiento de BSA/ALD) para aprender del otro", dijo Gurdak.

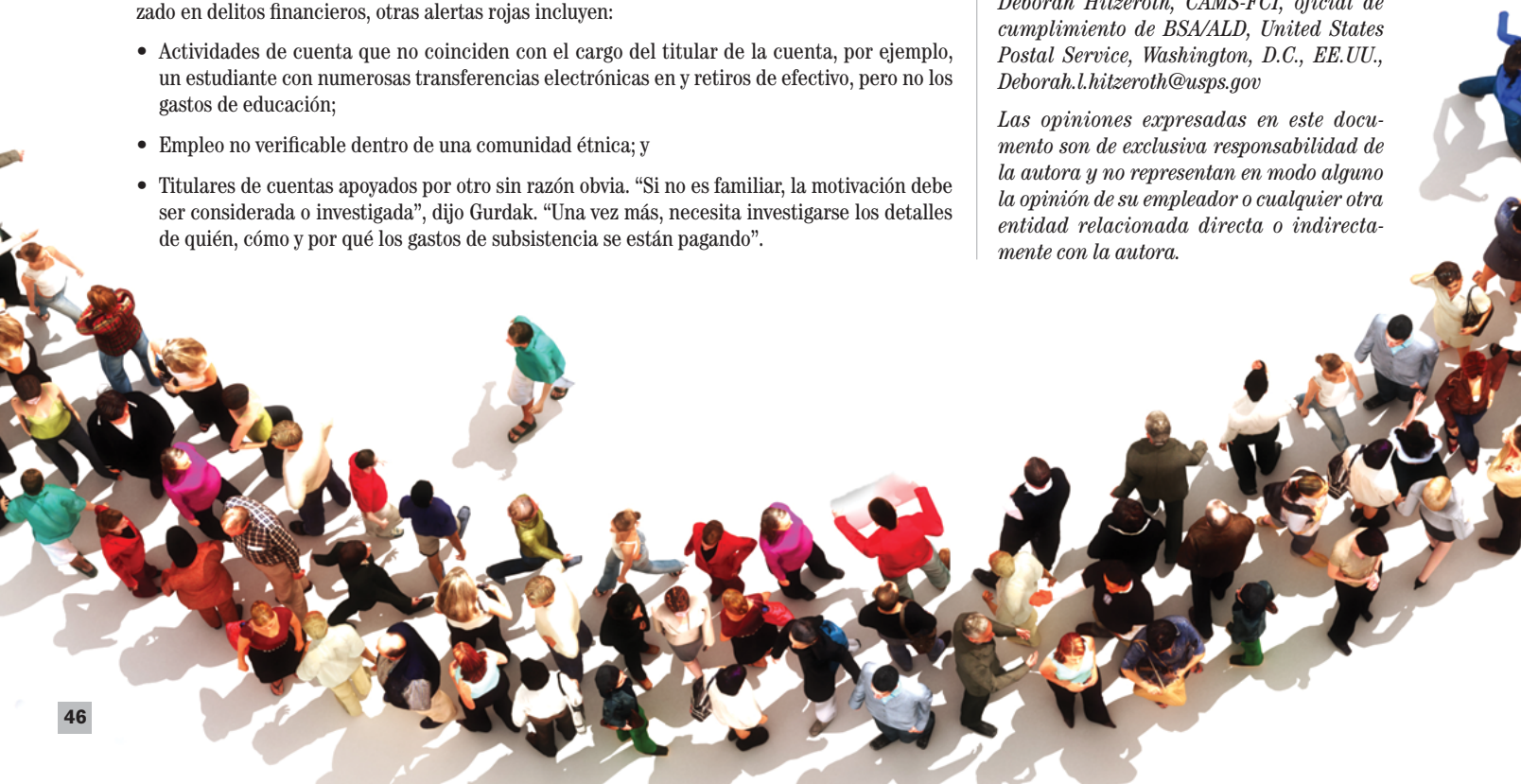
Es un esfuerzo conjunto

Con el llamado de ISIL pidiendo seguidores dentro de los países occidentales para lanzar ataques contra los militares, el gobierno y la población civil, el problema de los ataques terroristas de cosecha propia seguirá creciendo. Los profesionales de control legal y de cumplimiento en las instituciones financieras necesitan conocer los signos sutiles que apuntan a un terrorista de cosecha propia y estar dispuestos a trabajar en estrecha colaboración para detectar y detener un ataque potencial.

"Sea más consciente de los signos y los indicadores y patrones", dijo Loughnane. "Aprender de nuestros errores del pasado y de nuestros éxitos pasados y compartir esa y nueva información con el grupo más grande posible es aumentar el esfuerzo de colaboración". A

Deborah Hitzeroth, CAMS-FCI, oficial de cumplimiento de BSA/ALD, United States Postal Service, Washington, D.C., EE.UU., Deborah.l.hitzeroth@usps.gov

Las opiniones expresadas en este documento son de exclusiva responsabilidad de la autora y no representan en modo alguno la opinión de su empleador o cualquier otra entidad relacionada directa o indirectamente con la autora.



REAL WORLD. REAL CRIMES. REAL...

HEROES

Do you know someone who should be recognized for their achievements that has significantly contributed to the fight against financial crime?

Nominate them for an ACAMS Recognition Award

2014 Award Winners

AWARD CATEGORIES

ACAMS
AML Professional of the Year Award

ACAMS TODAY
Article of the Year

ACAMS
Al Gillum
Volunteer
OF THE YEAR

Nominate your peers on acamsglobal.org/2015/awards.asp
Deadline for submissions is July 31, 2015

For nomination questions contact:
AML Professional of the Year
Karla Merrell | kmerrell@acams.org | +1 786.507.4430

ACAMS Today Article of the Year
Karla Monterrosa-Yancey | editor@acams.org | +1 786.871.3064

Recipients will be recognized at the ACAMS 14th Annual AML & Financial Crime Conference in Las Vegas on September 29, 2015, in the *ACAMS Today* magazine and on acamsglobal.org.

Una era de **ciberguerras** y conciencia de la **seguridad**

En una era en que los países están en una nueva carrera armamentista, no por territorio o armas, sino por los hackers informáticos o los atacantes, la guerra estalla. Algunos atacantes están asignados a infiltrarse en redes extranjeras para exponer y prevenir ataques terroristas, mientras que otros están a cargo de poner en peligro los números de Seguro Social y venderlos al mejor postor.

Las violaciones de la seguridad de las computadoras empeoran todos los años. En 2013, el número total de infracciones fue de 62 por ciento más que en 2012.[1] La tendencia continuó en 2013-2014 con infracciones en compañías de Fortune 500, como Sony, Home Depot, Target y JPMorgan. Ahora, el 2015 comenzó con una de las peores violaciones de la industria financiera con el ataque cibernético del malware Carbanak. Estos son los hechos que hacen los titulares y nos recuerdan que la seguridad informática es real y necesaria.

Como los ataques cibernéticos siguen ocurriendo, los legisladores y las autoridades de control legal han comenzado a hacer la ley del delito cibernético un punto focal. La promulgación de leyes como la Ley del Patriota permite a las autoridades de control legal de los EE.UU. vigilar las comunicaciones de Internet para interceptar y potencialmente prevenir los ataques cibernéticos. Cuando se produce un ataque de interés, los funcionarios encargados de hacer cumplir la ley asignarán investigadores especializados y expertos forenses digitales al caso en los intentos de identificar y procesar al atacante o los atacantes.

Con la gran cantidad de información sensible y de identificación personal (por ejemplo, la fecha de nacimiento, números de Seguro Social y cuentas bancarias) almacenados en una variedad de entornos informáticos, la protección es crucial. Este artículo analiza las metodologías de ataque comunes, vectores de ataque y las mejores prácticas para protegerse de estas amenazas.

Metodologías y vectores de ataque comunes

Los atacantes utilizan una variedad de técnicas para infiltrar los entornos de la red. Cada metodología se caracteriza por su serie de desafíos y depende en gran medida del entorno de destino. Algunos ataques comunes utilizados para infiltrar entornos implican software obsoleto, seguridad de la contraseña y la ingeniería social.

Software anticuado

Los atacantes suelen comenzar enumerando un entorno para ejecutar servicios y/o software. Si identifican un servicio o software obsoleto, la investigación comienza a buscar vulnerabilidades y puntos flojos

[1] Symantec, "2014 Internet Security Threat Report," http://www.symantec.com/security_response/publications/threatreport.jsp

“El mundo ya no está dirigido por las armas o energía, o dinero. Está dirigido por los ínfimos unos y ceros, pequeños trozos de datos.”

—*Sneakers* (1992)

existentes. Un atacante crea o bien modifica un punto flojo existente del sistema informático que contiene el software obsoleto. Una vez que el ataque se ha ejecutado con éxito, el atacante obtendrá un punto de entrada y, posiblemente, se infiltrará en el sistema de ordenador en su totalidad. Un ejemplo real de una componenda debida al software obsoleto es la violación de Sony PlayStation.

En 2011, los atacantes comprometieron aproximadamente 77 millones de cuentas de la red de Sony PlayStation debido al software obsoleto.[2] Los atacantes aprovecharon el servicio de Apache[3] para infiltrarse en las redes de Sony, exponer información de tarjetas de crédito de los usuarios y negar la disponibilidad de la red PlayStation. Sony reveló una pérdida de $171 millones debido al ataque cibernético.[4]

Seguridad de la contraseña

Según la investigación de SplashData, la contraseña más común durante tres años consecutivos es 123456.[5] Un atacante con el último hardware descifrador de contraseñas puede romper esa contraseña en 0,0000111 segundos, si no más rápidamente. Los usuarios que utilicen esta o contraseñas similares deben cambiar sus contraseñas de inmediato.

De manera similar a la metodología del software obsoleto, los atacantes enumeran el medio ambiente y los servicios de red. Una vez que un servicio que requiere autenticación se identifica, un atacante procederá a tratar de adivinar la contraseña. Un atacante suele comenzar adivinando las contraseñas por defecto para el servicio respectivo y luego procede con el enfoque de fuerza bruta. Los ataques de fuerza bruta en este contexto son un intento de obtener acceso no autorizado a un servicio utilizando varias combinaciones de contraseñas junto con herramientas automatizadas. Con el hardware adecuado, los ataques de fuerza bruta pueden lograr más de mil millones de contraseñas por segundo.

Ingeniería social

La ingeniería social es el uso de la influencia y la persuasión para manipular a personas para que revelen información confidencial. Los métodos comunes de ingeniería social incluyen llamadas pretexto, los correos electrónicos de phishing y entregas de USB.

Imagínese atacantes que pueden obtener contraseñas o incluso información de la cuenta bancaria con solo pedirla. Este es el arte de las llamadas pretexto. La llamada pretexto es un ejemplo perfecto de cómo un atacante puede obtener información sensible sin el uso de la tecnología. En 2011, Microsoft informó que varios atacantes estaban suplantando a representantes de Microsoft cuando hacían llamadas pretexto.[6] Los atacantes pasaban por representantes de Microsoft y llamaban a individuos al azar, notificándoles de una supuesta infección de su computadora y cobrando por la "solución del problema o problemas".

Los correos electrónicos de phishing son casi idénticos a su contraparte. Los atacantes pueden enviar correos electrónicos diseñados para parecer mucho como una invitación o anuncio oficial de LinkedIn o de una empresa para atraer a las personas para proporcionar información sensible o instalar accesorios. Esta fue la causa raíz en las violaciones recientes de Target y Carbanak.

En diciembre de 2013, un contratista de Target abrió e instaló una pieza de malware enviada como un archivo adjunto de correo electrónico que capturó credenciales del contratista y permitió a los atacantes infiltrarse en el entorno de red de destino. En última instancia, la violación se tradujo en comprometer las cuentas de crédito y débito de 40 millones de consumidores.[7] Del mismo modo, los atacantes enviaron correos electrónicos de phishing a varias instituciones financieras en todo el mundo. Se adjuntó a la dirección de correo electrónico el malware Carbanak.[8] Una vez abierto, infectaría las redes, que más tarde dieron lugar a retiros de $1 mil millones.[9]

Quizás uno de los tipos más eficaces de ataques de ingeniería social son las entregas de USB, un ataque que se alimenta de la curiosidad. Las unidades de USB se colocan o "entregan" en los estacionamientos a la espera de que las personas curiosas las recojan e inserten en sus computadoras. Los atacantes tienen la capacidad de programar los dispositivos de USB para tomar el control de una computadora segundos después de la inserción, con lo que este escenario se hace factible.

Mejores prácticas

Ya sea en un ambiente de trabajo profesional o en el hogar, resulta imprescindible para proteger la información propia. A continuación se presentan algunas de las mejores prácticas para la defensa contra las amenazas informáticas comunes.

Actualización de software

La actualización de software es crucial en cualquier entorno determinado, porque no aplicar parches y actualizaciones permite que persistan vectores de ataque—al igual que en la violación de Sony. La mayoría de los gigantes del software como Microsoft, Apple, Adobe y Java envían actualizaciones de software al menos una vez al mes. Estas actualizaciones suelen contener correcciones a errores o problemas de seguridad.

En un ambiente de trabajo, las políticas deben ser implementadas según cuándo y cómo hay que actualizar el software. En el hogar, los usuarios deben obtener notificaciones informándoles de actualizaciones

[2] Kazuo Hirai a la Cámara de Representantes de los EE.UU., "Letter to the U.S. House of Representatives," 3 de mayo del 2011, https://www.flickr.com/photos/playstationblog/sets/72157626521862165/

[3] Marc Perton, "Data security expert: Sony knew it was using obsolete software months in advance," *Consumer Reports*, 4 de mayo del 2011, http://www.consumerreports.org/cro/news/2011/05/data-security-expert-sony-knew-it-was-using-obsolete-software-months-in-advance/index.htm

[4] Jason Schreier, "Sony Estimates $171 Million Loss From PSN Hack," *Wired*, 23 de mayo del 2011, http://www.wired.com/2011/05/sony-psn-hack-losses/

[5] SplashData, "Worst Passwords," *SplashData*, 20 de enero del 2015, http://splashdata.com/press/worst-passwords-of-2014.htm

[6] Microsoft, "Microsoft issues warning on phone scam," Microsoft, 26 de agosto del 2010, http://www.microsoft.com/australia/presspass/post/Microsoft-issues-warning-on-phone-scam

[7] Brian Krebs, "Sources: Target Investigating Data Breach," *Kreb Security*, 13 de diciembre del 2014, http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

[8] Kaspersky, "Carbanak APT The Great Bank Robbery," *Kaspersky*, 1 de febrero del 2015, https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

[9] "Carbanak," *Wikipedia*, https://en.wikipedia.org/wiki/Carbanak#cite_note-SangerPerlroth20150214-2

¿Sabías?

Las instituciones financieras no siempre están en peligro cuando se ven afectadas por una violación. Un ejemplo de esto está en la violación de Target 2013 donde millones de tarjetas de crédito fueron comprometidos y vendidos en el mercado negro. Las instituciones financieras gastaron más de $170 millones exclusivamente para sustituir las tarjetas de crédito y débito de esta violación.[10]

disponibles. A modo de ejemplo, las notificaciones de Microsoft Windows suelen alertar al usuario de una actualización en la parte inferior derecha de la barra de tareas, a diferencia de Apple, que presenta las notificaciones de actualización en la parte superior derecha de la pantalla. Asegúrese de mantener su software actualizado en todo momento, esto incluye el software antivirus.

Complejidad de la contraseña

Al crear contraseñas, utilice contraseñas complejas generadas aleatoriamente (por ejemplo, b@?t:n0xFXvh). Las aplicaciones de administrador de contraseñas son las que ayudan en la creación, almacenamiento y cifrado de contraseñas—son muy recomendables. Los gestores de contraseña únicamente requieren el recuerdo de una contraseña, la contraseña maestra. Es importante asegurar la aplicación de una contraseña maestra fuerte y compleja, ya que se utiliza para desbloquear todas las contraseñas dentro del almacenamiento cifrado.

En contraste con las contraseñas, las frases de contraseña son más largas, compuestas de varias palabras y por lo tanto son más seguras. Aquellos que no opten por utilizar gestores de contraseña, deben utilizar frases de acceso y garantizar que cumplan con los siguientes criterios de SANS:[11]

- Tiene al menos 12 caracteres alfanuméricos
- Tiene tanto letras mayúsculas como minúsculas
- Tiene al menos un número
- Tiene al menos un carácter especial (por ejemplo, !$%^&*()_+|~-=\`{}[]:";'<>?,/)

En un ambiente de trabajo, el personal técnico debe desarrollar e implementar políticas que describen la complejidad, caducidad y requisitos de reutilización de las contraseñas. Es importante señalar que una contraseña segura puede disuadir completamente un ataque de fuerza bruta.

Cifrar

Anthem Health, uno de los proveedores de atención de salud más grandes del país, reveló recientemente que los atacantes habían comprometido una información de identificación personal de un estimado de 80 millones de sus clientes.[12] Al momento de escribir este artículo, Anthem está trabajando con las autoridades federales y no ha revelado la causa raíz del ataque, pero una cosa está clara: Los atacantes obtuvieron la información de identificación personal debido a los controles de cifrado insuficientes de Anthem.

El cifrado distorsiona los archivos y los hace ilegibles para el usuario no autorizado, protegiendo así su confidencialidad. Es importante activar el cifrado en los discos duros con programas como BitLocker (Windows) y FileVault (Mac) para cifrar sus respectivos sistemas de archivos. Además, los documentos que contienen información sensible deben cifrarse antes de almacenarse o transferirse.

En un ambiente de trabajo, las soluciones deben ser implementadas para cifrar archivos en tránsito o los depositados, y cifrar los sistemas de archivos completos de las computadoras. En el hogar, la información sensible se debe guardar como documentos protegidos por contraseña (Microsoft Office tiene la capacidad de cifrar documentos) o contenedores (por ejemplo, archivos zip).

Conciencia de seguridad

Muchas veces, las organizaciones implementan las últimas tecnologías intentando asegurar su ambiente e impidiendo la entrada de los atacantes. Sin embargo, se olvidan de uno de los elementos más importantes en materia de seguridad: el elemento humano. Aquí es donde la conciencia de seguridad entra en acción.

La conciencia de seguridad es una clave importante para la prevención de las amenazas cibernéticas. Cuando hablas a un individuo, confirme su identidad y nunca proporcione información sensible por teléfono—el personal técnico nunca le pedirá su contraseña. Reporte llamadas sospechosas a los supervisores o el incidente apropiado al grupo de informes del trabajo. Esto puede ayudar a prevenir un ataque a toda la empresa.

Los correos electrónicos de phishing pueden identificarse inspeccionando cuidadosamente los encabezados de correo electrónico sospechosos, así como la supuesta identidad del remitente. Los atacantes suelen utilizar nombres de dominio que son similares a las oficiales, pero con sutiles diferencias. Abra los adjuntos de correo electrónico solamente cuando se le notifique previamente que recibirá uno, sin importar lo que

[10] Tom Crosson, "Cost of Target Data Breach Exceeds $200 Million," Consumer Bankers Association, 18 de febrero del 2014, http://www.cbanet.org/News%20and%20Media/Press%20Releases%202014/02182014_pressrelease.aspx

[11] SANS, "Password Construction Guidelines," junio de 2014, https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines

[12] Reed Abelson and Matthew Goldstein, "Anthem Hacking Points to Security Vulnerability of Health Care Industry," *Business Day*, 5 de febrero del 2015, http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0

parece intrigante. Una vez más, se deben reenviar correos electrónicos sospechosos a los supervisores o el grupo de notificación de incidentes para confirmar su legitimidad. El personal técnico debe tener soluciones avanzadas de correo electrónico de filtrado de spam, seguridad de correo electrónico y mucho más. En el hogar, los proveedores de correo electrónico, como Gmail, están empezando a tomar medidas enérgicas contra el phishing y alertarán a los usuarios con una alerta roja.

Además, no recoja dispositivos portátiles, como los USB. La investigación del Departamento de Seguridad Nacional de los EE.UU. concluyó que el 60 por ciento de las personas que recogían los USB de estacionamientos los conectan a las computadoras.[13]

Por último, piense antes de hacer clic. No haga clic en enlaces no acreditados o no confiables a páginas web, archivos adjuntos de correo electrónico abiertos o instale programas de fuentes no confiables. En ambientes de trabajo, el personal técnico debería haber implementado filtrado web para reducir las posibilidades de que las personas que visitan los sitios web no están acreditadas. En el hogar, instalar plugins del navegador como Web of Trust (WOT) para ayudar a identificar los sitios web seguros/reputados.

Reportando incidentes

Los sistemas informáticos podrían actuar lentos, a veces durante las actualizaciones o cuando hay mucha actividad. Sin embargo, si ha seguido durante varios días y se ha desarrollado comportamiento anormal (por ejemplo, pop-ups, aplicaciones instaladas no familiares, procesos sospechosos en ejecución), entonces es hora de reportar un incidente.

En el hogar, reporte cualquier actividad sospechosa al Internet Crime Complaint Center (IC3). El IC3 fue inaugurado en 2000 por el FBI en colaboración con el National White Collar Crime Center (NW3C) para recibir las actividades y/o quejas sobre actividades sospechosas de Internet como intrusión informática, espionaje, extorsión, lavado de dinero, robo de identidad y mucho más.[14]

En el trabajo, consulte con el personal de seguridad de computación sobre incidentes informáticos sospechosos. Cuando necesario, un equipo de respuesta a incidentes quedará notificado para realizar el análisis y la investigación forense en el sistema o sistemas afectados. Es imprescindible preservar el estado actual de un equipo en el momento de contactar con el personal de seguridad de la computadora hasta que la informática forense lo considera necesario. Los que respondan a incidentes decidirán la magnitud del ataque cibernético y de los representantes de las autoridades de control legal según sea necesario. A las autoridades de control legal se les debe informar de un incidente si afecta la seguridad de varias personas, la nación y/o si el resultado es la "pérdida significativa de datos, la disponibilidad del sistema, o el control de los sistemas".[15]

Además, las instituciones financieras pueden reportar operaciones de actividades sospechosas a la Red Contra los Delitos Financieros (FinCEN) mediante la creación de un reporte de operaciones sospechosas (ROS). El ROS incluye actividades financieras detalladas como las transacciones que parecen sospechosas. Estos informes ayudan a las agencias federales de control legal en la investigación de un posible fraude, el lavado de dinero, el terrorismo y más.

Aparte de los incidentes que informaron adecuadamente, la industria reconoció que empresas de consultoría de seguridad informática recomiendan encarecidamente programar evaluaciones frecuentes. Estas evaluaciones identificarán las vulnerabilidades de seguridad y/o mejores prácticas desaparecidas con el objetivo general de incrementar la postura de seguridad dentro de una organización.

Una era de la seguridad

Al final, no se trata de la cantidad de productos de seguridad que uno compra para mantenerse a salvo, sino del proceso. Es la combinación de productos, su aplicación y la conciencia de seguridad los que mejoran la seguridad del entorno y, en última instancia, la propia.

Con el conocimiento de metodologías de ataque comunes utilizadas por los atacantes y el conocimiento de las mejores prácticas, ahora uno tiene el conjunto de habilidades para protegerse contra las amenazas cibernéticas. Sin embargo, hay mucho más que aprender. No deje de pedirle al personal de seguridad de computación en el trabajo para obtener más información sobre las mejores prácticas.

A medida que continuamos viviendo en la era de la ciberguerra, esforcémonos para aumentar y mejorar la concientización sobre la seguridad. ¡Manténgase seguro!

Jonathan H. Broche, consultor, Optiv Security, Miami, FL, EE.UU., jbroche@accuvant.com

Los puntos de vista y opiniones expresados en este artículo son responsabilidad exclusiva del autor y no reflejan necesariamente los puntos de vista de Optiv Security Inc., sus afiliados o sus empleados.

¿Sabía usted?

En 2002, el FBI estableció el programa Laboratorio Regional de Informática Forense (RCFL). El RCFL proporciona a las autoridades de control legal herramientas forenses avanzadas para facilitar con el decomiso y la investigación de los delitos cibernéticos, así como la capacitación de las autoridades de control legal en los EE.UU. Hoy en día existen 16 laboratorios de RCFL que cubren la mayor parte de la nación.[16]

[13] Cliff Edwards, "Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy," *Bloomberg Business*, 27 de junio del 2011, http://www.bloomberg.com/news/articles/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy

[14] IC3, http://www.ic3.gov/about/default.aspx

[15] FBI, Law Enforcement Cyber Incident Reporting, http://www.fbi.gov/about-us/investigate/cyber/law-enforcement-cyber-incident-reporting

[16] RCFL, http://www.rcfl.gov/about

ACAMS® | AML General Awareness

Your Solution for Enterprise-wide AML Training

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

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

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

La explotación de los mayores—

En general, a los oficiales de cumplimiento no les gustan las zonas grises. Las áreas grises piden juicios de valor, los juicios de valor conducen a errores y los errores conducen a malas situaciones para las instituciones financieras y, en ocasiones, para los clientes. Las áreas grises referidas a la explotación financiera de los mayores[1] van más allá del color del pelo de un cliente. Desde la definición de quién califica como "mayor", a si el mayor es "explotable", hasta los requisitos de información, un director de programa de antilavado de dinero (ALD) debe tener una visión global del problema que está tratando de resolver con el fin de desarrollar una solución integral sostenible.

La vigilancia financiera es sólo una parte de la solución

La explotación económica de los mayores ha obtenido mucha prensa en los últimos años. Según la Senadora Claire McCaskill en su declaración de apertura a la Comisión Especial del Senado sobre el Envejecimiento, "Aproximadamente uno de cada cinco adultos mayores será objetivo de explotación financiera de alguna forma, por valor de miles de millones en pérdidas cada año".[2] La explotación financiera de los mayores probablemente aumentará a medida que nuestra población envejece con 10.000 personas cumpliendo 65 años todos los días durante los próximos 15 años.[3] Esto suponiendo que la tasa de explotación se mantendrá constante en uno de cada cinco, lo que equivale a aproximadamente 73.000 nuevas víctimas todos los años. Al añadir a esa estadística alarmante el hecho de que la mayoría de las víctimas no hacen denuncias por un sinnúmero de razones (vergüenza, miedo de las acusaciones penales contra un familiar o cuidador, miedo a la pérdida de la independencia), resulta bastante fácil entender por qué hacer frente a la explotación económica de los mayores ha adquirido un sentido de urgencia. A medida que la economía lucha por recuperarse, los adultos mayores se hacen más atractivos para los estafadores porque tienen activos tangibles tales como bienes raíces, ahorros en efectivo, pensiones y otros ingresos de jubilación.

Aunque no sea un tema nuevo, el aumento de la exposición del papel que juegan las instituciones financieras en el fenómeno probablemente se remonta a la *Asesoría FIN-2011-A003 de Instituciones Financieras en la Presentación de Reportes de Operaciones Sospechosas Respecto de la Explotación Financiera de Mayores* de la Red Contra los Delitos Financieros (FinCEN). La Asesoría deja muy en claro a las instituciones financieras que la sospecha de la explotación financiera de un individuo de edad avanzada es una ofensa que merece un reporte de operaciones sospechosas (ROS). Se aconseja a las entidades financieras utilizar la frase "explotación económica de un mayor" en la narrativa del ROS al informar incidentes sospechosos. Además, la Asesoría afirma que una posible víctima de explotación financiera nunca debe aparecer como el tema del ROS sino que la información que identifica debe añadirse a la narrativa del ROS.

Curiosamente, la Asesoría FIN-2011-A003 prosigue afirmando que "El abuso de los mayores, incluida la explotación económica, se reporta e investiga generalmente en el ámbito local, con los Servicios de Protección para Adultos [APS], las oficinas del Fiscal del Distrito, las oficinas de alguaciles y los departamentos de policía tomando papeles clave. Hacemos hincapié en que los contribuyentes deben seguir reportando todas las formas de maltrato a personas mayores de acuerdo con las políticas institucionales y los requisitos de las leyes y reglamentos estatales y locales, en su caso". La declaración es interesante debido a que un estudio de 2011 de la Oficina de Contabilidad General sobre Abuso de Mayores[4] indica que sólo 10 de los 50 estados establecen la obligación de denunciar la sospecha del maltrato a personas mayores (incluida la explotación financiera) a APS. Los reportes indican que muchas instituciones financieras en los estados sin reportes obligatorios de APS luchan por equilibrar el deseo de denunciar la explotación financiera sospechosa con los requisitos de varias leyes de privacidad que protegen la información de los clientes que debe mantenerse reservada.

En un golpe de genio, siete autoridades reguladoras se reunieron en 2013 para emitir la *Orientación Interinstitucional sobre Leyes de Privacidad y Denuncias del Abuso Financiero de los Adultos Mayores* NR 2013-148.[5] La Orientación es clara en su mensaje: "la denuncia del abuso financiero sospechoso de los mayores a las agencias estatales o federales locales adecuadas no viola, en general, las disposiciones de privacidad de la GLBA (Ley Gramm-Leach-Bliley) o su normativa de desarrollo".

Los empleados de las instituciones financieras se encuentran a menudo en buena posición para ser la primera, y a veces la única, parte autónoma capaz de ver y analizar posibles alertas rojas de explotación financiera (véase el Apéndice A). Si bien los reguladores no han documentado específicamente en el manual de examen del Consejo Federal de Inspección de Instituciones Financieras (FFIEC) de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD), la expectativa de tejer indicadores de alertas rojas sobre la explotación financiera de mayores en un programa de ALD, el tema ha sido cubierto ampliamente por seminarios de Internet y conferencias sectoriales.

La amplia cobertura de la explotación financiera de mayores en un programa de ALD requiere un enfoque reflexivo sobre el tema. Si bien la presentación de informes automatizados o manuales puede incorporar ciertas tipologías en el programa de vigilancia, un gestor de programas de ALD debe pensar dos veces antes de confiar únicamente en el programa de vigilancia para cubrir el riesgo totalmente. Hay otras áreas de un programa de ALD que merecen igual consideración: conozca a su cliente (KYC), la diligencia debida del cliente (DDC), la mayor clasificación empresarial de riesgos y la formación, por nombrar unos pocos.

---

[1] La definición de "explotación" del Centro Nacional sobre el Maltratado a Adultos Mayores es "la toma ilegal, uso indebido u ocultamiento de fondos, propiedades o bienes de una persona mayor vulnerable".

[2] Claire McCaskill, la Comisión Especial del Senado sobre el Envejecimiento, 4 de febrero del 2015, http://www.aging.senate.gov/imo/media/doc/SCA_CMC_2_4_15.pdf

[3] Kathleen M. Quinn, *Broken Trust: Combatting Financial Exploitation of Vulnerable Seniors*, 4 de febrero del 2015, http://www.aging.senate.gov/imo/media/doc/SCA_Quinn_2_4_15.pdf

[4] Oficina de Contabilidad General, *Elder Justice: Stronger Federal Leadership Could Enhance National Response to Elder Abuse*, 21 de marzo del 2011, http://www.gao.gov/new.items/d11208.pdf

[5] La Oficina del Contralor de la Modeda, "Federal Regulators Issue Guidance on Reporting Financial Abuse of Older Adults," 24 de septiembre del 2013, http://www.occ.gov/news-issuances/news-releases/2013/nr-ia-2013-148.html

Comience con lo básico—KYC. Hay tantos aspectos de este principio fundamental de la BSA que se pueden aplicar a la construcción de un sólido programa de explotación financiera de mayores. Por empezar, su institución debe definir claramente "mayor" en su programa de ALD. ¿Es mayor cualquier persona de más de 50 (piense en AARP) o se trata de cualquiera elegible para las pensiones de la Administración de Seguridad Social (por ejemplo, 62 años o más)? Cada estado ofrece su propia definición de "mayor". Las instituciones financieras que hacen negocios en varios estados harían bien en establecer firmemente y documentar su definición de mayor para proporcionar orientación a los que tratan al cliente y los asociados de investigación. Asegúrese de que está cómodo con cómo su proveedor de software de vigilancia define "mayor" y que la definición sea coherente con las orientaciones impartidas en otra documentación y/o programa de capacitación.

Para los clientes que entran en la definición institucional de la tercera edad, la institución debería considerar si se justifica un DDC añadido y/o diligencia debida mejorada (EDD). ¿El cliente vive solo? ¿El cliente tiene un cuidador familiar o no familiar que ayuda con las tareas o las finanzas diarias? ¿El cliente ha dado poder legal? La actividad transaccional esperada es información crítica al determinar si los fondos que salen de la cuenta de las personas mayores resultan inusuales o sospechosos. Es comprensible que muchos clientes (o sus familiares/cuidadores) consideren que preguntas como éstas son una invasión de la privacidad o un exceso del banco en su necesidad de información. Lamentablemente, muy pocas personas van a ver las preguntas detalladas como una herramienta para la protección de los activos o para que la entidad financiera tome su responsabilidad fiduciaria en serio.

Philip Marshall, nieto del filántropo y mayor víctima de explotación financiera Brooke Astor, declaró bastante elocuentemente en su discurso preparado ante la Comisión Especial del Senado de los EE.UU. sobre el Envejecimiento el 4 de febrero del 2015, que "la vigilancia fiscal debe coincidir con el seguimiento físico para asegurar el bienestar de los ancianos". El tema es que los clientes pueden no apreciar la "vigilancia fiscal" que ofrece una DDC robusta o programa de EDD. El entrenamiento para los que se manejan con los clientes y los asociados de la trastienda es crucial para el éxito de la identificación, la derivación y la notificación de posibles casos de explotación financiera de los mayores.

La clasificación de negocios a un nivel de riesgo más alto también puede desempeñar una parte importante de un programa integral de ALD para combatir la explotación financiera de los mayores. Los directores de programas de ALD son conscientes de las tradicionales empresas de "mayor riesgo", tales como las empresas de servicios monetarios (MSB) y otras empresas que usan efectivo de manera intensiva. Las instituciones financieras no bancarias (IFNB) también representan un mayor riesgo de lavado de dinero para una entidad financiera.[6] El Manual de Examen de FFIEC de BSA/ALD establece, que las "IFNB se definen ampliamente como instituciones distintas de los bancos que ofrecen servicios financieros". El Manual lista siete industrias que pueden ser consideradas IFNB, incluyendo casinos y compañías de seguros. El Apéndice D del Manual lista 25 empresas/industrias diferentes que se consideran legalmente "instituciones financieras". Un tipo de empresa que ofrece servicios de banca, que claramente no es un banco y, a menudo no es considerada en discusiones de instituciones financieras no bancarias (y no está incluida en el Apéndice D) es el hogar de ancianos. Los hogares de ancianos pueden ser una amenaza no identificada para un programa de ALD que se esconde a plena vista.

Muchos hogares de ancianos mantienen cuentas de residentes. Los residentes que han agotado sus propios fondos y están recibiendo Medicaid generalmente tienen que aplicar todos sus cheques del Seguro Social (excepto una asignación para gastos personales) a los costos de su cuidado de ancianos con el saldo pagado por Medicaid. En 2013, los residentes de hogares de ancianos tenían derecho a mantener aproximadamente $50 de sus cheques mensuales de Seguro Social a sus gastos personales. En estos casos, los cheques del Seguro Social se endosan a la residencia de ancianos al momento del ingreso, la residencia de ancianos entonces "devuelve" el importe de adjudicación personal cada mes al residente. A menudo, la devolución de los fondos al residente se logra mediante la apertura de una "cuenta" en el hogar de ancianos donde el residente puede solicitar un retiro de fondos en efectivo o puede solicitar fondos a los distintos servicios que ofrece la casa, tales como peluquería o lavandería. Además, los residentes o sus familiares pueden hacer depósitos en la cuenta. Por otra parte, en Nueva York (y potencialmente en otros estados) la Ley de Higiene Mental[7] permite que los hogares de ancianos obtengan el poder legal sobre los fondos de los residentes mediante la presentación de peticiones de tutela. Los residentes o miembros de la familia a menudo no son conscientes de que la petición ha sido presentada hasta que se ha concedido la tutela.

Aunque no suelen clasificarse como "empresas de efectivo intensivo", puede haber más dinero cambiando de manos en un hogar de ancianos que lo que imagina inicialmente un banquero. Desde una perspectiva del programa de ALD, cuando se ofrecen servicios bancarios a un hogar de ancianos, se debe considerar si la actividad representa un riesgo oculto de lavado de dinero o explotación económica mayor. ¿Se le ocurre cualquier blanco más fácil para el robo de fondos de personas mayores que pueden encontrarse con discapacidad mental o física, o ambas cosas? Las posibilidades de robo incluyen desde la malversación por parte de la residencia de ancianos (¿quién echaría de menos estos fondos?) hasta el ayudante "útil" que ofrece conseguirle algunos artículos necesarios a un residente y, o bien no compra los artículos o bien factura por encima del precio de los artículos comprados. Este párrafo no debe interpretarse en el sentido de que todos los hogares de ancianos son paraísos de delincuentes ni que toda la gente que sirve a nuestros ancianos en los asilos de ancianos son ladrones, sino más bien que las cuentas no reguladas (por examinadores bancarios federales) en hogares de ancianos presentan un mayor riesgo de robo, fraude y explotación económica de los mayores.

El entrenamiento sobre la explotación financiera de los mayores debe ser más que un ejercicio de "marcar la casilla". Al diseñar un programa integral para hacer frente a la explotación financiera de los mayores, un gestor de programas de ALD debe tener

[6] The Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, 14 de noviembre del 2014, http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014.pdf

[7] La Ley de Higiene Mental, http://www.nycourts.gov/ip/gfs/Article_81_Law_2008.pdf

un entrenamiento reflexivo, y si es posible, específico, para hacerles frente a las mejoras en el programa. Los asociados que tratan con los clientes deben estar expuestos a las alertas rojas de posible maltrato y explotación a personas mayores. Los asociados de las oficinas interiores deben saber si se requiere la notificación obligatoria a APS en su estado. Muchos estados están participando en el esfuerzo de formación mediante el reconocimiento de las instituciones financieras como parte integral de una solución al problema de la explotación. Cada vez más, las instituciones financieras son invitadas por organizaciones estatales a entrenamientos dedicados al tema. Por ejemplo, Maine ha desarrollado un programa titulado Senior$afe que se utiliza como modelo para otros programas estatales. "Senior$afe fue creado para aumentar la identificación y notificación de casos sospechosos de explotación financiera de mayores—específicamente, por las instituciones financieras".[8] Senior$afe incluye la capacitación de los cajeros y otros empleados de cara al cliente y se centra en las alertas rojas para el maltrato de los mayores y la explotación financiera. Una segunda capacitación en el marco del programa es para los directivos y el personal de cumplimiento y se centra en el desarrollo de un programa documentado para tratar los casos identificados de potencial abuso de los mayores y la explotación económica. Los directores de programas de ALD harían bien en considerar un enfoque de dos niveles similares en la formación.

Algunos profesionales de cumplimiento pueden creer que el paso final en el proceso de construcción de un programa de ALD integral para hacer frente a la explotación financiera de mayores consiste en documentar las decisiones que se han hecho. Si bien la documentación de decisiones es claramente un paso vital en cualquier programa de ALD, en este caso no es el paso "final". El paso final es estar al tanto del paisaje siempre cambiante de las leyes y regulaciones que afectan a los mayores. Si la definición de "mayores" cambia en cualquier estado en que usted hace negocios, como oficial de cumplimiento de ALD, usted tiene que estar al tanto de los cambios y tener procesos para actualizar el programa según sea necesario. Un programa de ALD de explotación financiera de mayores debe ser lo suficientemente flexible como para cambiar con las expectativas regulatorias. Una vez que se haya implementado un programa de ALD integral para hacer frente a la explotación financiera de los mayores, no se ha llegado al final—sólo se ha llegado a un nuevo comienzo. "Ser complaciente con la justicia de los mayores es ser cómplice en el maltrato de ancianos".[9] A

Amy Wotapka, CAMS, CRCM, jefa de programa de ALD, Johnson Bank, Racine, WI, EE.UU., awotapka@johnsonbank.com

[8] Judith M. Shaw, *Broken Trust: Combating Financial Exploitation of Vulnerable Seniors*, 4 de febrero del 2015, http://www.aging.senate.gov/imo/media/doc/SCA_Shaw_2_4_15.pdf

[9] Philip C. Marshall, *Broken Trust: Combating Financial Exploitation of Vulnerable Seniors*, 4 de febrero del 2015, http://www.aging.senate.gov/imo/media/doc/SCA_Marshall_2_4_15.pdf

[10] "Preventing Financial Abuse of the Elderly," *Consumer Reports*, 4 de noviembre del 2009, http://www.specialneedsnewyork.com/pdf/consumer-reports-october-2009.pdf

[11] Marion Trelle, "Financial Exploitation of the Elderly: A Critical Review," http://www.uwplatt.edu/files/urce/BigMTrelleVI.pdf

[12] La Oficina del Contralor de la Moneda, "Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults," http://www.occ.gov/news-issuances/news-releases/2013/nr-ia-2013-148a.pdf

Apéndice A

Alertas Rojas: Explotación Financiera de Mayores[10, 11, 12]

Transaccional (vigilancia):

- Retiros grandes e inexplicables de las cuentas bancarias
- Cambios en los patrones de gasto, las compras de dólares o grandes transacciones de débito incoherentes para el adulto mayor
- Falta de pago no característica de servicios (honorarios de cajas de seguridad, pagos de servicios públicos, hipoteca/alquiler)
- Actividad con insuficiencia de fondos
- Transferencias electrónicas no características
- Cierre de los CD o las cuentas sin tener en cuenta las sanciones
- Firmas desconocidas en los cheques

Documentación (diligencia debida):

- Estados de cuenta bancarios y cheques cancelados que ya no van al domicilio del mayor
- Cambio en el poder notarial
- Cambios en los bancos o abogados
- La adición de uno o más nombres a la cuenta de un cliente

Interacciones de primera línea:

- Falta de comodidades, tales como ropa limpia y aseo
- Grado inusual de miedo o sumisión a un cuidador; signos de intimidación y amenazas por parte de otro
- Un cuidador u otra persona que muestra interés excesivo en las finanzas o bienes del adulto mayor, no permite que el adulto mayor hable por sí mismo, o es renuente a dejar el lado de la persona mayor durante las conversaciones
- Indicación de aislamiento de la familia, los amigos, la comunidad y otras relaciones estables (el mayor ya no menciona a los hijos o nietos)
- Citas perdidas
- Ansiedad sobre las finanzas personales o la falta de conocimiento acerca de la situación financiera
- Menciones de un nuevo "mejor amigo"
- La entidad financiera no puede hablar directamente con la persona mayor, a pesar de los repetidos intentos de ponerse en contacto con él o ella

Los anillos de defensa necesarios para hacer frente a las amenazas del terrorismo al país

La amenaza terrorista para el país que las naciones occidentales enfrentaron el 11 de septiembre del 2001 (9/11), es muy diferente de la que enfrentamos hoy. Lo que experimentamos en 9/11 fue una organización terrorista, al-Qaeda, que posee la capacidad de tener un grupo de sus yihadistas realizando con éxito un ataque devastador en suelo estadounidense. A pesar de que todavía desean perpetrar ataques similares, al-Qaeda ya no tiene la capacidad para hacerlo. Otros grupos terroristas prominentes como al-Qaeda en la Península Arábiga (AQAP), el Estado Islámico en Irak y el Levante (ISIL) y al-Shabaab, aspiran a llevar a cabo ataques terroristas en Occidente. Sin embargo, ninguno de estos grupos posee la capacidad para ejecutar ataques en los EE.UU. y otros países occidentales en el corto plazo. Aunque hay un énfasis importante y necesario en las organizaciones terroristas, la amenaza más significativa para las naciones occidentales proviene de los individuos del propio país que siguen el llamado de estas organizaciones.

Grupos como AQAP e ISIL han desarrollado mecanismos de contratación por Internet extremadamente sofisticados usando las redes sociales y otras plataformas para reclutar a su causa personas en riesgo y con problemas. Han tenido éxito al alcanzar una amplia franja de personas en Internet susceptibles de ser radicalizadas y de llevar a cabo actos violentos. Semejante a un culto, esta población en riesgo ha sido o está siendo acondicionada o se le lava el cerebro para convertirse a una representación falsa del Islam. Algunas de estas personas han viajado a Siria para unirse a ISIL o a la franquicia de al-Qaeda en Siria, el Frente al-Nusra. Otras personas con problemas han sido, o están en

proceso de ser radicalizadas para quedarse en casa y cometer yihad en sus países de origen. Esto se evidenció en Canadá en octubre de 2014, en París en enero de 2015 y Copenhague en febrero de 2015.

En un discurso pronunciado el 13 de marzo del 2015, ante la Organización Nacional de Ejecutivos de Autoridades Legales Negros (NOBLE), el Director del FBI James B. Comey dijo que la amenaza terrorista de hoy es muy diferente a la amenaza terrorista que los EE.UU. enfrentaron en 9/11. El Director Comey informó que grupos como ISIL han conseguido ser muy hábiles en el uso de los medios sociales y que propalan un mensaje venenoso por Internet. Afirmó que "ISIL está emitiendo un canto de sirena a almas atribuladas".[1] El Director Comey agregó que el FBI está llevando a cabo investigaciones sobre la amenaza de los extremistas violentos nacionales en los 50 estados de los EE.UU. Comentó, además, que la gente en los 50 estados están en alguna etapa de consumición del veneno hacia la radicalización. Esto no es sólo un problema de los EE.UU. sino que nos impregna a todo el mundo occidental y les presenta a los países occidentales importantes problemas de seguridad nacional. Estas preocupaciones justifican respuestas antiterroristas más proactivas e innovadoras.

Entonces, ¿cómo podemos hacerle frente a la propagación cancerosa de este problema de la radicalización de cosecha propia?

Hay tres anillos de defensa. Cada uno juega un papel igualmente importante en el tratamiento y la tarea hacia la eliminación de la amenaza extremista violenta nacida en el país. Debemos desarrollar estrategias reactivas y proactivas dentro de los tres anillos de defensa para hacer frente a la amenaza planteada por el cambio de los extremistas violentos de cosecha propia. Desde el 9/11, nuestro enfoque principalmente ha estado mirando hacia afuera por la amenaza de la organización que plantean los grupos terroristas fuera del país. La amenaza ha evolucionado hasta convertirse en una interna causada por individuos caprichosos atraídos por los mensajes de reclutamiento falsos de organizaciones terroristas extranjeras. A medida que miramos hacia adentro, las agencias policiales estatales y locales se convierten en engranajes importantes en nuestro esfuerzo de frustrar la amenaza extremista nacional.

Los tres anillos de defensa son similares para todas las naciones occidentales. Su aplicación será diferente en cada país en función de su marco legal y regulatorio, así como la composición de la jurisdicción de las autoridades de control legal federales, estatales y locales. Usando los EE.UU. como ejemplo, los tres anillos de defensa deben funcionar como sigue:

Primer anillo de defensa

El primer anillo de defensa consiste en seguir conteniendo y desbaratando la amenaza mundial del terrorismo utilizando medidas militares, diplomáticas, de inteligencia, de las autoridades de control legal y con sanciones antiterroristas. Esto requiere de una colaboración interinstitucional coherente y coordinada que se basa en las capacidades de cada participante gubernamental. Un área importante de la colaboración interinstitucional es identificar combatientes extranjeros de los EE.UU. que viajaron a Siria y que puedan regresar a los EE.UU.

En cuanto a la amenaza de cosecha propia dentro de los EE.UU., el FBI tiene la responsabilidad primaria de investigar en la lucha contra el terrorismo. Necesita el apoyo de la comunidad interinstitucional para identificar las amenazas internas, en especial a través de enlaces de inteligencia global. Más que nada, es imperativo que el FBI se asocie con las agencias policiales estatales y locales para identificar e impedir a los extremistas violentos nacionales. En el discurso del Director del FBI Comey ante NOBLE el 13 de marzo del 2015, donde habló sobre la amenaza extremista violenta del propio país, el Director señaló que se trata de una amenaza muy diferente a la que nos enfrentamos en 9/11. El Director Comey señaló que era muy poco probable que los agentes federales se enteraran de que un individuo se está radicalizando. Afirmó que alguaciles y policías que patrullan en el barrio—y que conocen sus barrios—tienen más probabilidades de identificar a las personas que se han convertido o están en proceso de radicalizarse.

Desde un punto de vista interno, con respecto a este primer anillo de defensa, los policías estatales y locales sirven como nuestra primera línea de defensa en la identificación de los extremistas violentos de cosecha propia. ¿Qué pueden hacer oficiales de la policía local o estatales—especialmente aquellos en los departamentos más pequeños y de áreas más rurales—para aprender más sobre la identificación de las amenazas terroristas? Esta es una pregunta importante y que podría ser la diferencia entre un ataque terrorista exitoso y la interrupción de un ataque. El Director Comey y el FBI están comprometidos a compartir tanta información de inteligencia como sea posible con las agencias de policía estatales y locales. Dos importantes mecanismos para lograr este flujo de información son los principales centros de fusión de la zona urbana (centros de fusión) y las Fuerzas de Tarea de Terrorismo Conjuntas (JTTF, por sus siglas en inglés). Todas las autoridades de control legal estatales y locales deberían aprovechar compartir plataformas de información y la experiencia de los centros de fusión y JTTF.

Los centros de fusión son propiedad de y están operados por entidades estatales y locales. Están destinados a estar en una ubicación singular para empoderar la aplicación de primera línea de las autoridades de control legal, la seguridad pública, los servicios de bomberos, la respuesta a emergencias, la salud pública y el personal de seguridad del sector privado para recoger legalmente y compartir información relacionada con las amenazas. Los centros de fusión son una plataforma para que el FBI y otras agencias provean información de inteligencia procesable para su difusión. Los policías estatales y locales deben aprovechar esta fuente de información relacionada con las amenazas. Algunos centros de fusión son muy eficaces y algunos no lo son tanto. La razón de la variación es el factor humano, lo que equivale al nivel de la cooperación, la comunicación y la coordinación en cada centro de fusión. Mientras más coherente el compromiso, la capacidad y la colaboración, probablemente más efectivo será el centro de fusión.

Las JTTF han sido una herramienta valiosa de primera línea de las autoridades de control legal antiterroristas desde su formación en la ciudad de Nueva York en 1980. Hoy en día, las JTTF están ubicadas en 104 ciudades, incluyendo una en cada una de las 56 oficinas locales del FBI. Las JTTF

[1] James B. Comey, discurso sobre la aplicación de la ley y la raza, FBI, 13 de marzo del 2015,

Aprovechando la experiencia y los contactos de los profesionales de extensión del gobierno, los líderes comunitarios y oficiales de policía locales, mejoraría nuestra capacidad para identificar a las personas susceptibles a la radicalización

se componen de alrededor de 4.000 socios en todo el país. Provienen de 500 agencias estatales y locales, y 55 agencias federales. Las JTTF proporcionan una ventanilla única para la información relativa a las actividades terroristas. Permiten una base de inteligencia compartida a través de muchas agencias. Desde su creación, las JTTF han tenido un gran éxito. Una de las claves del éxito ha sido la capacidad de proporcionarles a los policías estatales y locales la autorización de seguridad para compartir información reservada. Otra clave del éxito es la formación impartida a los miembros de las JTTF. Las JTTF funcionan como la punta de lanza para las investigaciones sobre terrorismo.

La mayoría de las investigaciones antiterroristas son llevadas por las JTTF. Aunque el FBI tiene jurisdicción primaria en las investigaciones antiterroristas, otras agencias de control legal federales, estatales y locales llevan a cabo investigaciones que tienen un nexo con el terrorismo y es probable que con los extremistas violentos naturales del país. Es importante que esas investigaciones se coordinen con las JTTF en los lugares en los que se están llevando a cabo investigaciones. Algunos departamentos de policía, como el Departamento de Policía de Nueva York y el Departamento de Policía de Los Ángeles operan oficinas altamente eficaces contra el terrorismo para proteger sus ciudades y coordinan el intercambio de información de inteligencia con centros de fusión y las JTTF.

Segundo anillo de defensa

El segundo anillo de defensa es la comunidad interagencia del gobierno con responsabilidades de alcance para establecer iniciativas de extensión comunitaria con un amplio espectro de líderes de la comunidad. Esto representaría una muy importante asociación entre el sector público y privado. Para realmente tener éxito, cualquier iniciativa de este tipo debe ser lo más diversa posible. Esto llevaría a acceder a más personas, sobre todo a las que están en riesgo.

El Departamento de Estado, el Departamento del Tesoro y el FBI tiene cada uno programas de extensión. Deben trabajar con las comunidades para educar y promover la lucha contra el extremismo violento radicalizado nacional. Esta iniciativa debería centrarse en la lucha contra el reclutamiento de los mensajes venenosos de grupos como ISIL y AQAP. Además, diversas comunidades deberían estar mirando internamente, hacia la identificación y la interdicción de los individuos en riesgo susceptibles a la radicalización.

Desde un punto de vista nacional interno, al igual que con el primer anillo de defensa, las autoridades de control legal estatales y locales que patrullan en los barrios y comunidades en todos los EE.UU. están en la primera línea dentro de este círculo de defensa. Aquí es también donde las autoridades de control legal estatales y locales que sirven en las JTTF pueden hacer contribuciones significativas. Las autoridades de control legal de primera línea deben ser incluidas en este tipo de iniciativa comunitaria. En muchos casos, ellos conocen la comunidad en la que trabajan mejor que nadie y están en la mejor posición para identificar a las personas en situación de riesgo y los cambios de comportamiento de los que se están radicalizando. Aprovechando la experiencia y los contactos de los profesionales de extensión del gobierno, los líderes comunitarios y oficiales de policía locales, mejoraría nuestra capacidad para identificar a las personas susceptibles a la radicalización.

Los grupos como ISIL, con sus publicaciones en Internet *Dabiq*, y AQAP, con *Inspire*, han demostrado que son conocedores de Internet. Nuestra extensión comunitaria pública y privada debe llegar a los privados de sus derechos y a los individuos en riesgo de manera tan sofisticada como nuestros adversarios. Una de las estrategias que empleamos debería ser explotar la brecha entre ISIL y al-Qaeda. Esta brecha ha expuesto a estos grupos a la falsedad de sus representaciones en los medios sociales. El gobierno y la extensión a la comunidad debería tratar de explotar la brecha y hacer hincapié en la falacia de la propaganda que se presenta.

Tercer anillo de defensa

El tercer anillo de defensa consiste en identificar alertas rojas o anomalías identificables con los extremistas y los nacionales reclutados como combatientes extranjeros quienes logran o bien intentan unirse a ISIL u otros grupos en Siria. Sin otra inteligencia o indicadores, es extremadamente difícil identificar a los extremistas violentos propios por medio del monitoreo de transacciones u otras alertas rojas financieras. Las señales de advertencia y los patrones de actividad asociados a los combatientes extranjeros son más perceptibles que para los extremistas violentos de cosecha propia que no viajan al extranjero. Este anillo de defensa exige una fuerte asociación público-privada que afecta principalmente a las autoridades de control legal, el Departamento del Tesoro y la industria de servicios financieros.

En cuanto a la amenaza terrorista nacional que involucra a extremistas violentos de cosecha propia y combatientes extranjeros, el FBI, el Departamento del Tesoro y la Red Contra los Delitos Financieros (FinCEN) son los actores fundamentales del gobierno.

Les incumbe a ellos compartir información de inteligencia con las instituciones financieras, en la máxima medida permitida. Esto les permitiría a las instituciones financieras desarrollar mecanismos más proactivos para identificar amenazas de cosecha propia. Dentro del FBI, las JTTF y la Sección de Operaciones de Financiación del Terrorismo (TFOS) son responsables del terrorismo y las investigaciones de financiamiento del terrorismo. La misión de TFOS es liderar a las autoridades de control legal y las agencias de inteligencia de los EE.UU. en derrotar el terrorismo mediante la aplicación de técnicas de investigación financiera y de explotación de la inteligencia financiera. TFOS apoya casos de las JTTF, ya sea realizando investigaciones financieras o proporcionándoles a las JTTF inteligencia financiera procesable para aumentar sus investigaciones.

TFOS se encuentra en el proceso de elaborar la información de inteligencia que planea entregar a las instituciones financieras de manera recurrente. Este es un signo alentador para las instituciones financieras que podrían beneficiarse de este tipo de intercambio de información. Del mismo modo, TFOS y FinCEN están trabajando en una iniciativa para evaluar las características de todos los combatientes extranjeros identificados que han viajado desde los EE.UU. a Siria. Esto tiene el potencial de ser una iniciativa muy importante para desarrollar la inteligencia significativa que las instituciones financieras podrían utilizar para fines de vigilancia específicas.

Las alertas rojas para los combatientes extranjeros que viajan a Siria desde los países occidentales incluyen:

- IP en zonas de conflicto tales como cerca de la frontera Siria, incluyendo Jordania y el Líbano, pero sobre todo Turquía
- Períodos de latencia de transacciones, que podrían ser el resultado de un entrenamiento terrorista o participación en combate
- Retiros de efectivo de cajeros automáticos en zonas de conflicto
- Transferencias bancarias a zonas de conflicto
- Publicaciones en medios de comunicación social (muchos combatientes extranjeros occidentales utilizan los medios de comunicación social)
- Préstamos estudiantiles, becas o derechos de dinero o cierres de cuentas asociadas con la compra de los billetes de avión para viajes al extranjero

Respecto de la financiación del terrorismo, las autoridades de control legal estatales y locales deben buscar la guía de las JTTF o directamente desde el TFOS, en la sede del FBI. Además, las autoridades de control legal estatales y locales deben participar en grupos de base con las entidades financieras que trabajan en sus jurisdicciones y en las de extensión con investigadores de fraude y antilavado de dinero (ALD) en instituciones financieras específicas.

Conclusión

Al enfrentar el cambio de las amenazas terroristas al país, con el cambio de énfasis en extremistas violentos nacionales y combatientes extranjeros, debemos asegurarnos de que nuestras defensas contra el terrorismo se adaptan para abordar la amenaza en evolución. Hay tres anillos de defensa que son igualmente importantes. La primera consiste en el sector público con la comunidad interinstitucional responsable de la amenaza global del terrorismo. Debido a la concentración en el país, debería haber un mayor énfasis en la aplicación de la ley, en particular a nivel local. Las JTTF son la pieza clave para nuestra seguridad nacional operativa interna. Afortunadamente, las JTTF han sido un modelo para la colaboración de las autoridades de control legal y para su éxito. El segundo anillo de defensa es la extensión a la comunidad para identificar e interceptar a las personas susceptibles de radicalización. Esto representa un desafío importante, pero si tiene éxito, podría obtener los mejores resultados a largo plazo para disminuir la amenaza de la cosecha propia. El tercer anillo de defensa consiste en identificar a los extremistas violentos de cosecha propia y a los combatientes extranjeros por medio del análisis financiero. Es alentador que TFOS y FinCEN se dedican a iniciativas analíticas para identificar patrones de actividad. Del mismo modo, muchos profesionales de cumplimiento de las instituciones financieras se dedican a iniciativas internas para identificar a los extremistas violentos de cosecha propia y a combatientes extranjeros.

Es mucho sobre lo que deberíamos estar preocupados por las amenazas terroristas cambiantes que enfrentamos. Tienen proporciones enormes. Al mismo tiempo, debemos congratularnos por los profesionales dedicados tanto en el sector público como en el privado que están trabajando diligentemente para asegurar que los tres anillos de defensa contra la amenaza a la patria puedan protegernos de los ataques. He tenido el privilegio único de estar asociado con muchos profesionales dedicados en ambos sectores. Trabajan incansablemente, con pasión y contracción a su labor para minimizar las amenazas terroristas difíciles que enfrentamos. Ya sea trabajando en la aplicación de ley, la extensión del gobierno hacia la sociedad o en otros cargos en el gobierno o en el cumplimiento del sector privado o de divulgación, estos profesionales dedicados merecen nuestra gratitud y respeto. Sigan luchando la buena batalla.

Debido a la concentración en el país, debería haber un mayor énfasis en la aplicación de la ley, en particular a nivel local

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

DE Columbo A Holmes

Los investigadores de delitos financieros pueden encontrarse tanto en el sector público como en el privado. Trabajan en actividades de control legal, organismos gubernamentales, instituciones financieras y empresas privadas. Al comienzo de sus carreras de investigación, muchos están provistos de una excelente formación y tienen investigadores de alto nivel que actúan como sus mentores. Muchos otros aprenden casi exclusivamente a través de la formación en el puesto de trabajo y dependen de sus habilidades innatas para progresar. Sin embargo, todos los investigadores, especialmente los nuevos, pueden encontrar inspiración y técnicas a menudo válidas junto con ideas en las obras de ficción.

Hay quienes hacen caso omiso de las obras de ficción de la literatura, el cine y la televisión considerándolas inútiles en tanto manuales de investigación porque a menudo suponen escenarios idealizados de resolución de delitos. Sin embargo, dentro de la narrativa central de las obras de ficción muchos de los atributos de los investigadores exitosos están allí para ser descubiertos. Estos atributos pueden adaptarse al mundo real y ayudar a guiar las investigaciones de la vida real. Una charla con casi cualquier investigador experimentado, incluso uno que no toma el concepto de ficción como una herramienta de formación útil, revelará que él o ella emplea muchos de estos atributos, si no todos. De hecho, los atributos más importantes para cualquier individuo a menudo son la pieza central de su reputación como investigador experto.

Vamos a explorar estos atributos y usted, el lector, puede sacar sus propias conclusiones. A los efectos de nuestro análisis, estos son los atributos:

- El razonamiento deductivo
- La tenacidad y la determinación
- La atención al detalle
- El conocimiento enciclopédico
- La intuición
- La utilización talentosa de datos
- El operador encantador

El razonamiento deductivo

Las dos formas principales de razonamiento son el deductivo y el inductivo. Ambas pueden ser precisas y defectuosas. El inductivo se basa por completo en la observación personal y su extrapolación a una teoría. Por ejemplo, todas las aves que John ha visto pueden volar. Por lo tanto, según John, todas las aves pueden volar. Si John no tenía conocimiento de un avestruz, emú o pingüino podría creer que esto es cierto sobre la base de todas las pruebas a su disposición. Un ejemplo adecuado sería que cada día de la vida de John el sol ha salido en el este. Por lo tanto, John confía en que mañana el sol saldrá por el este. Ese es el razonamiento inductivo adecuado y preciso.

> La clave para que el razonamiento deductivo sea efectivo son las pruebas exhaustivas y la aplicación del sentido común a los resultados

Pero el tipo de razonamiento a menudo citado en la resolución de los crímenes es el razonamiento deductivo. El razonamiento deductivo es muy similar a la base de este artículo. Uno desarrolla una teoría general, comprueba la teoría y luego la extrapola a partir de los resultados para llegar a una conclusión. Un ejemplo sencillo, pero defectuoso, es que Sally cree que todos los gusanos son comidos por las aves. Sally acaba de ver un ratón comiendo un gusano. Por lo tanto, el ratón es un pájaro.

Estos ejemplos de razonamiento defectuoso muestran que no es el atributo en sí mismo el que es un éxito, sino la forma en que se aplica. Por ejemplo, el razonamiento deductivo puede ser muy valioso si se utiliza correctamente. Un ejemplo de investigación del razonamiento deductivo de un delito básico sería que el examen de una víctima de asesinato demostró claramente que fue asesinado por un golpe en el lado derecho de la cabeza desde un ángulo que indica claramente que fue hecho por una persona zurda. Hay cuatro sospechosos: Bob, Jane, Bill y Fred. De los cuatro, sólo uno, Bob, es zurdo. Por lo tanto, Bob se ha convertido en el principal sospechoso. La clave para que el razonamiento deductivo sea efectivo son las pruebas exhaustivas y la aplicación del sentido común a los resultados. Muchas historias de delitos de ficción, y por desgracia muchas de los reales, contienen ejemplos de razonamiento deductivo defectuoso. Estas fallas a menudo quedan ilustradas en la ficción por las acciones de los investigadores incompetentes o ineficaces, como el Inspector Lestrade de las historias de *Sherlock Holmes* de Sir Arthur Conan Doyle.

Este enfoque de razonamiento es la herramienta principal de una serie de investigadores de ficción. El proceso se describe mejor en trabajos más largos, tales como libros y películas. En los formatos más cortos, especialmente programas de televisión, grandes porciones del proceso deductivo son conocidas generalmente sólo por el protagonista hasta que hay una "gran revelación" en la última escena, cuando surge la identidad del/a delincuente y de cómo el investigador lo/a identificó. La clave para el razonamiento deductivo con éxito es la aplicación de otros atributos críticos en el proceso de pruebas, como la atención a los detalles. Estos otros atributos se describen más adelante, ya que son los atributos que definen a otros investigadores de ficción. La conclusión es, como Sherlock Holmes declaró de manera sucinta: "Cuando se ha eliminado lo imposible, lo que queda, por improbable que parezca, debe ser la verdad".

La tenacidad y la determinación

La descripción clásica de este atributo es un "buen y sólido trabajo policial". Se destaca por largas horas de clasificación de datos y registros, una tediosa investigación de los testigos y una vigilancia aparentemente interminable. Los poseedores de este atributo se describen a menudo como bulldogs o terriers, razas conocidas por su renuencia a renunciar a una lucha y por la capacidad de desgastar a sus oponentes. La representación de este tipo de trabajo de una manera que se aproxima a la realidad rara vez se encuentra en la ficción que no sea la

literatura, simplemente por el tiempo necesario para llevarla a cabo. Sin embargo, en los procedimientos policiales más realistas, como demuestra *Law & Order* (la Ley y el Orden, en español), a menudo se alude a ello por parte de un superior/jefe que ordena que se pase a una acción o por el investigador de aspecto demacrado que acaba de regresar de caminar por la ciudad en busca de testigos o ha pasado horas buscando en cajas y cajas de documentos legales. Los investigadores nuevos deben darse cuenta de que este aspecto de la profesión, si bien recibe poca atención en la ficción, probablemente será la mayor parte de su trabajo. Sin embargo, es esta determinación de desenterrar pistas y encontrar respuestas que hace que un investigador sea exitoso. El programa de televisión

más elogiado porque representa la realidad de la investigación de delitos por los colaboradores y el público fue *Dragnet*. Este drama policial de 1960 se desarrolló en torno al concepto de mostrar la realidad de la labor policial en Los Ángeles, California, a raíz de las hazañas de los detectives Joe Friday y Bill Gannon. Fue tal el éxito en este esfuerzo que recibió elogios y reconocimiento por parte de los agentes de policía reales y las organizaciones policiales. Un nuevo investigador que se da cuenta de este atributo y lo acepta como parte del trabajo probablemente tendrá una carrera de investigación muy exitosa.

La atención al detalle

Uno de los aspectos de muchas historias de delitos es que una clave importante normalmente no es descubierta porque no se pone atención a los detalles iniciales de la investigación. Esta es también una herramienta dramática conveniente para construir tensión y proporcionar un gran número de giros a la trama. Para investigadores experimentados, a veces es la fuente de mayor frustración en una determinada pieza de ficción, simplemente porque los personajes no siguieron los procedimientos básicos para la investigación de la escena del delito. Este atributo es tal vez el mejor socio del razonamiento deductivo, ya que garantiza que todos los aspectos de una teoría han sido investigados y que la deducción resultante es muy probablemente correcta. La representación extrema de este atributo se exhibió en un programa de televisión titulado *Monk*. El ex detective de la policía Adrian Monk trabajó para el Departamento de Policía de San Francisco. La muerte de su esposa debido a un coche bomba lo lleva a una crisis nerviosa que resulta en el desarrollo de un trastorno obsesivo-compulsivo (TOC). La aflicción de la vida real aumenta significativamente las fobias de Monk, pero también mejora significativamente su atención a los detalles, a veces, los excesivamente minuciosos. Este atributo era a menudo la clave de su capacidad para actuar como consultor del departamento de policía a pesar de que le impedía la labor policial normal. El mensaje clave es que ningún detalle es demasiado pequeño y que vale la pena el tiempo y esfuerzo para revisar los aspectos aparentemente pequeños y sin importancia de un caso, porque es allí donde a menudo se encuentra una pista crítica.

El conocimiento enciclopédico

Este es uno de los atributos más improbables del investigador, a menos que haya nacido con una memoria fotográfica, porque el investigador promedio no tendrá el tiempo para leer, estudiar y memorizar toda la información necesaria para desentrañar todos los casos, ya que estará demasiado ocupado haciendo su trabajo. Sherlock Holmes, por supuesto, es el ejemplo obvio de la mente enciclopédica típica. Sin embargo, el surgimiento de especialistas en tecnología de la delincuencia en las funciones de investigación también ha dado lugar al genio que resuelve delitos de ficción (o al menos establece maneras de encontrarle una solución al caso). Estos personajes van desde la Dra. Temperance "Bones" Brennan, antropóloga forense de la serie de televisión *Bones* hasta a la Agente Especial Abby Sciuto de *NCIS* a todo el elenco de *Scorpion*. El conocimiento es mucho más accesible debido a la propagación de la tecnología de la información viable. Lo que un nuevo investigador lleva en su cabeza reduce el tiempo de la investigación sobre algunas pistas. Eso puede comprar suficiente tiempo para capturar al malo de la película antes de que huya del país.

La intuición

Este atributo está en la lista sólo porque se lo encuentra a menudo en historias de ficción de investigación y no porque no haya ninguna forma real de obtener este atributo. Algunas obras de ficción han seguido las hazañas de los detectives videntes. La validez de esta capacidad está mucho más allá del alcance de este artículo. Sin embargo, hay algunos programas de televisión recientes que se centran en las habilidades intuitivas de personajes involucradas en la investigación—sobre todo *The Mentalist* y *Psych*. Ambos programas se centran en personajes que pasan por ser videntes o son antiguos videntes "descubiertos". Ambos conjuntos de personajes utilizan habilidades de observación realzadas para aparecer ser conscientes de las cosas de las que los demás no se dan cuenta. La lección de este conjunto de personajes de ficción es que no hay que hacerse pasar por algo, sino que hay que utilizar cualquier habilidad (como la de observación) innata del individuo. Muchos investigadores de alto nivel contarán innumerables historias de guerra de cuando "siguieron su intuición" al investigar un caso. Un sentimiento intuitivo apoyado en la lógica no debe ser pasado por alto como talento útil de investigación.

La utilización talentosa de datos

Cuando se trata de resolver delitos financieros, vale la pena tener alguien en el equipo que puede manipular las hojas de cálculo e informes sin dudarlo. Por esto usted estudió matemáticas en la escuela primaria. En el

ambiente laboral de hoy impulsado por la tecnología, tendrá que usarlas. La representación ficticia de esto se encuentra a menudo en el especialista en informática en todos los procedimientos policiales como el de la serie CSI. Recuerde que tienen esas computadoras de compresión de tiempo y el acceso a todas las bases de datos que conoce la humanidad. No es así en el mundo real. Sin embargo, había un programa de televisión titulado *Numbers* donde el hermano de un agente del FBI, un genio de las matemáticas, utiliza funciones y herramientas matemáticas complejas para ayudar a resolver delitos principalmente por medio de probabilidades determinantes. Para los especialistas en matemáticas este era un espectáculo digno de ver, porque todos los cálculos eran reales, aunque no siempre se aplicaban adecuadamente. De hecho, Cornell University tiene un sitio web[1] donde todas las fórmulas matemáticas utilizadas en la serie son revisadas y explicadas. Tal vez la característica más satisfactoria de esta premisa para el investigador de la vida real es que las matemáticas siempre fueron calculadas en una pizarra, no en una computadora. Si es en una pizarra, tenía que ser real y lo era.

Es bastante difícil resolver delitos

Tal vez la conclusión clave de la ficción de hoy para los nuevos investigadores sea no tenerle miedo a la tecnología o las aplicaciones innovadoras de la ciencia o las matemáticas. Aunque nunca sustituirán a la mente humana como herramienta deductiva creativa, se puede ahorrar mucho tiempo y esfuerzo (cuando se usan y programan correctamente). También es probable que los investigadores del más alto nivel en una organización puedan restarle importancia al papel de la tecnología frente a los enfoques más tradicionales. Es un enfoque que podría dificultar una nueva carrera de investigación. Es bastante difícil resolver delitos. ¿Por qué pasar por alto los recursos técnicos y sin una buena razón? Sólo recuerde el aspecto de tiempo comprimido. Las computadoras son rápidas, pero no tan rápidas. Las representaciones de ficción como las citadas le dicen que si usted tiene una herramienta eficaz a su disposición la debe usar.

El operador encantador

Por último, pero casi no menos importante, aparece el operador encantador conocido como el especialista en interrogatorios. Esta habilidad es una característica tan común en la resolución de delitos de ficción como el razonamiento deductivo. Hay un subconjunto de esta habilidad que se basa en la intimidación física. Este subconjunto se descuenta para esta discusión y no es parte de ninguna habilidad recomendada a nuevos investigadores. Los estilos de interrogatorio más adecuados para los nuevos investigadores son los que emplean artimañas, técnicas psicológicas y "don de gentes" ejemplares. Dos interrogadores de ficción se destacan en programas de televisión. El primero es el Detective Columbo cuyo estilo sin pretensiones hacía que los sospechosos se sintieran superiores y en control y luego hacía "una última pregunta" que develaba el caso. El segundo es la Subjefa Brenda Leigh Johnson, del programa de televisión *The Closer*, una maestra en el reconocimiento y la explotación de los temores y debilidades de un sospechoso. Hay un montón de ejemplos de interrogatorio en la literatura, las películas y los programas de televisión. Si descarta los que utilizan la violencia física o la tortura, tiene una colección de herramientas viables para ayudar a llegar al meollo de la cuestión.

La realidad contra la ficción

Si bien las obras de ficción no son manuales para nuevos investigadores, proporcionan una visión de los conjuntos de habilidades aplicables que pueden dar forma a una carrera exitosa. El desarrollo de estos atributos básicos puede ampliar las capacidades de un investigador profesional y facilitar muchas de las tareas más arduas. Resolver un caso financiero puede identificar a los delincuentes que han evitado el enjuiciamiento o mucho más. Al Capone, apresado por evadir impuestos, es un ejemplo clásico. A veces tener a Holmes, Columbo o a Friday mirando sobre el hombro de uno—en sentido figurado por supuesto—puede ayudar a llevar una investigación a un final exitoso.

Ed Beemer, CAMS-FCI, APR, director, CorpComm Solutions LLC/Compliance Comm, Arlington, VA, EE.UU., efb@compliancecomm.com

[1] "Numbers Math Activities", Cornell University Department of Mathematics, http://www.math.cornell.edu/~numb3rs/

Los T-MEN:

Un legado de los Asesinos de Gigantes

"Scarface" Al Capone aparece aquí en la Oficina de Detectives de Chicago tras su detención por vagancia como Enemigo Público No. 1.

No hay un gánster más famoso que Al Capone. El nombre de Capone aún tiene una connotación infame en los EE.UU. y en todo el mundo. En el apogeo de su carrera de delitos, Capone fue tan bien conocido que las estrellas de cine y los extranjeros que viajaban a Chicago lo hacían sólo para obtener una visión de quien las autoridades llamaban el enemigo público número uno. Considerado como uno de los personajes más famosos del mundo y así de iconoclasta logró la portada de la revista *TIME* en 1930.

Hay quienes idealizan a Capone como un hombre que se hizo por sí solo viviendo según un código de honor. Para que nadie lo olvide, Capone era un matón despiadado, el símbolo de la anarquía épica que infectó rápidamente a los EE.UU. en los años 1920 y 30. Tan odiosas fueron sus hazañas que el Partido Comunista de los EE.UU. lo usó a él como propaganda.

Capone puede haber sido el gánster más llamativo, pero no era el único. Los EE.UU. estaban llenos de gánsteres como Capone que hacían sus negocios como empresarios con la bebida ilícita, la prostitución y el juego. Y por si sus fraudes no fueran suficientes, estaban en camino de controlar muchos aspectos del comercio diario. Si se quería hacer negocios, bueno, entonces mejor era pagarles. En este periodo de oscuridad, los ciudadanos perdieron muchas libertades a manos de gánsteres despiadados. Parecerá increíble ahora, pero los EE.UU. casi se parecía a lo que es México hoy: cárteles delictivos controlando la mayor parte del país. Como relató de aquellos tiempos el periodista, autor y ganador del Premio Pulitzer Marquis Childs: "En una ciudad tras otra, en comunidades grandes y pequeñas, el delito tenía licencia, estaba subsidiado. La gente decente desesperaba".

No era la escopeta la que permitía que estos mafiosos alcanzaran tal poder. Sí, tenían una predilección para repartir violencia, pero lo que permitió que el delito organizado floreciera durante la Prohibición fue la corrupción. Considere esto, Capone pagaba el 20 por ciento de cada dólar que invertía en el soborno. Un hombre al que no le temblaba la mano para romperle la cabeza con un bate de béisbol a alguien, nunca habría desembolsado tanto dinero si no le servía bien. Al llenarles los bolsillos a los políticos, la policía, los jueces y los funcionarios del gobierno se encontraba por encima de la ley y era intocable. Los policías honestos estaban bloqueados y desmoralizados. Incluso si arrestaban a un gánster, en poco tiempo el caso caía debido a algún alto funcionario al que se sobornaba.

La única cosa que le quitaba el sueño a Capone eran los pandilleros rivales. La competencia era mortal en aquel entonces, literalmente. En un esfuerzo por controlar las luchas internas de los gánsteres, Enoch "Nucky" Johnson (sobre quien se basa en realidad el tipo de *Boardwalk Empire*), organizó una reunión famosa en Atlantic City para que las diferencias territoriales pudieran resolverse sin violencia competitiva. Todos los grandes de la mafia estadounidense estaban allí. Estos cabecillas estaban empeñados en establecer nichos en el país y tenían la osadía de dejar que los periódicos lo informaran, posando para que se les fotografiara mientras paseaban por el malecón.

¡Atrapar a Capone!

No queriendo ver que el país rodara cuesta abajo, cuando fue elegido como presidente en 1929, Herbert Hoover hizo de "atrapar a Capone" una prioridad. En ese momento, las autoridades de control legal federales, incluyendo el FBI, eran pocas y generalmente ineficaces en cuanto al delito organizado. El Presidente Hoover necesitaba desesperadamente combatientes de delito federal de capacidad y habilidades probadas, un equipo de primera división. Aquí es donde Hollywood y los hechos históricos pierden contacto. Las películas retratan al gobierno recurriendo a Eliot Ness y a sus Intocables para salvar al país cuando los demás no podían o no querían. Aunque les cayó una lluvia de nominaciones a los Oscar, la película *The Untouchables* (*Los Intocables*, en español) es bastante una ficción. No hay evidencia de que el trabajo de Ness llevara a un solo día de cárcel para Capone.

Los principales asesores de Hoover le habían estado hablando al Presidente de la exitosa labor de un grupo de investigadores de delitos de la Oficina de Impuestos Internas denominado la Unidad de Inteligencia. La Unidad de Inteligencia estaba dirigida por un modesto, altamente calificado ex inspector de servicio postal cuyo nombre era Elmer Lincoln Irey. Desde 1920 hasta 1927, Irey lideraba la hercúlea tarea de librar al Servicio de Prohibición de sobornos causando que 256 agentes y funcionarios de alto nivel fueran imputados y que otros 706 perdieran sus cargos. Dentro de los altos cargos del gobierno, el modesto Irey era conocido como un empleado eficaz, un líder consumado.

Eliot Ness era un oficial de las autoridades legales en Chicago, jefe de "Los Intocables".

Bruno Hauptmann

Para capturar la pista de dinero de Capone, los T-MEN se embarcaron en una de las mayores operaciones encubiertas de la historia de las autoridades legales

En 1927, a Irey y sus T-MEN (como se les conoce comúnmente por su afiliación al Tesoro) se les entregó una herramienta muy novedosa pero eficaz para atrapar a los gánsteres. Mabel Walker Willebrandt, fiscal general adjunta, supervisora de delitos fiscales y de prohibición, argumentó convincentemente ante la Corte Suprema de Justicia que a un gánster se le puede imputar por evasión fiscal. Puede parecer una tontería ahora, pero entonces los gánsteres audazmente proclamaban que no tenían que reportar los ingresos obtenidos por actividades ilegales porque violaría su derecho de no autoincriminarse.

Con la victoria en la Corte Suprema de Justicia en mano, Willebrandt animó repetidamente hasta el punto en que logró que Irey formara un grupo especial que se focalizara en gánsteres que evadían impuestos. Willebrandt, la mujer del rango más alto en el gobierno federal, estaba frustrada porque el Servicio de Prohibición no hacía mella en el capo que controlaba el comercio de alcohol con impunidad. Aunque Irey tenía las manos llenas con otros infractores de grandes impuestos en los sectores de banca, corretaje de valores y la industria del cine (los grandes evasores de ese momento) apaciguó a Willebrandt y le dio un intento más. Nada más empezar, los T-MEN comenzaron a capturar a mafiosos antes considerados intocables. En particular, el presidente Hoover estaba contento de escuchar que los T-MEN estaban construyendo un caso sólido contra Ralph Capone, hermano de Capone. Confiado en que había encontrado su equipo de primera división, el Presidente instruyó al Secretario del Tesoro para que "atrapara a Capone".

Irey asignó a su investigador principal, Frank Wilson, como el agente encargado de la supervisión del grupo de T-MEN elegidos a mano para atrapar a Capone. Para capturar la pista de dinero de Capone, los T-MEN se embarcaron en una de las mayores operaciones encubiertas de la historia de las autoridades legales. El equipo de Capone tuvo la osadía de ocupar abiertamente tres pisos del Lexington Hotel en el centro de Chicago, que sirvió como sede central de la delincuencia. El agente encubierto de los T-MEN, Mike Malone, se infiltró en la organización Capone durante casi tres años viviendo con los gánsteres en la habitación 724 en el Lexington Hotel justo al lado del guardaespaldas de Capone. Malone se acercó tanto a Capone que se lo invitó a la fiesta de despedida de Capone, una velada de Capone cuando pensaba que iba a conseguir un arreglo favorable con la fiscalía. Capone lo conocía como "Mike Lepito", un gánster de Filadelfia que se escondía de la policía de Pensilvania.

La desaparición de Capone

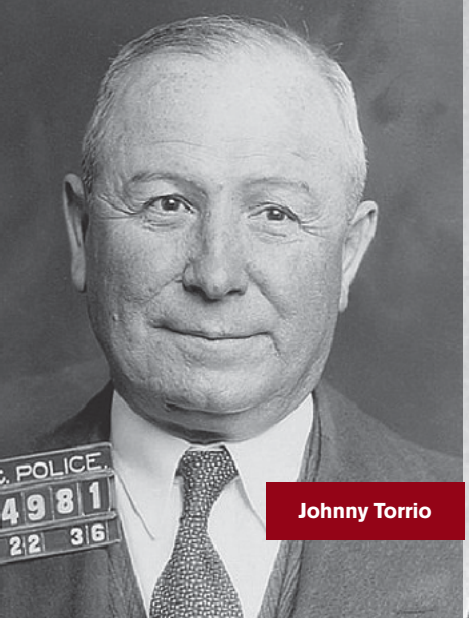
Todos los ojos del mundo estaban en el juicio de Capone. Wilson le demostró hábilmente al jurado cómo metódicamente había montado las piezas de los ingresos ocultos de Capone. Irey incluso atestiguó. Y, lo que muchos consideraron un deseo de muerte, Malone, todavía incógnito, reveló su verdadera identidad durante un descanso, cuando puso al guardaespaldas de Capone, Phil D'Andrea, contra la pared y lo apuntó con un revólver cargado. D'Andrea se había sentado junto a Capone durante el juicio mirando fijamente a cada testigo del gobierno con el fin de intimidarlos.

El 18 de octubre del 1931, los T-MEN lograron una victoria inimaginable cuando un jurado condenó a Capone por evasión de impuestos. Cuando los periodistas salieron a toda prisa para decírselo al mundo, de alguna manera Malone y Capone terminaron en el mismo ascensor. Capone miró a Malone y le dijo al agente encubierto sin miedo, "Jugaste, yo jugué. Perdí".[1] El derrotado poniéndose de hinojos ante el gladiador victorioso.

La desaparición de Capone fue noticia de primera plana. La condena de Capone les envió escalofríos por la espina a muchos capos. En un intento desesperado por salvarse a sí mismos, poco después de la condena de Capone, las filas de mafiosos se formaban en la Oficina de Impuestos Internas para presentar declaraciones de impuestos y pagar impuestos. Sólo en el área de Chicago, la recaudación de impuestos creció a más del doble.[2] Según el legendario experto en delito organizado y autor Hank Messick en su libro, *Secret File*, "La Unidad de Inteligencia se

[1] Elmer L. Irey, *The Tax Dodgers*, 1948.

[2] IRS.gov, Documentos históricos de Capone fueron liberados a través de una solicitud de FIOA en 2010.



Johnny Torrio


Waxey Gordon

encontró famosa después de la condena.... Sus investigadores silenciosos se convirtieron en los nuevos héroes populares de América, y su jefe, Elmer Irey, fue repentinamente una celebridad".[3]

Cuando a Capone lo sacaban de la sala, un periodista le preguntó a Irey, "¿Cuándo piensa perseguir a la mafia de Nueva York?" a lo que Irey respondió: "Salgo para Nueva York esta noche". De acuerdo con Messick, durante el próximo par de días los titulares proclamaban una nueva ofensiva contra mafiosos de Nueva York hecha por los "Asesinos de Gigantes". El apodo, los Asesinos de Gigantes (Giant Killers, en inglés), fue acuñado por primera vez por un juez federal que se dio cuenta de que los T-MEN constantemente derribaban gánsteres de tipo Goliat que nadie más había podido para matar.[4]

Según Robert Folsom en su libro *The Money Trail* (El Rastro del Dinero, en español), "Nueva York, no Chicago, fue la capital real del delito del país". En particular, Waxey Gordon, quien tenía un conglomerado criminal más sofisticado que Capone.[5] En marzo de 1931, el Presidente Hoover envió al Fiscal General de los EE.UU. un memorando declarando: "La organización especial establecida para el enjuiciamiento de los gánsteres de Chicago ha trabajado con más éxito....me pregunto si usted consideraría la creación de una organización tan especial en Nueva York....Creo que tal actividad puede ser beneficiosa para el país".[6] El presidente estaba llamando a su equipo de primera división de nuevo. Tomando en cuenta los deseos del comandante en jefe, Irey asignó a varios agentes para que trabajaran con un fiscal federal bastante joven llamado Thomas Dewey.

Queda enterrado en la historia el hecho de que fue el trabajo de los T-MEN lo que llevó a la captura del secuestrador del bebé de Lindbergh, Bruno Hauptmann

Irey y sus T-MEN tuvieron tanto éxito en Nueva York que no sólo derrocaron a Gordon sino que también entregaron evidencia a Dewey que condujo a las convicciones de corrupción de otros 46 mafiosos y funcionarios. Gordon estaba prófugo, pero Malone milagrosamente lo rastreó hasta su escondite en las montañas Catskill. La notoriedad que logró Dewey por el caso Gordon puso al joven fiscal en la mira pública, tanto que más tarde se convirtió en el gobernador de Nueva York y casi le gana la elección presidencial a Harry Truman.

El caso Lindbergh

En medio de numerosos viajes a Nueva York para pacificar al exigente Dewey, a Irey se le dio una tarea singular, que necesitaba la habilidad principal de un detective tipo Sherlock Holmes. En marzo de 1932, Irey recibió la orden de ir a Hopewell, Nueva Jersey, para asistir a uno de los hombres más famosos del mundo, Charles Lindbergh.

Al secuestro del hijo de Charles Lindbergh se le llamó el Delito del Siglo. Todo el mundo estaba seguro de que lo habían hecho gánsteres. Capone le dijo al famoso reportero Arthur Brisbane que sabía qué mafioso lo había hecho y si lo dejaran salir de la cárcel tendría al bebé en los brazos de los padres en el corto plazo. Millones de personas en todo el país leyeron el artículo de Brisbane, incluyendo Lindbergh. Haciendo caso omiso de la petición de J. Edgar Hoover para tomar el control de la investigación, el famoso aviador pidió la asistencia de Irey. Queda enterrado en la historia el hecho de que fue el trabajo de los T-MEN lo que llevó a la captura del secuestrador del bebé de Lindbergh, Bruno Hauptmann. Tras la condena de Hauptmann, Lindbergh pasó una nota personal a Irey en la que declaró: "Si no hubiera sido por su equipo, Hauptmann no estaría ahora enjuiciado y su equipo se merece todo el crédito por haberlo aprehendido".[7]

La búsqueda de la justicia

Por no dormirse sobre los laureles del trinomio Capone, Hauptmann y Gordon, Irey y sus T-MEN continuaron su búsqueda incesante de la justicia. Hubo un jefe político, Tom Pendergast, de Kansas City; Leon Gleckman, conocido como el Al Capone del Noroeste; el competidor de Gordon y miembro fundador de Murder Inc., Dutch Schultz; y el mentor de Capone y jefe del delito de Nueva York, Johnny Torrio. Con cada derribo de un capo vino la destrucción de los funcionarios

[3] Hank Messick, *Secret Files*, 1969
[4] Allen Hynd, *The Giant Killers*, 1945.
[5] Robert G. Folsom, *The Money Trail*, 2010.
[6] Robert G. Folsom, *The Money Trail*, 2010.
[7] Jim Fisher, *The Lindbergh Case*, 1994.

sobornados del gobierno incluida la pandilla de Huey Long—el mayor despliegue de corrupción en los EE.UU. Y luego, después de décadas de esfuerzos infructuosos por parte de las autoridades de control legal, los T-MEN lograron que se condenara a Nucky y fue Malone quien le puso las esposas.

Como dijo la revista *LIFE* de manera tan sucinta: "Cuando los mafiosos y políticos corruptos desafiaron las leyes locales, los T-MEN los atraparon por el delito federal de evasión de impuestos".[8] Debido a los Asesinos de Gigantes, las ciudades ya no eran del estilo de Gotham, controladas por pandilleros. Ya no se perdían las libertades a mansalva debido a despiadados delincuentes organizados.

> Cuando los mafiosos y políticos corruptos desafiaron las leyes locales, los T-MEN los atraparon por el delito federal de evasión de impuestos

Los T-MEN crearon un cambio de paradigma. Los jefes mafiosos y políticos corruptos ahora tenían que vivir en las sombras financieras, un enorme obstáculo para la construcción de un imperio delincuente. La riqueza inexplicada se había convertido en su talón de Aquiles.

Sobre la base de su trabajo como agente principal en los casos de Capone y Lindbergh, Wilson, de los T-MEN, fue designado Jefe del Servicio Secreto. Wilson revolucionó la forma en que el Servicio Secreto protegía al Presidente y la forma en que llevó a cabo investigaciones de falsificaciones. Fue Wilson quien mantuvo a Franklin D. Roosevelt (FDR) a salvo a todo lo largo de la Segunda Guerra Mundial. El siempre ingenioso Wilson reequipó la limusina a prueba de balas incautada a Capone, para que pudiera utilizarse para conducir al Presidente a dar su discurso del Día de la Infamia ante el Congreso el 8 de diciembre del 1941. Antes de esto, el Presidente no tenía un vehículo a prueba de balas, sólo J. Edgar Hoover tenía uno.

Impresionado por las destrezas de liderazgo de Irey, además de sus funciones como Jefe de la Unidad de Inteligencia, el Secretario del Tesoro Henry Morgenthau, Jr. creó un nuevo cargo en 1937 para Irey con el cual lo hacía coordinador de todas las agencias de actuaciones legales del Tesoro, incluyendo el Servicio Secreto, la Oficina de Alcohol, Tabaco, Armas de Fuego y Explosivos (ATF), Aduanas y la Oficina de Narcóticos. Los esfuerzos de liderazgo de Irey tuvieron tanto éxito que las autoridades de control legal del Tesoro contribuyeron con el 64 por ciento de todos los presos federales.[9]

En 1940, cuando el Congreso se reunió para aprobar el proyecto de ley de apropiación de la Unidad de Inteligencia, el presidente del comité de apropiaciones, el congresista John Cochran, señaló especialmente, para que quedara documentado en el registro del Congreso, los logros épicos de los T-MEN. Comenzó diciendo: "Cuando las autoridades legales perdieron su rumbo, especialmente en las grandes ciudades del país, esta unidad, por sus investigaciones de las evasiones de impuestos provocó acusaciones y envió a algunos de los mafiosos más notorios del país a la penitenciaría".[10]

El Servicio Silencioso

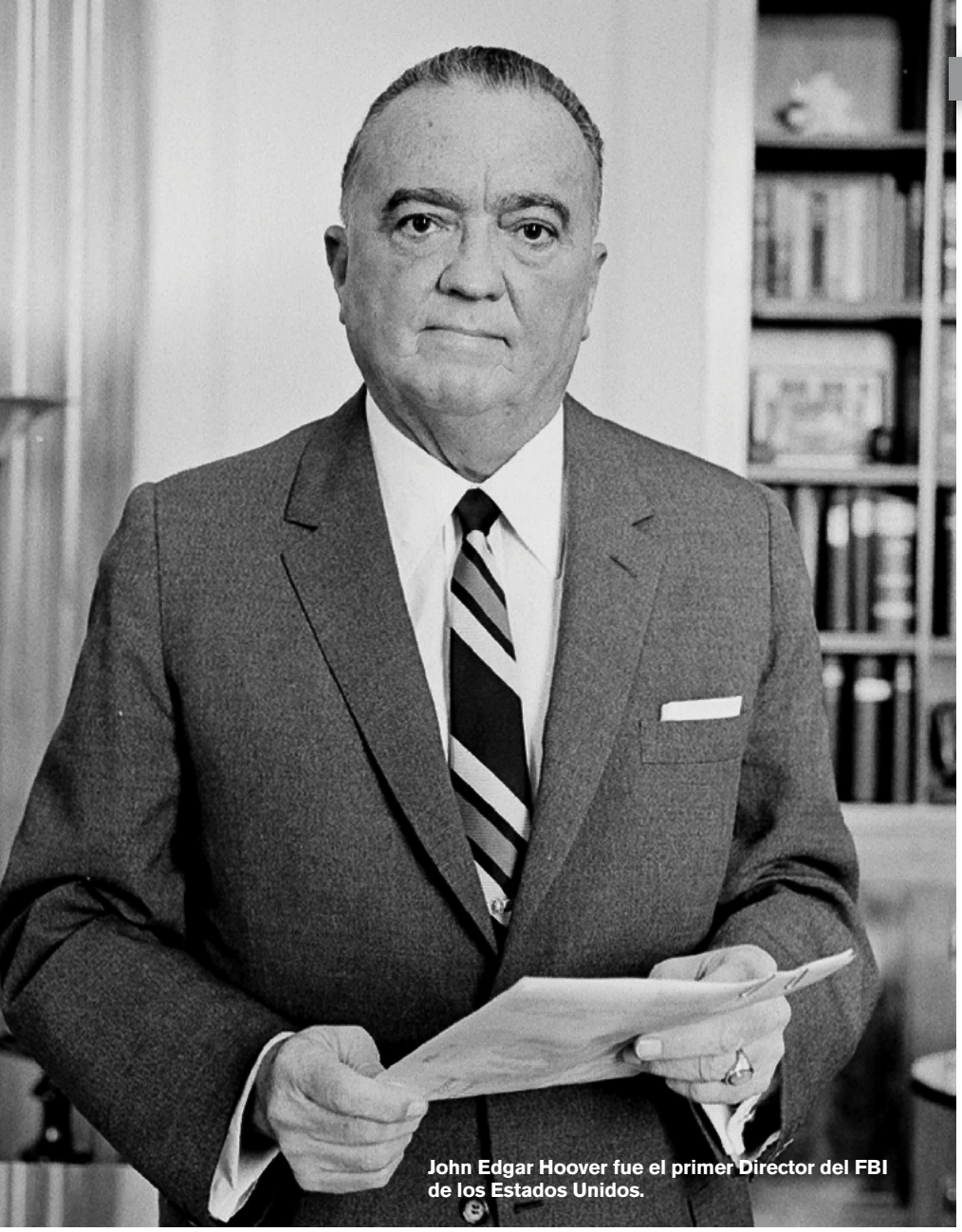
Durante su testimonio, Cochran dio a entender por qué muchos estadounidenses a menudo incorrectamente dieron crédito a los G-MEN de J. Edgar Hoover por los logros de los T-MEN de Elmer Irey, "Esta organización no tiene un agente de publicidad, ni servicio de información. No se encuentra en la primera página de los periódicos todos los días".[11] Desde el apresamiento de Capone, J. Edgar Hoover se había embarcado en una campaña masiva para darle al público una imagen que él representaba toda la autoridad legal. Esto incluía influir en Hollywood para producir 65 fotos de él y sus G-MEN en una gloriosa luz.[12] En marcado contraste, los T-MEN a menudo eran llamados el "Servicio Silencioso" sin hacer ningún esfuerzo para presumir de sus logros. Para señalar lo que el público se había perdido, Cochran dijo a sus compañeros miembros del Congreso, "Si la verdadera historia de sus actividades [de Irey] se pusieran en un libro se clasificaría como uno de los más vendidos en los Estados Unidos".[13]

Otra razón por la que Cochran probablemente conmemoró las hazañas policiales de los T-MEN fue por reconocer su sincronización impecable. Ya en 1927, cuando el presidente Hoover dirigió la Unidad de Inteligencia de "atrapar a Capone", la Segunda Guerra Mundial se acercaba al punto ciego del país. Parece casi providencial que el efecto colateral de salvar al país del submundo e infundir confianza y fe en la labor del gobierno se logró justo cuando Adolf Hitler alzó su fea cabeza hacia los EE.UU. y cuando el país necesitaba recoger significativamente más impuestos para financiar la guerra.

Promulgado en 1942, fue llamado el Impuesto de la Victoria, "Impuestos para derrotar al Eje." Rosie la Remachadora no sería capaz de soldar un solo tornillo sin los fondos críticos para pagar por los aviones, barcos y tanques. Hitler tenía más armas que los EE.UU. a principios de la Segunda Guerra Mundial y todos lo sabían. En cierto sentido, la Segunda Guerra Mundial fue toda sobre dinero. Los EE.UU. no podían imprimirlo o pedirlo prestado y los bonos de guerra no iban a cubrir el costo total. Nunca hubo tanta confianza en el sistema de impuestos para salvar a un país. Los EE.UU. incluso contrataron a Disney para producir un cortometraje protagonizado por el Pato Donald que promovía la presentación oportuna de las declaraciones de impuestos. Ganó un Óscar en 1943.

Para la comodidad de muchos, incluido el Presidente, para cuando los EE.UU. entraron en la Segunda Guerra Mundial, los ciudadanos estadounidenses tenían fe y

[8] "Elmer Irey Retires: Boss of Treasury T-Men was One of the World's Greatest Detectives," *LIFE* magazine, 2 de septiembre del 1946.
[9] Proceedings and Debate of the 76 Congress, third Session, The Congressional Record, 1940.
[10] Proceedings and Debate of the 76 Congress, third Session, The Congressional Record, 1940.
[11] Proceedings and Debate of the 76 Congress, third Session, The Congressional Record, 1940.
[12] Curt Gentry, *J. Edgar Hoover: The Man and the Secrets*, 1991.
[13] Curt Gentry, *J. Edgar Hoover: The Man and the Secrets*, 1991.



John Edgar Hoover fue el primer Director del FBI de los Estados Unidos.

un sentido de equidad respecto del sistema tributario. Fue un cambio radical en relación a los comienzos del decenio de 1920, cuando muchos sentían que el país se estaba convirtiendo en un experimento fallido de la democracia. FDR, reflexionando sobre este logro, dijo de los T-MEN en una carta personal a Irey de fecha de marzo de 1942, "A través de los años la Unidad de Inteligencia se ha convertido no sólo en una marca brillante de incorruptibilidad, sino también de servicios de primera calidad".[14] FDR sabía que la Oficina de Rentas Internas había sido marcada con el carácter de los T-MEN y que cualquier persona que intencionalmente no pagara su parte justa en los tiempos peligrosos de guerra sería llevada quirúrgicamente y rápidamente a la justicia, un gran consuelo para el comandante en jefe.

Cuando Irey se jubiló en 1946, una de las muchas cartas de gente que lo apreciaban vino del Director de la Oficina Federal de Prisiones, James Bennett. La carta decía: "Las cosas van a ser bastante especiales cuando pierda a mi mejor cazatalentos. Usted realmente nos ha mantenido ocupados durante tantos años que no voy a saber qué hacer conmigo mismo cuando pase a su muy merecida jubilación".[15] Las altas alabanzas de Bennett validan lo que la revista LIFE proclamó con motivo del retiro de Irey: "Jefe de Tesorería de los T-MEN fue uno de los mejores detectives del mundo".[16]

Siga el dinero

Para conmemorar la importante contribución de los T-MEN (ahora conocidos como el Centro de Investigación Penal del IRS), el Museo Nacional de la Delincuencia Organizada y Autoridades de Control Legal (The Mob Museum) presentará una nueva exposición llamada "Follow the Money" (Siga el Dinero, en español), con raras artefactos que cuentan la historia de los T-MEN librando al país de los mayores mafiosos de funcionarios corruptos. Se incluyen en esta exhibición cartas originales de FDR y Charles Lindbergh. La pieza central de la exposición será el arma personal del gran agente encubierto Malone. La pistola estaba bajo la almohada de Malone cuando falleció en sueños en 1960, mientras que aún era un T-MEN.

Según William Slocum en el libro *The Tax Dodgers* (Los Evasores de Impuestos, en español), "Se cuenta que la Unidad de Inteligencia de Elmer Irey era, literalmente, la última esperanza de los estadounidenses en nuestra batalla contra el submundo. Fue una batalla que la ciudadanía estaba perdiendo cuando la Unidad de Inteligencia desempolvó su coraje, astucia y las estatuas de ingresos de impuestos para detener a un enemigo dentro de nuestras fronteras que nos tenía más cerca de la derrota que cualquier enemigo extranjero". Slocum entonces hace la pregunta que da miedo, "¿Qué sería de todos nosotros, si esta última defensa hubiera fallado?" Pero los asesinos de gigantes no fallan. Y para la mala suerte fatal de Hitler los hombres salvaron a la nación justo en el último momento.

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

[14] Carte del 9 de marzo del 1942 de FDR a Irey; original en posesión del Mob Museum
[15] Carta del 14 de agosto de 1946 de James Bennett; el original en el Mob Museum.
[16] "Elmer Irey Retires: Boss of Treasury T-Men was One of the World's Greatest Detectives," *LIFE* magazine, 2 de septiembre del 1946.

La reestructuración de las investigaciones de BSA/ALD

Isaac Newton escribió una vez que "Construimos demasiados muros y no suficientes puentes". Estas palabras nunca han sido más ciertas. Nuevas tendencias en el siglo XXI están obstaculizando inadvertidamente a las autoridades de control legal y frustrando el intento de la Ley de Secreto Bancario (BSA). El péndulo de la opinión pública respecto de las tácticas de la aplicación de la ley, una vez más ha oscilado de incuestionable a escéptico. Lo que una vez fueron los modelos destacados y probados de intervención de las autoridades de control legal ahora deben ser técnicas reinventadas con el fin de continuar arrasando empresas criminales.

La historia

Si bien la BSA fue promulgada en 1970, no alcanzó su pleno potencial hasta después del 9/11. A raíz de esos ataques, las autoridades de control legal llevaron a cabo esfuerzos para combatir mejor la financiación del terrorismo y el lavado de dinero. El gobierno reconoció la necesidad de más Equipos de Revisión de Reportes de Operaciones Sospechosas (ROS) diversos y activos. En noviembre de 2005, el Departamento de Justicia (DOJ) publicó "A Guide to Creating a Suspicious Activity Report Review Team" (una guía para la creación de un equipo de revisión de reportes de operaciones sospechosas). Fue natural y lógico que las dos principales divisiones de confiscación de bienes de los organismos de aplicación, la Sección de Confiscación de Bienes y Lavado de Dinero (AFMLS) del DOJ y Oficina Ejecutiva de Confiscación de Bienes del Tesoro (TEOAF) del Departamento del Tesoro de los EE.UU., serían los principales coordinadores y financiadores de estos esfuerzos. El decomiso de activos se consideró un importante componente de investigación en cualquier caso de lavado de dinero y el lavado de dinero fue y sigue siendo un aspecto subrepticio de numerosos delitos.

El Congreso buscó, luchó por y finalmente promulgó una ley que refleja que el delito de estructuración de divisas no tiene por qué estar asociado a un delito específico. Por su propia naturaleza, ¡el delito involucra decenas de miles de dólares en efectivo! De acuerdo con el GAFI, "la Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC) realizó un estudio para determinar la magnitud de los fondos ilícitos generados por el narcotráfico y el delito organizado y para investigar en qué medida estos fondos se lavan. El reporte estima que en 2009, se lavaron ganancias del delito que ascendieron a 3,6 por ciento del PIB mundial, con 2,7 por ciento (o $1,6 trillón)".[1] Con tanto dinero lavado por año, la discreción procesal estaba disponible para los delitos de estructuración con motivos claramente más regulatorios o de evasión fiscal. La confiscación de bienes civil a menudo parecía una adjudicación apropiada en lugar de una potencial condena penal grave en casos de esa naturaleza.

Ya existía la Ley de Reforma de la Confiscación de Activos Civiles (CAFRA) de 2000. CAFRA fue diseñada y aprobada como ley para hacer frente a los mismos supuestos abusos del gobierno que actualmente están haciendo titulares. Un elemento disuasorio de CAFRA requiere que el gobierno pague los honorarios legales de un abogado litigante cuando cualquier activo fue identificado como injustamente incautado. Esto se refiere específicamente a las preocupaciones de que los altos honorarios legales impedían desafíos judiciales. Desafiar una confiscación en el "tribunal de la opinión pública" lo convierte en titular excitante para los diarios; sin embargo, con demasiada frecuencia, la verdad total detrás de muchos casos relacionados con actividades de dinero en efectivo tienen historias menos nobles. Muchos de los que reclaman probablemente se han negado a aprovechar la protección de la CAFRA porque temen la exposición surgida de las cuestiones subyacentes: el subterfugio, el engaño, la mentira y temas fiscales referidos a la razón por la cual se usó efectivo. Los familiares, amigos y compañeros de trabajo a menudo se encuentran entre los que están siendo engañados por estos esquemas. Por ejemplo, está la señora mayor que había planeado presentar sus operaciones sospechosas en efectivo simplemente como un pobre manejo de sus ahorros de toda la vida. Eso fue hasta que los investigadores rastrearon el origen de los fondos a su hijo médico que estaba tratando de ocultar más de un millón de dólares durante su proceso de divorcio. Para los medios de comunicación se trataría de una "pobre vieja" víctima del exceso de celo de las autoridades de control legal, pero la ex esposa del médico discreparía.

[1] "What is Money Laundering," The Financial Action Task Force (FATF), http://www.fatf-gafi.org/pages/faq/moneylaundering/

Las paredes

Recientemente, una serie de noticias del diario han estado creando la percepción de que la mayoría de los casos de estructuración implican principalmente a pobres inocentes o propietarios de pequeñas empresas luchadores que desconocen que las múltiples transacciones que suman decenas de miles en efectivo podrían levantar sospechas. Las confiscaciones de estructuraciones están retratadas ahora como afectando desproporcionadamente las empresas indigentes o pequeñas que están al borde de la quiebra. El sin sentido potencial es irrelevante en tales causas excesivamente dramatizadas. Por ejemplo, tras investigar, se encontró que el propietario supuestamente luchador de una licorería en un barrio pobre dirigía un negocio muy lucrativo en efectivo, tenía casi un millón de dólares en ingresos no justificados por un análisis de costo/beneficio. El dinero había sido estructurado en una cuenta bancaria y había sido reportado como ingresos en su declaración de impuestos de negocios.

El tribunal de la opinión pública, independientemente de los hechos, prevalece en la actualidad. Las leyes de la BSA diseñadas para la detección, la interrupción y el desmantelamiento de las organizaciones delictivas son ahora objeto de un intenso escrutinio. El decomiso de activos o la amenaza de que se hará, ha dado lugar a cientos, si no miles, de exitosas investigaciones penales de lavado de dinero y otras motivadas financieramente. Se han alegado acusaciones y titulares sensacionalistas sobre dinero confiscado sin que hubiera delito y sin la orden de un juez cuando en realidad a menudo ambos existían. Los acuerdos con los fiscales para reducirse a sanciones civiles en vez de denuncias penales ahora se caracterizan como casos de víctimas totalmente inocentes en vez de adjudicación razonable. Esta "cuestionable" exageración está siendo utilizada como justificación para eliminar esta poderosa herramienta de investigación. De hecho "la Restauración de la Ley de la Integridad de la Quinta Enmienda (FAIR), introducida recientemente por el Senador Rand Paul, R-Ky., y el Rep. Tim Walberg, R-Mich., frenaría las confiscaciones relacionadas con la estructuración, y corregiría los defectos de la ley de decomiso civil federal que juega en contra de las personas

cuya propiedad se confisca y permite que los organismos de control legal se beneficien de la confiscación".[2]

En una época en que debería haber más, y no menos intervención, a los equipos de revisión de ROS que operaban bajo la guía estricta de las leyes federales y un sistema de frenos y contrapesos ahora se les pide que reduzcan este enfoque tradicional de investigación. De acuerdo con un comunicado de prensa del 31 de marzo del 2015 del Departamento de Justicia de los EE.UU., "como parte de la revisión integral continua del programa de confiscación de bienes del Departamento de Justicia, el fiscal general Eric Holder emitió hoy un documento dedicado al uso de las autoridades de confiscación de bienes en las más graves transacciones bancarias ilegales, restringiendo los decomisos civiles o penales para la estructuración hasta después de que un acusado lo ha sido penalmente o se ha encontrado que se ha involucrado en una actividad delictiva adicional, en la mayoría de los casos".[3] Los movimientos sospechosos de gran cantidad de efectivo más comúnmente reportados en ROS serán considerados legítimos a menos que un nexo delictivo articulable pueda asociarse fácilmente. Esto parece contradictorio con la propia naturaleza de las fases de estratificación e integración de lavado de dinero para disociar los dineros de la fuente ilícita. El concepto de que el dinero lavado ilícito se estructuraría, y se integraría con "dinero limpio" con el fin de ocultar el origen delictivo fue reconocido durante la redacción de las leyes de la BSA.

Los fiscales federales asignados a los juicios basados en los ROS, especialmente los delitos de estructuración y lavado de dinero, ahora deben lidiar con la presentación de algo más que los elementos del(os) delito(s) a jurados potenciales desinteresados. Ahora los fiscales se ven obligados a demostrar los elementos delitos y que el acusado conocía los reglamentos y deliberadamente los evitó y/o debe probar que el acusado evitó deliberadamente las regulaciones para un propósito delictivo específico. En cuanto a la estructuración, algunos fiscales pueden ahora exigir comprobar que una persona tenía una razón para saber o sabía que el dinero provenía de una fuente delictiva. Los equipos basados en ROS están recibiendo instrucción de sus fiscales que, a fin de enjuiciar por estructuración, los equipos deben exponer el nexo criminal a pesar de la falta de disposición de las leyes de la BSA.

Cualquiera que haya pasado tiempo en un equipo de revisión de los ROS sabe que la BSA no sólo ha puesto al descubierto el lavado de dinero sino que también ha captado una gran cantidad de otros trucos financieros. El hecho es que la estructuración fue diseñada para captar el dinero sucio, pero una gran cantidad de "dinero limpio" se ensucia través de la estructuración. Engañar en un divorcio, una herencia, o una oferta de negocio; pagar por prostitutas, drogas, un trabajador no anotado, corredores de apuestas y casi siempre la evasión fiscal que los acompaña, son todas las cosas sucias que empiezan con dinero limpio. El requisito previo de que la definición ambigua de "estructuración de dinero limpio" se elimine antes de la iniciación de una investigación de estructuración ahora es una realidad en detrimento de los Equipos de Revisión de ROS.

Existen estos desafíos a la vez que las instituciones financieras están pidiendo más validación de que sus gastos de BSA/ALD están logrando los objetivos previstos. ¿Hay datos empíricos o evidencia más allá de las declaraciones de autoridades de control legal genéricas que los ROS están produciendo una verdadera interrupción y desmantelamiento de los esquemas de lavado de dinero? Las instituciones financieras a menudo expresan su frustración por el aumento y confusas regulaciones sobre todo cuando ni los reguladores ni las autoridades de control legal no proporcionan ninguna prueba verificable de que los requisitos adicionales son eficaces o eficientes en la misión del ALD. ¿Es el estado actual de la BSA funcionando como fue diseñada ni pensada? La falta de un puente de comunicación entre la reglamentación y las autoridades de control legal necesita una revisión igualmente seria.

Con el fin de "cerrar las brechas" entre estas barreras y cumplir con esta carga de prueba obligatoria, las tácticas de investigación deben mejorar y superar la publicidad negativa de los equipos de decomiso de activos basados en los ROS logrando:

- La obtención detallada de ROS de manera rápida
- La implementación de "Llame y Converse"
- La colaboración con la policía local
- Entrevistar a los asociados del objetivo

Los puentes

Los equipos de investigación basados en ROS pueden seguir prosperando sólo a través de relaciones de trabajo de voluntariado con las entidades financieras que se requieren para reportar operaciones sospechosas. Por lo general, sólo hay una revisión mensual, por lo tanto, una oportunidad para un ROS para darle una impresión a un investigador. Las instituciones financieras pueden detectar fácilmente la identificación inicial de conducta sospechosa por medio de sus programas de ALD; pero la detección no es lo mismo que la divulgación. Al igual que cualquier investigación eficaz, es necesario contar con una comunicación clara, incluyendo los detalles minuciosos de conducta sospechosa.

También es imprescindible que las secciones de BSA/ALD de las instituciones financieras hacen divulgación constante a la policía para hacer y mantener su existencia y la misión conocida. Los ROS, como muchas otras bases de datos de autoridades de control legal, son impersonales. "José el Sinvergüenza" puede estar en la base de datos de antecedentes penales, pero no es hasta que a un detective se le dice que "José" se acaba de mudar al barrio que empieza a prestarle atención a "José". Lo mismo puede decirse de los ROS. Simplemente archivarlos y pasar al siguiente caso no les dará la atención que se merecen.

Desde que se abre una cuenta hasta la primera señal de actividad financiera inusual, la responsabilidad que recae sobre la institución financiera consiste en obtener y documentar adecuadamente los detalles críticos y suministrarlos expeditivamente a las autoridades de control legal. Ahora más que nunca, la necesidad de detalles documentados y clara documentación de apoyo—no importa lo aparentemente pequeño o insignificante—puede ayudar a fundamentar el motivo, un nexo criminal, una fuente ilícita, etc. Un ROS

[2] "Too East to Seize: New Report on IRS Forfeitures Highlights Need for Broad Civil Forfeiture Reform," Institute for Justice, 3 de febrero del 2015, https://www.ij.org/seize-first-question-later-release-2-3-2015

[3] "Attorney General Restricts Use of Asset Forfeiture in Structuring Offenses," The Department of Justice (DOJ), 31 de marzo del 2015, http://www.justice.gov/opa/pr/attorney-general-restricts-use-asset-forfeiture-structuring-offenses

escrito con información concisa respecto al "qué y por qué" de la conducta sospechosa tiene una mayor oportunidad de llegar a los umbrales de investigación y procesamiento. El intercambio voluntario de todos los detalles puede ser la clave para el impulso y la motivación de la nueva necesidad para su enjuiciamiento.

Una técnica ventajosa frecuentemente subutilizada es el "Llame y Converse" ("Knock and Talk", en inglés), que es la oportunidad de las autoridades de control legal para hablar con el o los objetivo(s), testigos, compañeros de trabajo, familia, etc., en referencia a la anomalía inusual detectada durante la investigación financiera. En un nivel de "Llame y Converse", no se ha tomado ninguna acción de cumplimiento en este momento y por lo tanto cualquier entrevista se considera voluntaria. Además, los representantes de las instituciones financieras también son capaces de hacer contacto con el titular de la cuenta en relación con una irregularidad inexplicable. Generalmente, las personas son naturalmente inclinadas a explicar su comportamiento. Las minucias de las explicaciones/excusas pueden exponer el engaño y la desviación. Un objetivo que participa en la actividad nefasta muy probablemente exhibirá las alertas rojas indicadoras de utilizar el engaño, así como resistirá cualquier sustanciación.

Otra estrategia es la de los equipos basados en los ROS de colaborar más con la policía local que pueden estar llevando a cabo investigaciones sobre las actividades delictivas que puedan tener un nexo con el lavado de dinero. Trabajar un caso desde la perspectiva de la actividad delictiva subyacente puede exponer a un ROS que, aunque cuestionable, no puede tener inicialmente cumplido el umbral de un equipo de investigación y la actividad inusual que puede no haber sido evidente para la institución financiera. Una vez más, la documentación completa por parte de la entidad financiera en un ROS es esencial para ser capaz de identificar una relación entre la conducta delictiva y la conducta bancaria aberrante.

En un esfuerzo por demostrar la moneda ilícita en efectivo, las estrategias de investigación encargadas de las autoridades de control legal deben incluir esfuerzos de entrevistar a alguien que pueda haber tenido contacto con el objetivo. Puede ser engorroso recopilar información de esta manera, pero el contacto con los cajeros de primera línea, asociados, familiares, etc., constituye una medida necesaria a fin de disminuir la distancia entre una investigación y la acción de cumplimiento.

La reforma de las tácticas de investigación pueden ser inconveniente y exigente para las instituciones financieras y las autoridades de control legal. Ser flexible es la manera de que las autoridades de control legal superarán la mala prensa y, en definitiva, con la asistencia continua de los agentes de BSA/ALD, llevarán a cabo una investigación que dará lugar a una apropiada sentencia penal dura, así como un avance en la misión del ALD. Ahora es el momento para reestructurar una investigación de BSA/ALD.

Stacey Ivie, M.Ed., Oficial de la fuerza de tareas, Washington/Baltimore HIDTA, Northern Virginia Financial Initiative (NVFI), Annandale, VA, EE.UU., sivie@wb.hidta.org

Erik Rosenblatt:

ACAMS Today se sentó con Erik Rosenblatt, Agente Especial Adjunto a Cargo del Grupo de Tareas de Delitos Financieros de El Dorado (EDTF) y del Área de Delitos Financieros de Alta Intensidad de Nueva York/Nueva Jersey (HIFCA) para discutir el importante papel del EDTF y la importancia de asociarse.

Antes de trabajar en EDTF, Rosenblatt fue Agente Especial Adjunto Encargado de la División Nacional de Seguridad de Investigaciones de Seguridad Nacional (HSI) y también se desempeñó como enlace con el Departamento del Tesoro para el financiamiento del terrorismo y la delincuencia financiera y del Departamento de Justicia (DOJ), y la sección de confiscación de activos y lavado de dinero (AFMLS).

ACAMS Today: ¿Cuál es su papel actual y cuáles son sus responsabilidades dentro de este papel?

Erik Rosenblatt: Soy Agente Especial Adjunto a Cargo (ASAC) en la oficina de Nueva York de ICE Investigaciones de Seguridad Nacional (HSI). He sido Agente Especial durante más de 17 años y empecé con el Servicio de Aduanas de los EE.UU., Oficina de Investigaciones. El ASAC Steven Schrank y yo gestionamos el Grupo de Acción Financiera de Delitos de El Dorado ubicado dentro de la oficina de campo de HSI de Nueva York. También superviso la HIFCA NY.

AT: ¿Cómo se conecta HSI con el Grupo de Delitos Financieros de El Dorado (EDTF)?

ER: Las Investigaciones de Seguridad Nacional (HSI) lideradas por el Grupo de Tareas de El Dorado (EDTF) se estableció en 1992 como una iniciativa de un área de Alta Intensidad de Narcotráfico (HIDTA) para combatir la creciente amenaza de lavado de narcodinero en el área metropolitana de Nueva York. Desde su creación, la EDTF se ha diversificado para hacerle frente a todos los delitos financieros y ha evolucionado hasta ser el mayor y más exitoso grupo de tareas de delitos financieros en el mundo. El EDTF investiga todos los delitos financieros bajo jurisdicción de las leyes federales y locales.

Además de su función de investigación, el EDTF opera el Área Financiera de Delitos de Alta Intensidad (HIFCA) NY/NJ, una unidad de inteligencia financiera que sirve como componente táctico de inteligencia y de minería de datos del EDTF. HIFCA también proporciona capacitación para el sector privado y trabaja con referencias de ROS.

AT: ¿Qué papel juega el EDTF en la lucha contra la delincuencia financiera?

ER: Nos enorgullece mucho el alto nivel de especialización en HSI NY y dentro del EDTF. Ya que HSI tiene la autoridad de investigación más amplia de cualquier agencia federal, y el EDTF está compuesto por investigadores financieros que traen sus propios recursos, no hay límite a nuestro inventario de investigación—hemos hecho todo.

Pero igual de críticas son las relaciones muy fuertes que tenemos con los fiscales locales, estatales y federales en el área de Nueva York. Esto no sucedió de un día para otro sino que representa 25 años de construir confianza y demostrar que nuestros casos son minuciosos y honestos.

Debido a esta experiencia temática y las relaciones fuertes que tenemos con los fiscales, HIFCA puede hacer su investigación de una pista y ofrecer un paquete de investigación a un grupo de investigación dentro de algunas horas de haberse informado. También podemos lograr que un federal o un fiscal local se encargue del caso rápidamente.

El acceso no debe limitarse a "conozco a un tipo"

Foto por: Wilerson S. Andrade

AT: ¿Qué organismos participan con el EDTF?

ER: El EDTF está integrado por más de 250 personas de 29 agencias de autoridades legales del área de Nueva York y Nueva Jersey, incluyendo agentes especiales, investigadores estatales y locales, funcionarios, analistas de inteligencia y fiscales. Es realmente único.

AT: ¿Qué tipo de formación ofrece EDTF al sector privado?

ER: El beneficio de la experiencia y la amplia gama de investigaciones de HSI y otras agencias de EDTF participantes que le trae al sector privado de NY/NJ consiste en compartir ejemplos de casos con el sector privado para ayudarlo a entender lo que está buscando. Por ejemplo, es mejor entender cómo la trata de personas y el contrabando son diferentes y la forma en que funcionan, o cómo las redes contra la proliferación operan, para identificar mejor la actividad ilícita que conduce al movimiento sospechoso de dinero. Miembros de EDTF y analistas de HIFCA realizan rutinariamente presentaciones de divulgación en instituciones financieras locales y organizaciones empresariales. Cualquier persona interesada puede ponerse en contacto conmigo a través de la oficina de HSI NY.

AT: La EDTF ha tenido abundante éxito desde su creación, ¿puede compartir algunas estadísticas sobre los tipos de delitos financieros que han cerrado?

ER: Desde sus inicios, agentes de EDTF y oficiales del grupo de tareas han incautado más de 2 mil millones de dólares en ganancias ilegales, hecho más de 3.700 arrestos criminales y realizado más de 72 operaciones encubiertas. En el año fiscal 2014, los oficiales de EDTF lograron 396 detenciones, 247 acusaciones, 220 condenas e incautaron más de $58,4 millones.

AT: ¿Qué consejos puede compartir sobre cómo los sectores público y privado pueden construir alianzas mejores?

ER: El EDTF siempre ha tenido una fuerte asociación con el sector privado. Contamos con un grupo llamado Cornerstone, que durante más de una década, como parte de un programa nacional de HSI, interactúa con el sector privado para proporcionar conocimientos y para conseguir pistas e inteligencia. El HIFCA también tiene una comunicación abierta con las unidades de inteligencia financiera (UIF) del sector privado.

Pero este año dimos un paso más allá mediante la creación de una asociación con los ejecutivos de las instituciones financieras, y celebramos nuestra primera mesa redonda el pasado mes de febrero en Nueva York. Creemos firmemente que las discusiones de cumplimiento no deben limitarse a los ajustes formales. El cumplimiento de ALD no debe ser un juego de adivinanzas; tenemos tanto que aprender del sector privado como ellos de nosotros. Cada uno tiene su misión, y tenemos que entender el mundo del otro un poco más; el acceso no debe limitarse a "conozco a un tipo".

Además, en junio vamos a celebrar nuestro 13º *Simposio Anual de Delitos Financieros* en el Federal Reserve Bank de Nueva York. El simposio es principalmente sobre el cumplimiento del ALD, pero será también para autoridades del control legal y otros funcionarios del gobierno; sin embargo, es sólo por invitación a nuestros socios de la industria. Este año ya está completo, pero esto nos da la oportunidad de compartir las tendencias que hemos identificado, discutir temas de actualidad y presentar ejemplos de casos a una audiencia de unas 300 personas.

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

¿Cómo no pudo el sistema de ALD de Australia prevenir el lavado de miles de millones en ganancias de la corrupción?

Australia, miembro fundador del Grupo de Acción Financiera Internacional (GAFI) y del Grupo Egmont, ha sido considerado un país con un régimen robusto de anti-lavado de dinero/financiamiento contra el terrorismo (ALD/CTF). Sin embargo, el anuncio hecho por la Policía Federal Australiana (AFP)[1] de su operación para apoderarse y repatriar mil millones de dólares australianos ($770 millones de dólares) de activos ilícitos invertidos en Australia por funcionarios chinos corruptos[2] ha confirmado los temores de que el enfoque de Australia a la regulación de ALD en realidad ha dejado expuesto al país.

Existe la esperanza de que el nuevo director general de los Reportes de Operaciones de Australia Centro de Análisis (AUSTRAC), el regulador de ALD/CTF de Australia y la unidad de inteligencia financiera especializada (UIF), "hablará suavemente y llevará un gran garrote" cuando se enfrente a poderosos intereses creados por medio del cumplimiento de las leyes generales ya existentes, pero aparentemente poco utilizadas hasta la fecha.

Fondos ilícitos en Australia

La afirmación de que hay grandes volúmenes de activos extranjeros ilegales en Australia no resulta una sorpresa para algunos. Aunque Australia había quedado razonablemente bien en evaluaciones anteriores de ALD/CTF de GAFI, Australia no ha implementado una serie de mejoras recomendadas, mientras que el rechazo de las repetidas advertencias de que los sistemas de ALD de Australia no funcionan según lo previsto.

En una investigación de 2008 del Senado, AUSTRAC admitió que "Australia es un país de destino importante para los fondos derivados de la corrupción dentro de la región".[3]

Las autoridades de Papúa Nueva Guinea (PNG), el vecino geográfico más cercano de Australia, públicamente notificaron a Australia, en más de una ocasión, del mal uso habitual del sistema financiero australiano por delincuentes de su país. En octubre de 2012, el jefe del grupo de trabajo anticorrupción de PNG, Sam Koim,[4] destacó la cuestión de los bancos y las autoridades australianas a través de una presentación realizada en un evento de AUSTRAC.

A finales de 2013, se planteó en los medios de comunicación de Australia con denuncias concretas que el gobierno australiano hacía la vista gorda al lavado de dinero a gran escala.[5, 6] Esto incluía sumas de hasta cientos de millones lavados cada año por medio de bancos, agentes inmobiliarios y casinos.

La respuesta de Australia

Debida diligencia del cliente

La respuesta oficial a estas acusaciones del gobierno australiano en 2013 fue que "el gobierno de Australia rechaza estas afirmaciones. Australia tiene un marco sólido para prevenir y detectar el lavado de dinero, y para asegurar que Australia no es un refugio seguro para las ganancias de la corrupción".[7]

Esta respuesta del gobierno llegó a decir que este robusto sistema se basa en el hecho de que "se requiere que los bancos y otros negocios regulados tengan los controles adecuados para contrarrestar el riesgo de lavado de dinero planteado por funcionarios y políticos extranjeros corruptos".[8]

En realidad, el gobierno de Australia tenía razón en cuanto a que las recomendaciones del GAFI, antes y todavía hoy, requieren estas medidas de controles de diligencia debida del cliente (DDC). Sin

[1] Philip Wen, "Australia set to seize assets of corrupt Chinese officials," *The Sydney Morning Herald*, 20 de octubre del 2014, http://www.smh.com.au/world/australia-set-to-seize-assets-of-corrupt-chinese-officials-20141019-118kl3.html

[2] Deborah Cornwall, "Corrupt Chinese officials retreating to Australia targeted in joint China-Australia police operation, ABC News, 21 de octubre del 2014, http://www.abc.net.au/news/2014-10-21/corrupt-chinese-officials/5828768

[3] AUSTRAC, "Inquiry into the economic and security challenges facing Papua New Guinea and the island states of the southwest Pacific," octubre de 2008, http://www.aph.gov.au/~/media/wopapub/senate/committee/fadt_ctte/completed_inquiries/2008_10/swpacific/submissions/sub45_pdf.ashx

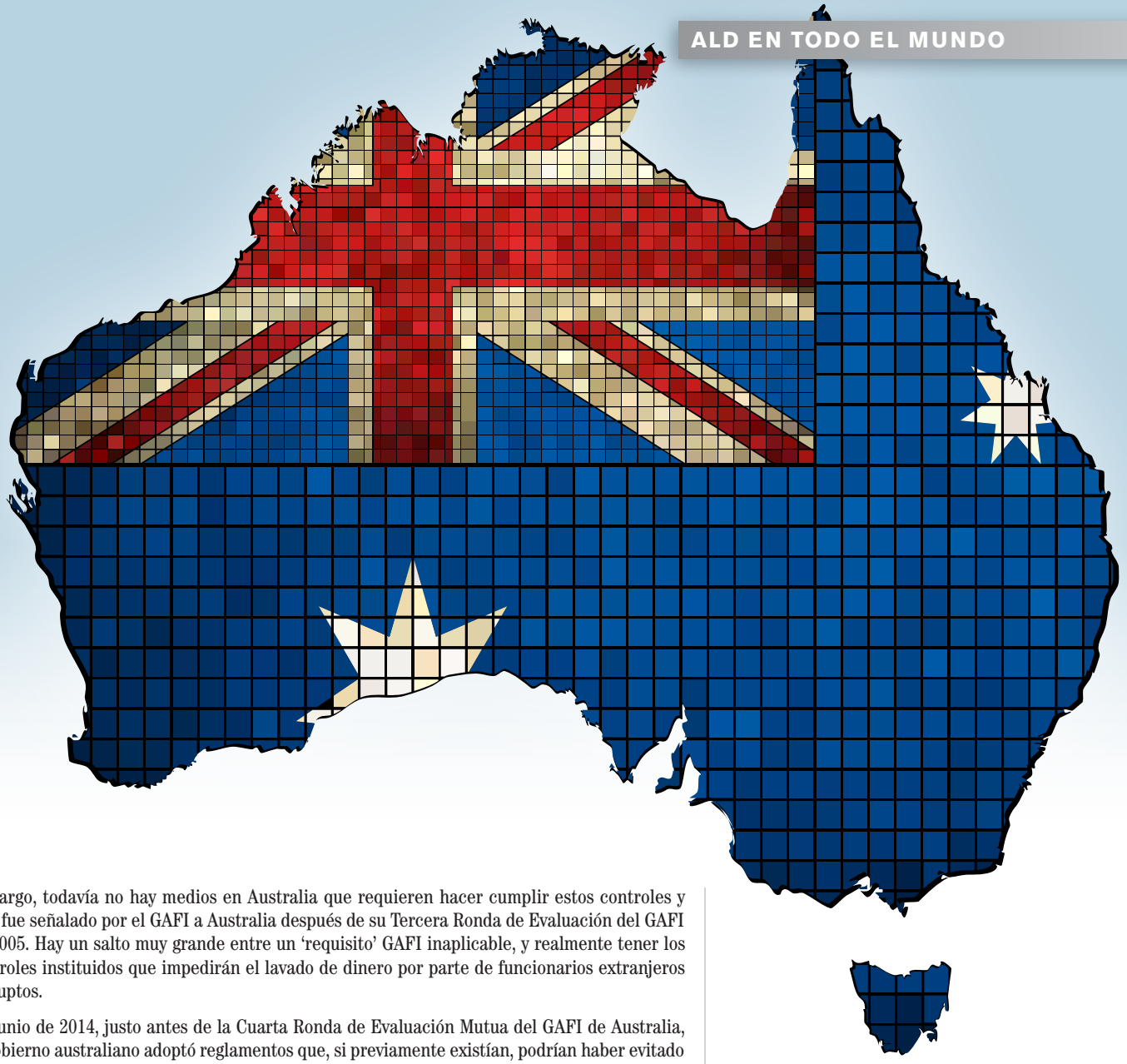
[4] Sam Koim, AUSTRAC Major Reporters Meeting, 4 de octubre del 2012, http://www.abc.net.au/4corners/documents/PNG2013/Speech_SamKoim.pdf

[5] Professor Jason Sharman, PNG Money Laundering, Today Tonight, 6 de agosto del 2013, https://www.youtube.com/watch?v=DMbJbm8boBk

[6] Marian Wilkinson and Lisa McGregor, "Preying on Paradise," *Four Corners*, 23 de septiembre del 2013, http://www.abc.net.au/4corners/stories/2013/09/23/3852506.htm

[7] AUSTRAC interview, *Four Corners*, 2013, http://abc.net.au/4corners/documents/PNG2013/AUSTRAC_statement.pdf

[8] AUSTRAC interview, *Four Corners*, 2013, http://abc.net.au/4corners/documents/PNG2013/AUSTRAC_statement.pdf



embargo, todavía no hay medios en Australia que requieren hacer cumplir estos controles y esto fue señalado por el GAFI a Australia después de su Tercera Ronda de Evaluación del GAFI en 2005. Hay un salto muy grande entre un 'requisito' GAFI inaplicable, y realmente tener los controles instituidos que impedirán el lavado de dinero por parte de funcionarios extranjeros corruptos.

En junio de 2014, justo antes de la Cuarta Ronda de Evaluación Mutua del GAFI de Australia, el gobierno australiano adoptó reglamentos que, si previamente existían, podrían haber evitado el lavado por funcionarios chinos corruptos y/o de PNG. Este reglamento aparecía como una modificación de las Reglas de ALD/CTF que exigen que los bancos identifiquen si un cliente o beneficiario real es una persona expuesta políticamente (PEP).[9] En un addendum inquietante, y, posiblemente, un indicador potencial del poder de los bancos en Australia, estas enmiendas no pueden aplicarse hasta enero de 2016.

Desafortunadamente, la falta de apoyo a la diligencia debida de las PEP se extiende a algunos sectores de la arena política australiana. Un senador australiano, en una investigación de 2014 sobre la delincuencia financiera, profesaba que estaba perturbado que las PEP podrían ser objeto de un análisis más profundo y que iba a trabajar para revertir estos requisitos en lugar de mejorarlos.[10]

¿De qué manera se presentan los esfuerzos de Australia?

A pesar de que se estima que AU$10 mil millones ($ 7,7 mil millones) al año se lavan a través del sistema financiero australiano,[11] y la conclusión de 2005 del GAFI fue que "el lavado de dinero visible se realiza predominantemente utilizando el sector financiero regulado", Australia no ha llevado a cabo el tipo de análisis o investigaciones que tienen el Reino Unido o los EE.UU. y que han marcado el progreso de sus regímenes de ALD/CTF.

El informe de 2011 del ex regulador financiero del Reino Unido, la Autoridad de Servicios Financieros (FSA), destacó los comportamientos de alto riesgo de los bancos británicos concluyendo que más de una cuarta parte de los bancos estaban "más que encantados" de ofrecer servicios a los polémicos políticos extranjeros sobre la base de

[9] Australian Government, "Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument 2015 (No.3), http://www.comlaw.gov.au/Details/F2014L00563/Explanatory%20Statement/Text

[10] Commonwealth of Australia, Proof Committee Hansard, Parliamentary Joint Committee on Law Enforcement–Financial Related Crime, 9 de septiembre del 2014, 43-45

[11] "Money Laundering," Australian Crime Commission, https://www.crimecommission.gov.au/publications/intelligence-products/crime-profile-fact-sheets/money-laundering

que las denuncias creíbles de corrupción aún no habían dado lugar a una condena penal.[12] Los reguladores estadounidenses también han llevado a cabo investigaciones sobre violaciones de sanciones de la banca, leyes y reglamentos que han resultado en multas a gran escala para los bancos que operan en los EE.UU.

La respuesta del gobierno australiano a las denuncias, parece estar colocando firmemente su fe en la voluntad de los bancos y otros negocios regulados para dejar de lado negocios rentables. Esa 'fe', dados los eventos en el Reino Unido y los EE.UU., parece potencialmente fuera de lugar. Es factible que un análisis de los bancos australianos podría proporcionar una prueba positiva de la inclinación de los bancos australianos por el riesgo cuando surgen tipos de situaciones a las que se enfrentan cuando se trata, por ejemplo, de fondos ilícitos provenientes de China o PNG.

Repatriación de activos

Australia quizás podría mantener que defiende su parte del acuerdo internacional de ALD si repatriara rutinariamente las ganancias del delito a los países de las que se tomaron. Por desgracia, el récord de Australia en este frente no es bueno. En total, Australia ha repatriado menos de AU$10 millones de las ganancias de la corrupción a todos los países en conjunto, sin repatriar dinero en los últimos cinco años.

Este récord, sin duda, refleja la opción oficial preferida de Australia para ayudar a las jurisdicciones extranjeras sólo cuando proporcionan una orden judicial.[13] Esta preferencia es contraria a las obligaciones del Plan de Acción Anticorrupción del G20 de Australia[14] haciendo caso omiso de la posibilidad de que el país víctima puede no ser consciente de que incluso ha perdido los fondos en cuestión. También deja de lado la posibilidad de que los organismos responsables de la obtención de tales órdenes judiciales de otros países pueden tener fondos insuficientes, y estar abrumados y obstaculizadas por la corrupción.

Hay cambios en marcha que pueden al menos reducir la facilidad con la que los funcionarios corruptos extranjeros podrían usar a Australia como un centro de lavado de dinero en el futuro. Sin embargo, Australia podría hacer más—al igual que el Reino Unido, los EE.UU. y un número de otros países—y adoptar medidas sin esperar a lo que es efectivamente una demanda por parte de las víctimas a que se devuelva lo que es suyo por derecho.

AUSTRAC

El nuevo CEO—¿El Eliot Ness de Australia?

Paul Jevtovic fue nombrado el nuevo CEO de AUSTRAC en octubre de 2014. Jevtovic tiene una carrera distinguida en la autoridad legal que abarca 33 años y él se une a AUSTRAC en un momento en que Australia aparece necesitar su "Eliot Ness", o por lo menos su "momento Lanny Breuer". Jevtovic bien puede encontrarse en conflicto directo con el sector bancario muy bien mantenido y políticamente poderoso de Australia, que nunca ha estado a punto de recibir sanciones significativas de ningún tipo en Australia.

Los poderes de AUSTRAC

Incluso sin las regulaciones de PEP 'relativamente recientes, pero, actualmente, impotentes', AUSTRAC cuenta con una amplia serie de poderes disponibles que podrían desplegarse para prevenir la continuación del lavado a gran escala, del tipo de China. Estos poderes incluyen la capacidad de obligar a la producción de información y respuestas a preguntas; la capacidad de ejercer una gama de sanciones civiles por infracciones tales como no llevar a cabo la debida diligencia en curso y no informar de cuestiones sospechosas;[15] y sanciones penales que van desde dos a 10 años de prisión y multas de hasta AU$1,7 millones ($1,3 millones).

Jevtovic, sin duda, estará trabajando duro para dar vida a la visión de AUSTRAC "para una comunidad australiana que es hostil al lavado de dinero, el financiamiento del terrorismo, la delincuencia grave y organizada" y su obligación de "adoptar medidas apropiadas y la aplicación de medidas".[16] Para este fin, es casi seguro que va a proseguir el primer enjuiciamiento de cualquiera de las aproximadamente 16.000[17] entidades que AUSTRAC regula—habiendo mostrado sus colores mediante la supervisión de la emisión de dos de los tres avisos de infracción alguna vez entregados en AUSTRAC en sus 25 años.

Nuevas leyes y reglamentos serán también concebiblemente requeridos para hacerles frente a las deficiencias en el régimen de ALD/CTF de Australia. Después de todo, mil millones de dólares de fondos ilícitos provenientes de China probablemente no llegaron al sistema financiero australiano sin que alguien en Australia le proporcionara ayuda, ya sea a través de una cuenta bancaria, el uso de una cuenta de fideicomiso en manos de un bufete de abogados o agente de bienes raíces, o por medio de cualquier otro mecanismo todavía por descubrir.

Uno de los retos que enfrenta Jevtovic, sin embargo, se revela en el comunicado de dirección estratégica del presupuesto de 2014-15 de AUSTRAC.[18] Además de dirigir la atención del AUSTRAC fuertemente a favor de la "función financiera de inteligencia" en lugar de "el papel regulador", AUSTRAC está obligado a:

- "Identificar oportunidades para reducir la carga regulatoria".

[12] Simon Bowers, "British banks ignore money laundering rules, says FSA," *The Guardian*, 22 de junio del 2011, http://www.theguardian.com/business/2011/jun/22/uk-banks-ignore-money-laundering-rules-says-fsa

[13] "2015-16 G20 Anti-Corruption Action Plan," Australia G20, https://g20.org/wp-content/uploads/2014/12/2015-16%20_g20_anti-corruption_action_plan_0.pdf

[14] "G20 Anti-Corruption Working Group Asset Recovery Guides," Australia 2014 G20, http://www.g20australia.org/g20_priorities_g20_2014_agenda/anti_corruption/g20_anti_corruption_working_group_asset_recovery

[15] AML/CTF Act 2006 sections 36, 43, 41 & 175-176.

[16] AUSTRAC Portfolio Budget Statements 2014-15, Australian Transaction Reports and Analysis Centre, https://www.ag.gov.au/Publications/Budgets/Budget2014-15/Documents/16%20PBS%202014-15%20AUSTRAC.PDF

[17] Ibid.

- "Limitar el flujo de la nueva regulación".
- "Consultar con las partes interesadas para reducir al mínimo los costos de cumplimiento y el impacto de los cambios regulatorios".

Las nuevas leyes no casan cómodamente con estos requisitos, pero, sin duda, el nuevo director general estará empujando al gobierno australiano a promulgar una legislación como la sugerida por el GAFI en 2006 y prometida en 2007,[19] cubriendo los agentes inmobiliarios y las profesiones jurídicas y contables.

Inteligencia financiera

La revisión de 2013 de la función de inteligencia de AUSTRAC de la Oficina Nacional de Auditoría de Australia (ANAO)[20] puede también plantear desafíos para Jevtovic. La ANAO luchó para medir la efectividad de la inteligencia que AUSTRAC está reuniendo.[21] Al igual que muchas UIF de todo el mundo, AUSTRAC se creó hace más de 20 años en un mundo antes de la conexión a Internet que Australia ahora disfruta y antes de que muchos de los métodos de transferencia de dinero en la actualidad populares fueran aún posibles. A pesar de esto, la amplitud de la recogida de información de AUSTRAC aparece arraigada en la era pre-Internet donde el "efectivo era el rey" y el dinero se transfería a través de las fronteras en bolsas o por medio de una transferencia telegráfica.

El futuro

Una fortalecida y ampliada recogida de información y programa de ejecución por AUSTRAC tropezará, por todos los cálculos, con resistencia de gran alcance. El sector bancario fuertemente retenido y altamente rentable de Australia ha tenido éxito en las negociaciones alrededor del ALD en el pasado y es probable que luche "con uñas y dientes" para evitar un cambio a gran escala. Para tener éxito, Jevtovic probablemente necesitará el apoyo internacional y un fuerte respaldo del gobierno australiano.

Un sistema robusto verá bancos australianos y otras entidades reguladas tanto asistidos como obligados a identificar correctamente los funcionarios extranjeros en sus registros, hacer esfuerzos razonables para identificar el origen de sus fondos y rechazar negocios cuando se descubre el hecho delictivo o no se puede descubrir su origen. Cualquier cosa menos, sin duda, significará que el sistema financiero australiano seguirá siendo un paraíso para los funcionarios corruptos de todo el mundo.

El proceso de investigación y la repatriación de mil millones de dólares en ganancias delictivas a China (con suerte seguida por la investigación y la repatriación de activos a otros países víctimas, tales como PNG) proporciona una visión de dónde y cómo el sistema de ALD australiano falló. Esperemos que las lecciones se hayan aprendido rápidamente y que las medidas correctivas se apliquen de manera expeditiva.

Un sistema robusto verá bancos australianos y otras entidades reguladas tanto asistidos como obligados a identificar correctamente los funcionarios extranjeros en sus registros

John Chevis, CAMS, BComm, MForAccy, ex miembro de la policía federal australiana y director de Contra$celus Pty Ltd, Orange, Nueva Gales del Sur, Australia, johnchevis@yahoo.com

Gill Donnelly, CPA, PI, CPCI, AIPIO, BComm, MAFraudInv, investigador principal, Just Integrity Solutions, Caloundra, Queensland, Australia, gdonnelly@justis.com

[18] Ibid.
[19] Second Tranche AML/CTF Legislation, AUSTRAC, http://www.austrac.gov.au/sites/default/files/documents/draft_scnd_trach_des_serv_tbls_archvd.pdf
[20] "AUSTRAC's Administration of its Financial Intelligence Function," Australian National Audit Office, http://www.anao.gov.au/Publications/Audit-Reports/2012-2013/AUSTRACs-Administration-of-its-Financial-Intelligence-Function/Audit-summary
[21] Según el informe: "Inteligencia financiera eficacia de AUSTRAC en términos de lucha contra el lavado de dinero y el financiamiento del terrorismo y otras formas de crimen organizado y serio no es fácilmente cuantificable".

Guía orientativa del GAFI para el sector bancario en la aplicación del enfoque basado en el riesgo: PARTE II

En octubre de 2014, el Grupo de Acción Financiera Internacional (GAFI) emitió una *Guia Orientativa para un Enfoque Basado en el Riesgo (RBA) para el Sector Bancario.* Esta guía se actualizó en 2007 para que estuviera en consonancia con las nuevas recomendaciones del GAFI. La guía está diseñada para el sector bancario, que incluye tanto las autoridades competentes, así como los bancos que supervisan (GAFI actualizará las versiones para otras industrias en el futuro). La guía fue elaborada por un grupo de miembros del GAFI y representantes del sector privado, que aportaron para el documento.

Este es el segundo de dos artículos que se ocupan de la guía, que se centra en la orientación para los bancos. El primer artículo aborda el concepto general RBA y la orientación proporcionada por los supervisores.

Como se ha señalado en el artículo anterior, la guía tiene cuatro propósitos principales:

1. Esquema de los principios implicados en la aplicación de un RBA para el antilavado de dinero (ALD)
2. Ayudar a los países, las autoridades competentes y los bancos en el diseño e implementación de un RBA proporcionando directrices generales y ejemplos de la práctica actual
3. Apoyar la implementación y supervisión efectiva de las medidas nacionales de ALD, centrándose en los riesgos y las medidas de mitigación
4. Apoyar el desarrollo de un entendimiento común de lo que implica el RBA

La guía reconoce que un RBA eficaz aprovechara y reflexionará sobre el enfoque jurídico y normativo de un país, la madurez y la diversidad de su sector bancario y su perfil de riesgo. Establece un marco de consideraciones para un RBA, pero no anula la competencia de las autoridades competentes y el marco normativo.

El enfoque basado en el riesgo en los bancos

Al igual que las evaluaciones de los riesgos nacionales discutidas en el artículo anterior, se espera que los bancos lleven a cabo las evaluaciones de riesgos para implementar los controles adecuados para prevenir y mitigar los riesgos de lavado de dinero. La evaluación de riesgos debe informar al banco de los riesgos, lo que le permite asignar sus recursos y organizar sus controles internos y el marco apropiado.

La Guía Orientativa para un Enfoque Basado en el RBA para el Sector Bancario identifica cuatro tipos específicos de servicios bancarios que implican claramente los diferentes riesgos que siguen:

1. La banca minorista, donde la oferta de productos como cuentas corrientes y de ahorros y préstamos directamente a los clientes individuales y comerciales, implica la prestación de servicios a empresas con efectivo intensivo, grandes volúmenes de transacciones, transacciones de alto valor y una amplia gama de servicios.
2. La banca corporativa y de inversión, que proporciona financiamiento corporativo, servicios bancarios y de inversión para corporaciones, gobiernos e instituciones, implica riesgos debido al gran volumen y alto valor de las transacciones y una amplia gama de servicios.
3. Servicios de inversión y gestión de patrimonios, que ofrecen servicios basados en el patrimonio del cliente, presenta riesgos de una cultura de confidencialidad, dificultad en identificar a los beneficiarios efectivos, el secreto bancario, la complejidad de los productos y servicios, clientes ricos y poderosos (incluidas las personas políticamente expuestas [PEP]), las transacciones de alto valor, las transacciones transfronterizas y la posibilidad de las fases de estratificación e integración de lavado de dinero (en las que generalmente resulta más difícil identificar el lavado de dinero).
4. La banca corresponsal, donde un banco (el banco corresponsal) proporciona servicios a otro banco (el demandado), presenta riesgos asociados con grandes volúmenes y valores altos de transacciones, a menudo con información limitada de los partidos y la fuente de los fondos involucrados en la transacción (por ejemplo, el beneficiario o remitente, dependiendo de la transacción).

La evaluación de riesgos

La evaluación de riesgos debe establecerse acorde con el tamaño y la complejidad del banco, teniendo en cuenta los servicios que presta. Por lo tanto, un banco que únicamente se dedica a la banca minorista puede utilizar una evaluación de riesgos más simple que uno que se dedica sólo a la gestión de patrimonios. Del mismo modo, si un banco se dedica a los cuatro tipos de banca, debe llevar a cabo un análisis más sofisticado de los riesgos. Otros factores por considerar en la evaluación incluyen información sobre los productos que se ofrecen, tales como:

- El mercado al que se dedica (target), incluida la clientela y sus ubicaciones y dónde hacen negocios los clientes;
- La naturaleza, escala y diversidad y complejidad de los productos ofrecidos, incluyendo los tipos de productos que ofrece y los lugares donde ofrece estos productos; y
- Los canales de distribución utilizados (por ejemplo, Internet, móviles, en persona) y el grado en que el banco cuenta con terceros, tales como introductores, para los clientes y la debida diligencia relacionada.

Además, el banco debe evaluar su exposición, tales como el número de clientes de alto riesgo, los volúmenes de actividad que realiza, la entrada de las propias líneas del banco de negocios y sus propias conclusiones de auditoría y de regulación.

Sin importar el nivel de sofisticación de la evaluación, debe estar debidamente documentado y revisado y aprobado por la alta dirección, mostrando que la administración es consciente de los riesgos y los controles establecidos para mitigar ese riesgo. Cuando los controles no son suficientes, deben mejorarse. En la práctica, esto implica un proceso de gestión para supervisar controles que permitan tomar medidas adecuadas cuando surjan preocupaciones.

La evaluación debe ser comunicada al personal pertinente del banco. Una vez que se complete la evaluación, es importante que el banco mantenga actualizada la evaluación, sobre una base periódica, pero especialmente cuando surgen cambios significativos en la evaluación anterior, tales como productos de importantes nuevos, mercados, clientes o cambios significativos en los volúmenes de actividad, clientes de alto riesgo o de auditoría/hallazgos de reguladores. La evaluación de riesgos no es un esfuerzo de una sola vez y que queda estática, sino más bien es la intención de reflejar la naturaleza dinámica del banco y de demostrar que el banco está gestionando activamente su riesgo.

La mitigación del riesgo

Una vez documentados y evaluados los riesgos, las políticas y los procedimientos adecuados por escrito deben ponerse en marcha para mitigarlos.

La diligencia debida del cliente (DDC)

Una de las funciones más importantes del ALD es la DDC, la etapa inicial, que permite a los bancos entender quiénes son sus clientes, qué tipo de negocio llevan a cabo y el tipo y nivel de actividad esperados de estos clientes. Esto permitirá a los bancos evaluar el riesgo global del cliente.

A través de este perfil de riesgo el banco puede determinar el nivel de vigilancia y diligencia debida que debe realizar para el cliente, así como la posibilidad de iniciar, o incluso continuar, una relación con el cliente. El perfil de riesgo se puede aplicar a los clientes individuales, así como a grupos, cuando los grupos son similares. La agrupación de clientes es particularmente útil en el contexto de la banca al por menor, en la que muchos clientes tienen niveles esperados de actividad

La evaluación de riesgos no es un esfuerzo de una sola vez y que queda estática, sino más bien es la intención de reflejar la naturaleza dinámica del banco y de demostrar que el banco está gestionando activamente su riesgo

similares; también es útil cuando se compara a los clientes con sus compañeros (por ejemplo, industria similar, geografía similar y transacciones esperadas similares).

La DDC inicial que se debe hacer para todos los clientes implica la identificación del cliente y, cuando el cliente es una persona jurídica, el beneficiario efectivo de los clientes, la verificación de la identidad del cliente utilizando medios fiables y comprendiendo el propósito y la naturaleza prevista de la relación comercial con el cliente. La guía no detalla mucho sobre lo que se entiende por medio fiable de verificación de la identidad del cliente, pero al igual que con otros aspectos del banco, se debe considerar la ubicación geográfica (algunos países no cuentan con bases de datos comparables sobre las personas que permitan la verificación como en los EE.UU.), los medios de apertura de la cuenta (la identificación fotográfica en un contexto de la banca en línea es menos útil que en un escenario de apertura de la cuenta hecha personalmente), los documentos utilizados (los documentos extranjeros pueden ser menos familiares para el personal del banco, y por lo tanto menos fiables), así como el uso de los proveedores (capaces de verificar los clientes que utilizan más medios que un banco).

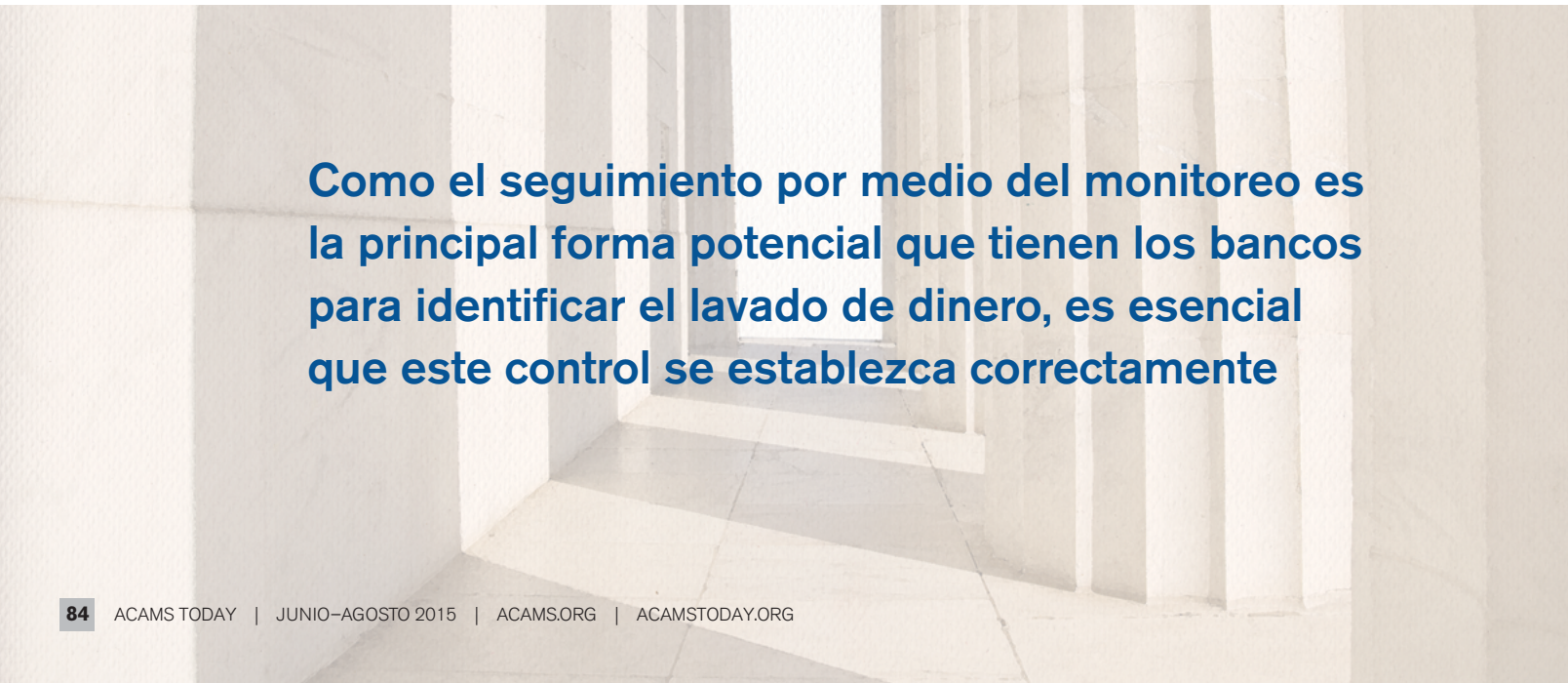
Esta información básica debe recogerse independientemente de los riesgos; el aspecto basado en el riesgo entra en juego, dependiendo de la cantidad de información adicional (como las fuentes más detalladas del patrimonio o los niveles esperados de actividad, en busca de noticias negativas o la realización de una investigación más detallada del cliente) o posterior verificación (tales como proporcionar documentación de apoyo para el origen del patrimonio o la realización de una verificación adicional de identidad) que se realiza a medida que aumenta el riesgo del cliente. Cuando el riesgo es bajo y simplificado de la debida diligencia, los estándares más bajos de la diligencia debida se pueden aplicar, como el aplazamiento de la verificación de la identidad del cliente, hasta un período razonable después de la apertura de cuentas o la realización de la verificación menos robusta (especialmente cuando se toma en cuenta la inclusión financiera, la prestación de servicios financieros a los tradicionalmente no bancarizados o sub-bancarizados, para los cuales los documentos normales de identificación pueden no estar disponibles). Sin importar el riesgo, los clientes deben estar sujetos a los requisitos de políticas y procedimientos adecuados; si un banco no puede cumplir con el DDC necesario para comprender adecuadamente el riesgo asociado con un cliente, no debe abrir la cuenta o, cuando exista, cerrarla.

Monitoreo y reporte de DDC en curso

El monitoreo permanente por lo general se refiere a dos procesos diferentes que se utilizan para evaluar si los clientes están participando en actividades potencialmente sospechosas incompatibles con su perfil de riesgo: uno que ve la actividad para constatar si es anómala y otra, que mira actualizar el perfil de riesgo del cliente y la información a medida que se producen cambios. Como el seguimiento por medio del monitoreo es la principal forma potencial que tienen los bancos para identificar el lavado de dinero, es esencial que este control se establezca correctamente. Ya sea en una base prescrita o continua, o cuando se produce un hecho desencadenante (como una nueva apertura de cuenta o que un cliente en contacto con el banco actualiza información), la información del cliente debe estar actualizada.

Del mismo modo, con revisiones de transacciones, los bancos deben establecer y mantener la vigilancia que realizan de los clientes para mitigar adecuadamente el riesgo. Esto implica generalmente los sistemas electrónicos, en particular cuando hay un volumen de transacciones. Sin embargo, sólo tener un sistema electrónico no es suficiente. El banco también tiene que entender lo que cubre el sistema automatizado, lo que no y si las áreas que no están cubiertas por el sistema son supervisadas adecuadamente por otros medios. Por otra parte, el banco debe confirmar periódicamente que el sistema de vigilancia está funcionando como se esperaba; esto puede implicar la evaluación de los parámetros utilizados para la activación de alertas (¿están generando demasiadas alertas de bajo valor?) y si el sistema sigue siendo eficaz en el tiempo (¿las alteraciones de código han afectado la forma en que el sistema de monitoreo identifica la actividad de codificación?).

Como con casi todo lo relacionado con el ALD, es fundamental que los resultados del monitoreo se documenten, si se trata de la actualización de la DDC en el sistema u observando cómo se resolvió una alerta de



Como el seguimiento por medio del monitoreo es la principal forma potencial que tienen los bancos para identificar el lavado de dinero, es esencial que este control se establezca correctamente

vigilancia a nivel de transacción correspondiente. Una de las cosas más importantes en la gestión del riesgo de ALD es crear un rastro de papel que permite (incluidos los auditores y reguladores) mirar hacia atrás y reconstruir lo que se hizo. Esto se aplica a cuestiones tan diversas como la forma en que la institución monitorea a alguien que deposita una maleta llena de dinero en efectivo a cómo se resuelve la investigación de esa actividad (incluyendo la orientación política y la consiguiente toma de decisiones para determinar si el depósito se considera normal para el cliente y por qué o si se presentó un reporte de operaciones sospechosas [ROS]).

Para ayudar a facilitar la retención de los registros relacionados con las alertas y las investigaciones, un sistema de gestión de casos que ayudará en la identificación, documentación y presentación última de los resultados, es muy útil. Si bien la determinación de lo que se considera sospechoso se basa en el riesgo en última instancia, una vez que la actividad se considera sospechosa debe ser reportada de inmediato a las autoridades correspondientes.

Gobernanza

Un fuerte liderazgo de la alta dirección y su participación son claves para la implementación exitosa de un programa de ALD. La administración puede tomar una serie de medidas para garantizar esto, a través de:

- Promover el cumplimiento como un valor fundamental
- Establecer, sobre todo, políticas claras y fuertes controles
- Mensaje claro de que las relaciones con clientes no deben mantenerse cuando los procedimientos de ALD no pueden seguirse
- Proporcionar recursos adecuados a la función de ALD
- Determinar el apetito de riesgo de la entidad con respecto a la cantidad de riesgo residual que se tolerará
- Establecimiento de funciones y responsabilidades claras y, en particular, proporcionar la autoridad y el apoyo necesarios para el funcionario responsable del programa de ALD del banco

Para comprender y mitigar el riesgo existente de ALD, la dirección debería asegurarse de que obtiene la información adecuada sobre el programa de ALD. La información debe compartirse regularmente con la alta dirección y debe involucrar la comunicación entre el oficial de ALD y la junta directiva, así como otras áreas del banco, tales como el departamento de tecnología y las diferentes líneas de negocio, según corresponda. Este nivel de información debería incluir información acerca de que el ALD en general presenta riesgos, riesgos específicos que pueden surgir, así como los riesgos emergentes en el horizonte y la eficacia general de los controles de ALD de la institución.

En consonancia con su responsabilidad de garantizar los recursos adecuados para su programa de ALD, el banco debe contar con personal debidamente calificado que pueda cumplir con sus responsabilidades, sobre todo en términos de la implementación de controles de ALD. Para ayudar a lograrlo, debe llevarse a cabo una investigación de antecedentes basada en el riesgo del personal. Para ayudar a minimizar los conflictos de intereses, la remuneración para el personal de cumplimiento de ALD debe reflejar una adecuada independencia de la empresa, como que el Comité de Supervisión Bancaria de Basilea (BCBS) señaló en su guía de 2005, sobre el *Cumplimiento y la Función de Cumplimiento en Bancos*.[1] Esta guía detalla cuatro elementos que permiten al banco tener una adecuada gestión de riesgo independiente en toda la cartera:

- El cumplimiento debe tener un estatus formal dentro del banco
- Debe haber un oficial de cumplimiento de grupo con la responsabilidad general de la coordinación de la gestión del riesgo de cumplimiento del banco
- El personal de cumplimiento no debe colocarse en una posición donde hay un posible conflicto de intereses entre sus responsabilidades de cumplimiento y cualquier otra responsabilidad que pueda tener
- El personal de la función de cumplimiento debe tener acceso a la información y el personal necesario para llevar a cabo sus responsabilidades

Formación y sensibilización

El personal del banco debe ser consciente de sus obligaciones de ALD en forma permanente; una sesión de entrenamiento individual en el momento de la contratación no será suficiente. Para mitigar los riesgos del ALD, la formación debe adaptarse a ser relevante para los riesgos de ALD de la base de clientes y de presencia geográfica actual del banco, y estar al día con las últimas obligaciones legales y reglamentarias y los controles internos. Por esta razón, la formación corriente por sí sola puede no ser suficiente, sino que puede necesitar ser complementada con información y formación específica. La formación debe ser obligatoria para todo el personal pertinente. Mientras que algunos miembros del personal de custodia pueden no necesitar saber cómo llevar a cabo la DDC, otros empleados tendrán algunas obligaciones de ALD y la formación debe adaptarse para ellos. El personal que se centra en la banca minorista, banca corresponsal, financiamiento para el comercio o la transformación de efectivo serán todos muy diferentes frente a los riesgos y tareas; se debe estar previsto formar a los que se ocupan de estas diferencias para que puedan desempeñar sus funciones en el programa de ALD. Estos esfuerzos de formación básica pueden reforzarse por el medio adicional de crear conciencia sobre los riesgos del ALD, tales como reuniones de equipo, ejercicios de entrenamiento que duran una sola vez, el intercambio de estudios de casos, comunicaciones por correo electrónico u otras comunicaciones internas. Esta disposición reiterada de información a los empleados ayudará a reforzar el mensaje de que el cumplimiento del ALD es responsabilidad de todos.

Por supuesto, el entrenamiento debe reflejar el equilibrio adecuado entre los costos para desarrollar esta formación y el tiempo para

[1] Basel Committee on Banking Supervision, *Compliance and the Compliance Function in Banks,* abril de 2005, http://www.bis.org/publ/bcbs113.pdf

En última instancia, la capacitación debe cumplir una cultura arraigada en la que el cumplimiento existe entre los empleados a medida que realizan su trabajo

tomarlo (especialmente teniendo en cuenta los costos involucrados en la formación para grupos grandes o por medio de múltiples canales). La efectividad del entrenamiento se puede evaluar al exigirles a los empleados pasar pruebas que demuestren los conocimientos necesarios. Los empleados deben confirmar que han tomado la prueba por su cuenta, sin ayuda exterior, para no frustrar el propósito de la prueba. Cuando los empleados no pueden pasar la prueba, incluso después de múltiples oportunidades, el entrenamiento de recuperación se debe considerar para asegurar que el empleado tiene los conocimientos adecuados para desempeñar con éxito sus responsabilidades de ALD. Esta educación de recuperación también puede ser útil cuando se encuentra que los empleados han violado inadvertidamente la política de la empresa (las violaciones intencionales no son susceptibles de ser abordados por la formación). En última instancia, la capacitación debe cumplir una cultura arraigada en la que el cumplimiento existe entre los empleados a medida que realizan su trabajo.

Evaluación de los controles

Uno de los controles internos más importantes es la evaluación de los otros controles (por ejemplo, la DDC, vigilancia, gobernanza). Dada la cantidad de recursos dedicados al programa de ALD, la administración debe evaluar si el programa de ALD está funcionando según lo previsto. Por otra parte, el oficial del ALD, a menudo personalmente responsable de supervisar el cumplimiento del día a día dentro de la organización, debe sentir que el banco está haciendo lo que debe, por lo que él/ella puede dormir de noche (y no encarcelado, ya que muchas jurisdicciones hacen al oficial de ALD personalmente responsable del éxito—o fallas—del programa de ALD). El oficial del ALD y/o su personal deben ser lo suficientemente independientes de las líneas de negocio y tener la autoridad correspondiente, recursos y experiencia para llevar a cabo esta evaluación. Como se señaló anteriormente, la independencia es fundamental, ya que la administración debe ser capaz de obtener una evaluación honesta e imparcial de los resultados de los controles de ALD, aunque—o quizá especialmente si—el negocio no se está haciendo tan bien como debería y necesitan hacerse mejoras.

Además, la mayoría de leyes requieren una evaluación independiente, o de auditoría, de los controles de ALD. Esta es una verificación adicional en el rendimiento del programa de ALD. Ciertamente, el oficial del ALD tiene un interés personal en demostrar la eficacia del programa que él/ella supervisa, por lo que la función de auditoría tiene la intención de servir como un tercero independiente que pueda evaluar la eficacia del programa.

Tanto el control del cumplimiento como la auditoría independiente tienen un papel clave que desempeñar, teniendo en cuenta toda la información disponible, incluida la información obtenida de forma confidencial (por ejemplo, a partir de la denuncia de irregularidades por líneas directas o mecanismos de referencia interna) para permitir una evaluación independiente y honesta de la eficacia del programa. Las funciones de auditoría y cumplimiento deben tanto reportar sus hallazgos como escalar sus preocupaciones a la administración, según el caso. Mientras que un RBA es muy informativo, centrándose únicamente en los riesgos más altos no puede proporcionar el nivel adecuado de información sobre el programa en general; por lo tanto, las zonas de riesgo estándar deben ser evaluadas, así como asegurar que la mayoría de los negocios del banco se controlan adecuadamente.

Conclusión

Dado su papel esencial y único en el manejo de la transferencia de valor a través del sistema financiero mundial, los bancos juegan un papel crítico en la disuasión y prevención del lavado de dinero. El RBA es especialmente importante para los bancos, ya que cuentan con recursos limitados para aplicar a su amplia base de clientes. Este documento de GAFI es extremadamente útil porque ayuda a proporcionar información a los bancos sobre cómo deben abordarse los riesgos de lavado de dinero que pueden estar presentes en sus instituciones. También es informativo para los reguladores, ya que necesitan entender cómo se espera que los bancos que supervisan despliegan sus recursos limitados para hacer frente a estos riesgos. Como señaló el GAFI, el RBA no es un enfoque de tolerancia cero; dentro del RBA previsto por el GAFI, habrá casos en los que se producirá el lavado de dinero o financiamiento del terrorismo. El RBA enfatiza la mitigación efectiva; no significa la eliminación total del riesgo.

El documento del GAFI debe ayudar a continuar el diálogo entre los reguladores y las instituciones que regulan. Ambos están tratando de estirar los limitados recursos disponibles en la medida de lo posible para reducir el riesgo del ALD, aunque desde perspectivas ligeramente diferentes. Los reguladores tienen que entender que los bancos no pueden eliminar el lavado de dinero y los bancos tienen que entender que los reguladores están presionando a los bancos para que sean más eficaces. El debate en curso entre los dos puede llegar a ser vivo a veces (como la naturaleza y la relativa amenaza de riesgo es eminentemente discutible), pero en última instancia ambas partes deben ser capaces de encontrar un terreno común en relación con su interés mutuo en la lucha contra el lavado de dinero y la actividad delictiva subyacente que los fondos lavados representan.

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

CAMS | Risk Assessment®

SURE, UNDERSTAND & EXPLAIN
R MONEY LAUNDERING RISKS

lp your institution:

Effectively detect financial crime patterns and spot red flags

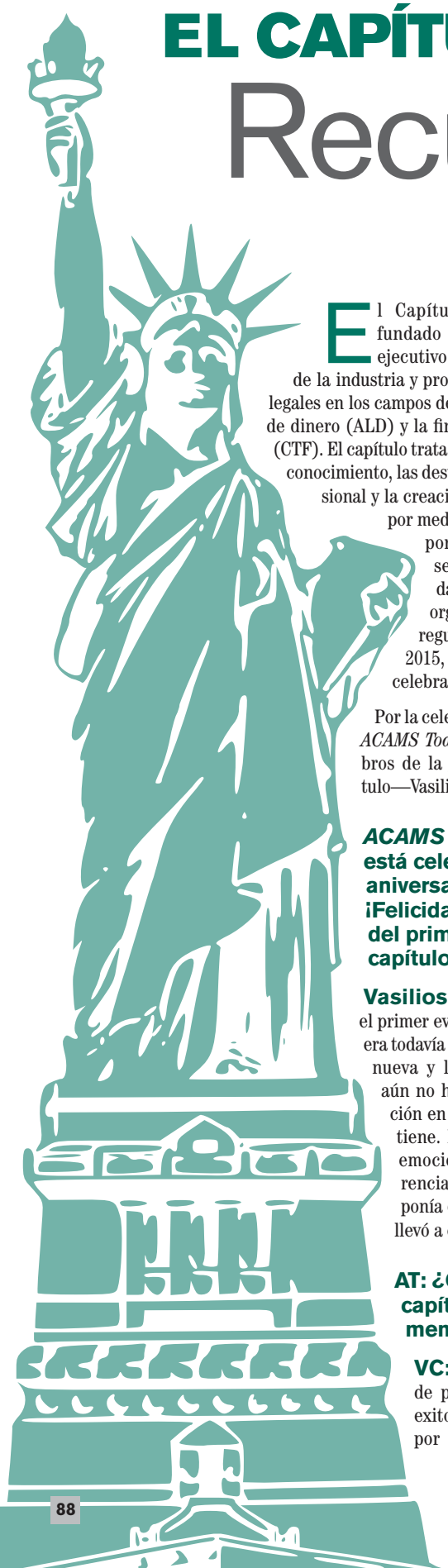
Mitigate risk and regulatory scrutiny by filling in the gaps in your detection and prevention controls

Save time and expense with comprehensive automation and updates

Clearly communicate risk through standardized scoring and automated reporting

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

EL CAPÍTULO DE NUEVA YORK: Recuerdos e hitos



El Capítulo de Nueva York fue fundado en 2005 por un comité ejecutivo compuesto por expertos de la industria y profesionales de autoridades legales en los campos de la lucha en el antilavado de dinero (ALD) y la financiación del terrorismo (CTF). El capítulo trata de promover el avance del conocimiento, las destrezas, el desarrollo profesional y la creación de redes profesionales por medio de eventos presentados por los profesionales en el sector privado, las autoridades de control legal y los organismos de supervisión y regulación. El 30 de junio del 2015, el Capítulo de Nueva York celebrará su 10º aniversario.

Por la celebración de su aniversario, *ACAMS Today* habló con dos miembros de la junta directiva del capítulo—Vasilios Chrisos y Meryl Lutsky.

ACAMS Today: Su capítulo está celebrando su 10º aniversario en junio—¡Felicidades! ¿Se recuerda del primer evento del capítulo?

Vasilios Chrisos: Sí recuerdo el primer evento del capítulo. ACAMS era todavía una organización bastante nueva y la designación de CAMS aún no había alcanzado la distinción en todo el mundo que ahora tiene. Dicho esto, había mucha emoción en la sala de conferencias en U.S. Trust, donde se ponía en marcha el capítulo y se llevó a cabo el primer evento.

AT: ¿Qué evento del capítulo fue el más memorable y por qué?

VC: Hemos tenido la suerte de producir muchos eventos exitosos en los últimos años, por lo que resaltar uno solo sería imposible. Si se me permite, me gustaría centrarme en unos pocos. En junio de 2011, nos convertimos en el primer capítulo en ofrecer un seminario de un día completo. Fue un evento fantástico que atrajo a casi 200 asistentes e incluyó oradores de primer nivel de los sectores público y privado.

También fuimos el primer capítulo en celebrar un evento de aprendizaje para crear conciencia sobre la cuestión de la trata/tráfico de personas. Este evento se llevó a cabo en 2009 y atrajo a más de 200 personas. También fuimos el primer capítulo en celebrar un evento de aprendizaje sobre bitcoin y los riesgos de la moneda virtual. Este evento atrajo a más de 300 asistentes.

Más allá de los eventos de aprendizaje, hemos sido el único capítulo en acoger ferias de trabajo y grupos de estudio del examen CAMS. Las ideas para estos vinieron directamente de nuestra membresía y, en mi opinión, dice mucho de cómo el Capítulo de Nueva York se mantiene relevante.

AT: ¿Qué tan exitoso ha sido su capítulo en alcanzar su misión de promover los conocimientos, las habilidades y la experiencia de los profesionales en el campo de antilavado dinero (ALD)?

VC: Creo que tomando en cuenta todos los aspectos, hemos sido el capítulo más exitoso en la red de ACAMS. No somos sólo el capítulo más antiguo, sino también somos el mayor, con más de 500 miembros activos.

La mayor razón por la cual el capítulo ha tenido tanto éxito ha sido que hemos proporcionado a nuestros socios programación de vanguardia que se mantiene actualizada con los tiempos e intereses rápidamente cambiantes de la capital financiera del mundo, que es la ciudad de Nueva York. Continuamente desafiamos a los miembros de la junta directiva a llegar a temas nuevos y relevantes sobre la base de nuestra comprensión colectiva del pulso de la industria.

Otra gran razón para el éxito sostenido de nuestro capítulo es nuestra legión de miembros. Estos son los profesionales de ALD dedicados y apasionados que han demostrado un deseo de avanzar en su conocimiento y crear redes de contactos en la industria.

Por último, siempre hemos promovido una cultura inclusiva dentro del Capítulo de Nueva York. La junta directiva ha invertido tiempo en conocer a los socios y también hace tiempo para hablar con todos durante los eventos. Además, la junta del Capítulo de Nueva York siempre ha estado abierta a las nuevas ideas o sugerencias. De hecho, los socios del capítulo en un par de ocasiones han asumido el liderazgo en la producción de eventos de aprendizaje. Esto ha incluido

ACAMS®

NEW YORK CHAPTER

Vasilios Chrisos

Meryl Lutsky

el desarrollo del tema y asegurando a los oradores. Algunos de nuestros socios con el tiempo se han convertido en miembros de la junta después de organizar y llevar a cabo con éxito eventos de aprendizaje.

AT: El Capítulo de Nueva York fue fundado tanto por autoridades de control legal como por profesionales de ALD, ¿por qué son las asociaciones entre los sectores público y privado importantes y cómo ha enriquecido el capítulo esta asociación?

Meryl Lutsky: La importancia de la colaboración público-privada no puede exagerarse. Los fundadores del Capítulo de Nueva York entendieron que en esta era de las nuevas tecnologías y paisajes geopolíticos siempre cambiantes, era imprescindible para las autoridades de control legal y los profesionales financieros tener un foro en el que pudieran reunirse de forma habitual para compartir información. Esto sigue siendo un objetivo principal del capítulo. Los eventos para establecer redes y contactos y de aprendizaje siguen proporcionando información valiosa para ambas partes—la comunidad de ALD gana percepción de las nuevas tendencias delictivas observadas por la policía y las autoridades de control legal se enteran de nuevos productos y métodos de transferir dinero. La capacidad de la comunidad del ALD para reaccionar rápidamente a las nuevas tendencias a través de ideas y asociaciones fomentadas en los eventos de capítulos beneficia a todos los interesados.

AT: ¿Qué consejo le daría a los nuevos capítulos o miembros que deseen iniciar un capítulo en su región?

VC: Sin duda los animaría a hacerlo. Un capítulo local puede dar a un socio de ACAMS acceso a una red de personas de ideas afines y proporciona foros donde los profesionales pueden mezclarse con los colegas, intercambiar ideas y mantenerse al tanto de las tendencias de la industria, de temas de actualidad y de las posibles soluciones que se pueden aplicar en su lugar de trabajo. Ser capaz de recurrir a una red de contactos locales que pueden compartir información, servir como cajas de resonancia y/o ayudar en la resolución de problemas puede ser invaluable.

AT: Como miembro de la junta de su capítulo, ¿qué le gustaría contribuir para ayudar a mantener el éxito del Capítulo de Nueva York?

VC: A nivel personal, mi participación en el Capítulo de Nueva York ha sido muy beneficiosa para mi carrera. El conocimiento adquirido y las relaciones que he sido capaz de forjar han sido realmente muy valiosos y ha contribuido a mi desarrollo como profesional de delitos de cumplimiento financiero. Espero pasar esta pasión a los demás para que podamos continuar la gran obra del Capítulo de Nueva York.

AT: ¿Qué le depara el futuro al Capítulo de Nueva York?

ML: El futuro es brillante para el Capítulo de Nueva York. Vamos a seguir trabajando con ACAMS y nuestra membresía diversa para garantizar una programación oportuna y pertinente. Nuestros eventos de contacto y extensión de redes continuarán para fomentar las relaciones entre las autoridades de control legal y la comunidad financiera para que todos podamos proteger mejor nuestro sistema financiero. Nuestras ferias de empleo proporcionarán un foro para que los empleadores busquen los candidatos más calificados para puestos de ALD. Además, vamos a seguir creando un ambiente donde los profesionales de ALD saben que pueden venir y hacer preguntas y encontrar respuestas a los acuciantes temas del día.

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

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

Graduados de la Certificación Avanzada

BONAIRE

Rudolf Gomez, CAMS-Audit

CANADÁ

Jochen Best, CAMS-Audit

Chris Galloway, CAMS-FCI

Henry Pleau, CAMS-FCI

ESTADOS UNIDOS

Edwin (Ed) Beemer, CAMS-FCI

Mary Christine Bray, CAMS-FCI

Lindsay Dastrup, CAMS-Audit

Sam Adam Elnagdy, CAMS-FCI

Claudia Gonzalez, CAMS-Audit

Ralph Guillou, CAMS-Audit

Deborah Hitzeroth, CAMS-FCI

Jonathan Kay, CAMS-Audit

Marion Keyes, CAMS-Audit

Nancy Lake, CAMS-FCI

Christopher Luangpakdy, CAMS-Audit

Umberto Lucchetti Junior, CAMS-FCI

David Thomas Martin Morris, CAMS-Audit

John McCormick, CAMS-Audit

Sean McCrossan, CAMS-FCI

Louis Napolitano, CAMS-Audit

Alexandra Rosi, CAMS-Audit

Michael Schidlow, CAMS-Audit

Jason Smith, CAMS-Audit

Iris Smith, CAMS-Audit

Joseph Weber, CAMS-Audit

LÍBANO

Rashid Assaad El Takash, CAMS-FCI

ZAMBIA

Katuna Sinyangwe, CAMS-Audit

Graduados de CAMS: Febrero-Abril

ALEMANIA
Amer Bektesevic
Naweed Khan
Nikolai Kohl
Holger Mies
Carla Pohle
Martin Schaub

ANTIGUA Y BARBUDA
Shaina Armstrong
Keri Matthew

ARABIA SAUDITA
Malek M. Al-Kawas
Dayana Al-Qaissi
Altaf Dossa
Amr Shams

ARGENTINA
Gustavo Juana
Walter Szcerb

ARUBA
Julienne Koolman

AUSTRALIA
Timothy Allen
Carol Daly
Rajesh Dhanekula
Victoria Eccleston
Jason Mills
Christopher Mojak
Michael Newbury
John Odria
Kylie Oliver
Simon Phinn
Dhruv Sabharwal
Nadia Teano

BAHREIN
Jinu Scaria
Aoun Sharaf

BARBADOS
Lisa Greaves

BÉLGICA
Peter Andries
Jorge Campo Serrano
Simon Muir

BERMUDA
Michelle Cardwell
Carmen Lindo

BRASIL
Rezivalda Borges
Ana Leite
Jacqueline Leoni

BULGARIA
Bozhidara Borisova

CANADÁ
Debbie Adjey Simone
Ross Alderson
Ivica Anastasov
Steven Beeksma
Elefteria Lea Belegris
Kenneth Bell
Richard Blissett
Samara Bolduc
William Boyd
Darren Boyer
John Bressette
Andrew Brintnell
Esther Chen
Sarika Chhabra
Marylynn Cook
Jennifer Davidson
Ryan Dmytruk
Cameron Dodson
Roman D'Souza
Munther Elkhaldi
Jesse Espedido
Matthew Fadden
Alberto Favila
Kris Gade
Sucheta Gandhi
Bruno Gatto
Chantal Gauthier
Attal Golzay
Danielle Guglielmucci
Amy Guillemin
Rachel Han
Michael Hiller
Andreas Hofmann
Andrew Hughes
See Mok Kim
Ana Lakovic
Vincent Lemoine
Gregor Lerche
Wing-Chi Leung
Denise Li
Xiqiao Liu
Yan Jun Liu
Margaret Lung
Ashley Macmillan
Sebastien Mandeville
Donald Merkel
Kaylan Olsen
Matthew Petretti
Tony Presutti
Lida Preyma
John Ramsay
Chris Randle
Courtney Robinson
Bradley Rudnicki
Deepak Saini
Aswath Shanmugathas
Archana Shukla
Guillermo Soto Martinez
Sam Stephens
Robert Stratford
Aleem Syed
Farhana Tabassum
Alana Takaki
Samantha Trope
Sharod Tucker
Khursheed Umer
Binod Upadhaya

Abhilash Viswanath
Ella Walders
Emily Wu
Ahmed Zafeer

CHINA
Grace Gao
Yaping Song
Yunfang Wang
Chen Ye
Xiao Zeng
Linna Zhao
Tao Zhu

CHIPRE
Nassos Paltayian
George Pelaghias
Stefanie Zagelow

COSTA RICA
Eddy Lizano Varela

CURAÇAO
Heidi Getrouw
Dinotra Pietersz-Coffie
Revonella Raphaela
Eugene Rhuggenaath
Anthony Rozendal

ECUADOR
Jaime Mancheno Vasquez

EL SALVADOR
Fabricio Monroy
Rosa Elena Rodríguez
Mirian Isabel Vides Guardado

EMIRATOS ÁRABES UNIDOS
Saleem Abbas Dodhiya
Pandey Avyaya
Pranav Baddukuli
Erwin Luis Damian
Kashish Hotchandani
Sreeja Jaideep
Harold Koster
Thomas Landgraf
Gagan Malik
Daryl Moraes
Muhammad Mushtaq
Muhammad Arif Pervaiz
Sridhar Ragunathan
Astha Talreja
Paritosh Tripathi
Ashar Zamin

ESPAÑA
Margarita G. de la P. Campo

ESTADOS UNIDOS
Katherine A. Skipsey
Kimberly Abbott
Lauren Agovino
Syed Ahmed
Lukman Ahmed
Brendan Akos
Mohsin Ali
Ana Amaral
Shelleen Anacay
Brenda Andriani
Andrei Anikin
James Ansberry
Daniel Antenor Jr.
Duwight Armstrong
Arda Arslanian
Omer Aslam
Gyanendra Asre
Judith Auten
Cecilia Ayala Seminara
Andrew Azzi
Steve Babinec
James Bachman
Michael Baird
Vazoumana Bamba
Lori Bannister
Faith Barare
Crystal Barela
Wendy Barnett
Catherine Bartucci
Alexander Bassitt
David Batchelder
Tiffany Bazinet
Annette Beaumont
Todd Beck
Sarah Becker
Baba Gurjeet Bedi
Joanne Belmont
Luke Berte
Christopher Beswick
Gregory Betchkal
Elizabeth Bethoney
Steve Bohner
Andrew Bonslater
Anita Borawska
Sari Borgen
Gregg Bowen
Matthew Bracken
Patrick Britton
Benjamin Brockman
Ann Broeker
David Brown
Ann Bullard
Sonya Burnett
Sylvia Bustamante Diaz
Jennifer Butkus
Audrey Bynoe
Jed Cabangon
Patricia Cabrera
Mark Cadiz
David Cagno
Leigh Caldwell
Elizabeth Caldwell
Colleen Callahan
Nicholas Campbell
Juan Carlos Canido
Michelle Carrasco
Lindsay Carroll
Janet Carter
Drew Cartwright
Sarah (Sally) Casey
Fred Casissa
Michael Cassino
Calvin Chang
Shelley Chang
Jason Chapman
Lori Chapman
Stephanie Chen
Chien Chen
Jane Huy Chheng
Mark Choi
Harrison Choi
Cory Christensen
Sandra Christiano
Sumeet Chugani
Ashley Ciavarella
Abdoul Cisse
Christian Claffy
Thomas Clautice
Kim Clinton
Deana Collins
Kevin Comerford
Danielle Connelly
Rosa Maria Corral
Andrew Cosby
Pedro Costa
Matt Craker
Katherine Crane
Melissa Cromer
Ese Crossett
Alexander Csik
Michael D. Patti
Alexander Daddario
Kyle Daddio
Amanda Dahms
Mike Dang
Edward Davis
Kevin Davis
Kerry Ann Davis-Whittingham
Terence Dawson
Alvis Day
Brendan De Grim
Nicole De La Roca
Zsuzsana Degia
Matthew D'Emic
Nicholas DeMonte
Darya Dergacheva
Daniele Dermesropian
John P. (Jack) Dever
Pedro Diaz
Lisa Dibona
Andrew DiMattina
Matthew DiTullio
Stefanie Dohman
Nathan Donahue
Qiao Dong
Leslie Dotson
Nailya Dovletova
Nora Doyle
MonaLisa Drake
Travis Dreibelbis
Ronald Dufour
Kevin Dunleavy
Latishia Easley Burr
Victoria Edison
Nana Edusah
Kevin Eick
Mina Ekladous
Erin Ekwall
Jason Eldredge
Jeremiah Ellisor
Robert Ellman
Scott Emerson
Joseph Enge
Joseph Englert
Bryan Erwin
Brittanie Eslick
Joseph Evans
Christa Far
Andre Fatovic
Salvatore Femia
Michele Fenning
Nicole Ferguson
Michelle Ferguson
Shlesin Fernandez
William Ferris
Andrew Findlay
Patrick Finley
Faranak Firozan
Karen Fischer
Jessica Fletchinger
Mark Ford
Marcy Forman
Matthew Foss
Charles Fox
Joel Frederique
Kristina Freese
William Freytag
Jennifer Friesz
Olivia Fung
Osman Gabeire
Peter Gandy
Lorraine Ganguzza
Adele Gantt
Ade Garcia
Rosslyn Garcia
Robin Garrison
Kimberly Garza
Michael Gaspar
Julie Gassler
Cornelia Gatz
Gilbert Gavia
Nicholas Gazzola
David Gefell
Andre Gelinas
Tiffany Nevine Georggi
Haik Gevorgyan
Erin Giannelli
Gagandeep Gill
Kevin Giza
Suzanna Gluck
Sandra Gobin
Bernard Goodman
Tina Granger
Daniel Greco
Hugo Grimbel du Bois
Judy Guerin
Fernando Guerra
Angelo Guglielmo
Brad Gunther
Mengting Guo
Shavata Gupta
Saurabh Kumar Gupta
Michael Hagan
Shelly Hallmark
Lauren Hanat
Jennifer Handzel
Dana Hansen
Jillian Harrigan
Thomas Harrington
Jacob Harris
Felix Haydar
Karen Haydock
Erica Hayes
Shelia Hedrick
Edgar Hernandez
Eric A. Hertrich
Christopher Hewitt
Laura Hidalgo
Brian Higdon
Edward Hildebrand
Kyle Hingher
Matthew Hinman
Yash Hiranandani
Samira Hitti
Sam Hoffman Vander Hoek
Leonard Hom
William Hook
Chiranda Hunter
Arianna Iapicca
Naoki Iida
Michael Ippolito
Valerie James
Catul Jean
Krystal Jenkins
Winnie Jiayi Wu
Arthur John
Rodney Johnson
Luke Johnson
Darrin Johnson
Roy Jones
Robert Jones
Martin Jones
Lori Joseph
Bhakti Joshi
Soo Ji Jung
Robert Kakareka
Matthew Kandl
Klayton Kaspar
Steven Katz
Jasmin Kaur
Jacqueline Kay
Crystal Kazemfar
Josh Kellam
Janis Kelley
Keith Kelley
Jeffrey Kelly
Ashley Kenny
Jeff Ketelhut
Mcaaron Ketor-Tay
Jack Kettler
Aadil Khan
Namwoo Kim
Joshua Kinzel
Eric Kinzel
Timothy Kissling
Brittany Klein
Alan Klipper
Jacqueline Knowles
Kalem Kopf
Christopher Kraj
Sarah Krenz
Laura Krueger
James Kudiza
Andrea-Lea Landano
Mariela Landazuri
Richard Lani
Camden Lapasky
David Larocque
Susan Lechko
Kristen Leidy
Yaima Leon
Kelly Lessard
Victor Lessoff
Rachel Levin
Ella Li
Sandra Lira
Hsiu-Hsiu Liu
Polleyanna Lo
Angela Lo
Virginia Lombard
Kelly Lopez-Clark
Tatiane Loung
Alexandre Loupy
Jin Lu
Terry Luby
Gloria Maria Lugo
Dariusz Luka
Scot Luther
Michael Lyudmir
Richard Macchio
Kevin Madden
Chris Madsen
Geetika Mahajan
Elliott Major
Yvonne Mak

Abhishek Malkampate
Marcus Maltempo
Yervant Manavian
Zachary Manes
Ken Mangaroo
Thomas Manillo
Joy Manning
Pasi Mantyla
Matthew Margolis
Daniel Markowski
David Marquez
Miguel Martinez
Jonathan Mason
Premi Mathai
Michelle Mathena
Roger Matthews
Cris Mattoon
Kevin McCormick
Peder McDermott Johansen
John McDonald
Alan McDougall
Todd McElduff
Daniel McGarrigle
Stephen Mcloughlin
Kenyada Meadows
Erin Meconnahey
Adriano Medina
Jason Medina
Stella Mendes
Leizl Mendiola
Carolina Mendoza
Katherine Meredith
Eileen Miclette
Leah Middendorp
Kristin Milchanowski
Jack Mitchell
Sukanta Mohapatra
Flora Mok
Bruce Monahan
Gary Moore
Matthew Moore
Mohammadreza Mostavi
Kasia Mruczek
Eric Mruczek
Annie Muire
Shabbir Mumtaz
Danet Munoz
Oscar Munoz
Timothy Murphy
Sally Murphy
Lisa Murphy
Kevin Murphy
Ryan Murphy
Raghunandan Mysari
Joseph Nacinovich
Prasad Naga
Nison Nagdimov
Gonzalo Nahme
Ivan Nair
Anjali Nanda
Karina Naringahon
Guillermo Nerio
Adam Nicholas
Holly Niro Kotlarchyk
Vilma Obando
Jeannine O'Brien
Marie O'Brien
Neolida Olouman
Matthew Olund
Melanie O'Neal
Naima Osman
Christine O'Sullivan
Caroline Oswald
Abimbola Otusanya
Sondah Ouattara
Obi Ovie
Catherine Owens
Peter Palleija
Brian Palmer
Calvin Parence
Sang Park
Graham Parker
Sudhakar Pasumarthy
Seema Patel
Nishith Patel
Rishin Patel
Milton Patrick
Dan Payne
Russell Pearce
Maria Pedulla
Cassandra Perdue
Meemanage Perera
Gabriel Perez
Carmen Perez Morrow
Romonie Permaul-Singh
Christina Perrone
William Pham
Som Phanouvanh
Steven Picarillo
Diane Pichette
Brian Pierick
Barbara Pietruszewski
Lashonn Pinkney
Keith Plamondon
Lorraine Plant
Dennis Pomo
Jennifer Powell
Donna Powell
Jeff Preloznik
Sajid Premji
James Preuss
Christopher Punke
Juliy Pyo
Patrick Quimby
Terri Quintana
David Rabbiner
Taofeek Raji
Allan Ramlall
Elbia Ramos
Justyna Ramotowski
Kishani Ratnayake
Holly Ray
Syed Raza
Alejandro Razo
Edward Recio
Rebecca Regan
Ryan Reid
Lucila Reinoso
Michael Richard
Katherina Richard
Mary Ring
Stephanie Ripp
Zachary Ritter
Enchennira Romero
Ian Rooney
Robert Roth
Evelyn Roxana Rousey
Deepthy Roy
Todd Rubel
Jose Ruiz
Walter Rybak
Sachin Sadana
Natasha Safaei
Omar Saif
Juan Salguero
Lita Salvagno
Irina Samoylova
Jennifer Sander
Kevin Sankat
Nicole Santora
Ganna Sapozhnikova
Alejandro Sardinas
Beth Savage
Nancy Sayer
Christopher Scarpati
Peter Sceusa
Lawrence Schaub
Michael Scheiwe
David Schneiderman
Kyle Schultz
Scott Schwed
Jean Scott-Black
Nicholas Secatore
Patrick Selby
Justin Serafini
Steven Serapin
Jennifer Sevigny
Arthur Shaffer
Lisa Shanks
Patricia Sharp
James Shoffman
Carole Shrader
Mohammad Siddique
Nicole Simon
Sidonna Simpson
Karina Simpson
Netra Pal Singh
Chante Slater
Nikolay Smeshko
Harrison Smith
Jermaine Smith
Bethany Sobol
Jeffrey Sottile
Jocelyn St. James
Thomas P. Stapleton
Christopher Stehle
Carly Stewart
David Stomski
Michael Storoniak
William Stoscup
Scott Straka
Matthew Stuart
James Sullivan
Sabina Sumner
Alexandra Suslova
Shobhit Nagendra Swaroop
Richard Sweeney
Michael Swenson
Abdul Nayeem Talukder
Arthur Taylor
William Tesler
Vishnu Thaver
John Thomas
Sunil Thomas
Diana Thompson
Steve Thomsen
Christine Tomassi
Benjamin Toplek
Andy Torbik
Elijah Torres
Susan Tramontelli
Bieu Tran
Stephen Tripp
Rachel Trujillo
Anna Tse
Kimberly Turner
Federico Umana
Maria Urviola Castillo
Michael Vail
Ada Varchola
Danny Vidal
Jennifer Viertel
Gabriella Villa
Karla Villalobos
Steve Vo
Nazar Voloshchuk
Hellen A. Vouthounis
Vincent Vullo
Lindsay Wagener
Nancy Walcott
McKenzie Walker
Daniel Walsh
Hsiao-Hua Alice Wan
Dan Wang
Xi Chuan Wang
Danping Wang
Nathaniel Washington III
Hillary Watanabe
Brian Watson
Arthur Wemegah
Albert Wen
Eileen Werbitsky
Andrew Wessell
Amanda West
Stephanie White
Thomas White
Juel Wiggan
Dana Wild
Alderick Williams
Ronnie Williams
Jeffrey Williams
Alan Willis
Jennifer Winters
Sarah Wise
Joe Wojkowski
Derek Wong
Lutricia Woodard
Ann Marie Wright
Francis Wright
Kevin Wuerfel
Xiao Xiao
Nataliya Yakhtelska
Qiang Yang
Yao Yao
Yeareen Yun
Lisa Zahniser
Kira Zalan
Kara Zandoli
Shannon Zeigler
Dan Zhou
Allison Ziegler
Esthefani Zighami

FILIPINAS

Meylord Capanzana

GHANA

Osei Asianoah
William Nutakor
Joseph Yeboah Takyi

GRECIA

Christos Michailidis

HONDURAS

Wendy Acosta Guifarro
Cesar Castellanos
Helsy C. Moncada Alvarado
Ixhel Osorio Meza
German Rodriguez

HONG KONG

Gary Acheson
Jamil Ahmed
Jodi Andersen
Man Wa Chak
Kwong Chu Cham
Man Ting Chan
Mei Lai Chan
Josephine Chan
Yi Lun Ellen Chan
Yi na Chan
Ching man Chan
Kam Yee Chan
May Chan
Pok Wa Chan
Alan Chan
Hin Pui Ava Chan
Shibani Chatterjee
Pui Sze Chau
Anthony Cheng
Tat Yan Cheng
Cathy Cheng
Wing Shan Cheuk
Lai Ping Cheung
Chai Kit Chiu
Fung Mui Choi
Yiu Cheong Choi
Kanas Chong
Wing Man Chow
Fan Fanny Chu
Mohan Datwani
Jayson Fan
Lulu Fan
Chan Fuk Ming
Andrea Geat
Yawen Guo
Abdul Qadir Hamdani
Nicholas Harrison
Gazell Heung
Ka Ki Ho
Kai Leong Clifford Ho
Wing Yan Hor
Oi Lei Hou
Jing Jin
Edward Kam
Tai San Kelvin Kwok
Mei Chu Kwok
Max Kwong
Mok Lai Wa
To Lam
Katherine Lam
Carrie Lam
Yuen Lam Lau
Chi Kin Lau
Tsz Wing Lee
Ho Yan Lee
Kay Ka Yee Lee
Roland Lee
Shing Kan Lee
Phoebe Lei
Philip Leung
Chuk Kwan Leung
Yuk Sheung Li
Joanne Li
Yan Yan Li
Man Wai Liu
Kris Liu
Wai Lun Liu
Kah Mun Carmen Lum
Ka Wing Ma
See Ling Ma
Sau Kwan Mak
Ivan Mak

Yau Man Yuen
Kong Sang Miu
Kin Chung Ng
Tung Yuen Ng
Winsome Wai Yee Ng
Wan Lung Ng
Samuel Ng
Fong Ting Ngan
David Ogilvie
Yik Chiat Ong
William Yu Wa Pang
Karen Poon
Cheung Pui Man
Jaya Ramaswamy
Ahmer Ramzan
Philip Rodd
Sze Yee Shing
Alok Singhvi
Diamond Tai
Yvonne Tam
Shuk Yin Tang
Mei Fong Tang
Aperaamo Tauialo
Bon Han Tee
Sik Fan To
Kin Fai Tsang
Wing Fung Tsang
Chun Wing Tsang
Pik Man Holly Tse
Sophie Tsoi
Ka Fai Tsui
Lee Tsz Kin
Yalin Wang
Po Shan Wong
Lei Yi Liana Wong
Lai Chun Wong
Yee Mui Wong
Kitty Wong
Suk Yee Wong
Erin Wong
Doris Wong
Yuen Ping Wong
Ying Suet Yang
Ellen Chan Ming Yi
Chiu Wah Yip
Au Yuen Man
Maggie Yung

HUNGRÍA
Istvan Batta
Csilla Gyenes
Imre Szabo

INDIA
P K Sheik Basheer Ahamed
K.T. Ajit
Arvind Bhat
Venu Kumar Burle
C. Chandrapriya
Vivek Choudhary
Silky Gandhi
Shivanath Gunda
Apsha Gupta
Shariff Irfanulla
Sidharth Iyer
Prachi Jadhav
Rishab Jain
Jithin Joseph
Allen Lopes
Tapas Mahajan
Hitesh Makhijani
Viswa A. Murthy Vuppala
Prashanth Nagabhushan
Dhanya Nellikkappillil
Veena Pandey
Satish Patil
Sudhanshu Pattanaik
Srinivas Raju
Praveen Kumar Rawalkual
Caroline Scolt
Rashmi Singh
Satyendra Singh
Amit Srivastava
V. Edwin Thomas
Saraswathi Vasu
Ajay V. Venkatesh

IRLANDA
Aoife Maria Murphy
Charlotte Michelle Nestor
Jennifer O'Shea
Elaine Power

ISLAS CAIMÁN
Shelly Brooks
Damion Tyndale

ISLAS VÍRGENES BRITÁNICA
Rebecca Kathleen Cook

ITALIA
Ginevra Brandi
Oana Stoica

JAMAICA
Shereen Segree
Courtney St. Hubert Welham

JAPÓN
Andrew Barger
Saeko Honoue
Yasunobu Kubota
Naoyuki Nemoto
Yoko Nishio
Takeo Sakata
Makoto Sato
Momoka Uchida
Koji Umezawa

JORDANIA
Ahmad Abdeen
Anas Ahmmad Farag
Akram Al Saad
Mohammad Al Shayeb
Yasseen Alsharif
Nasser Issa Ammari
Saif E Deen Bataineh
Raed Ghayadah
Amal Hammad Alhgaish
Rania Jaouni
Thair Majid Adameh
Zein Musharbash
Amal Marzouq Mustafa Allami
Muayad Nafeth Masheh
Omar Qaqish
Aseel Ramadan
Sameh Samawi
Abdallah Sweidan
Ola Yassin

KATAR
Nader Jalal
Mohamed Megahed Elhefnawy
Suhaib Nisar

KUWAIT
Bader Almudhaf

LA RÉPUBLICA CHECA
Eva Neubauerova

LÍBANO
Antoine El Asmar
Sandra Fallah
Diana Haidar
Robert Kanaan
Rita Naim
Cynthia Khalil Saleh
Nadine Hassib Wayzani
Michline Ziade

LUXEMBURGO
Edina Alic
Arnoud Van Heel

MALASIA
Mohamed Ibrahim
Francisco Joo Ee
Sheena Jose
Robert Joseph
Saravanan Kalaiselvan
Chua Kok Keong
Foo Yu Koon
Shyamal Padmanabhan
Saravanan Perumal
Senthamarai Ramadas
Mellissa Seebran
Teck Chang Seow
Cher Hau Tan

MALTA
David Ferguson

MAURICIO
Anusha Dindoyal
Sameerah Joomun
Sneh Lutchumun

MÉXICO
Walter David B. Buenrostro
J. Miguel M. Barquera
Azul Antinea Mata Gutierrez
Victor Hugo Olmedo Garcia

NICARAGUA
Karla Patricia Garcia Arancibia
Scarlett Machado

NIGERIA
Olugbenga Jaiyesimi
Oladimeji Olona
McLeish Otuedon
Akinyemi Oyeleye

NEUVA ZELANDA
Sara-Kate Bray
Sean Condon
Sue Gavin
Chris Haughey
Ash Johnstone
Kwang Min Park
Kirsten Roy-Reid
Wei-Jiat Tan
Sara Todd

OMAN
Abdullah Juma Al-Mamari
Ashish Nadar

PAÍSES BAJOS
Jacek Baranowski
Foteini Ioannidou
Daniel Van Kan
Huguette Verheijen Van de Loo
Giancarlo Vucchi
Hans-Erik Zwaagstra

POLANIA
Adam Anklewicz
Monika Kobosko
Kamila Kuznar
Zaneta Karina Niszczota
Marian Owczarzy
Jakub Wieliczko

PUERTO RICO
Betzaida Vega Perez

REINO UNIDO
David Abbotts
Vanessa Beattie-Jones
Michael John Beck
Rupert Blake
Alex Bray
Debra Burns
Maria Cherskova
Adrian Cox
Graham Delaney
Jenner D'Monte
Jonathan Dobson
Lawrence Edlmann
Jodie Fairburn
Sam Fisher
Aranzazu Garcia Colino
Alison Garfield
Vicky Gelder-Bird
Olive Geoghegan
Magdalena Gorbacz
Muhammad Mohsin Hassan
Peter Hawkins
Natalie Hough
Charles Jaja
Dinesh Karunadhara
James Kellett
Adrian Laird
Marcus Lightwood
Valeria Locatelli
Adrian Mahoney
Catherine McDonald
Ian McMillan
Lisa Meffan
Nazish Mehreen
Emeka Memeh
Timothy Brian (Tim) Minall
Vincent Mulligan
Miguel Oldenburg
Floxy Oluwadare
Tolulope Osijonwo
Lindsey Parr
Gary Pidgeon
Erencho Potgieter
Raheel Qayyum
Matthew Lang (Matt) Rigby
Tina Rowley
Shahzad Sadiq
Emmanuel Sirieys
Adrian Smith
James Spark
Nicholas Spooner
Kathrine Helen Stillwell
Malgorzata Tarnowska
Stephen Taylor
Krzysztof Tokarski
Sevdiye Turkyolu
Liam Twamley
Andy Veasey
Varadarajan Viswanathan

RUMANÍA
Alin Becheanu
Flaviu Otel Mihai
Sorana Zikeli

RUSIA
Inga Yatskovskaya

SAN CRISTÓBAL Y NIEVES
Collin Walwyn

SAINT LUCÍA
C. Glenroy Tross

SERBIA
Vladimir Bacic
Aleksandar Markovic

SINGAPUR
Xinli Chen
Suyi Chew
Zhenwei Dai
Fairoz Khan
Windel Lacson
Dorothy Li
Jia Jeen Loo
Marc Edward Martinez
Caren Gwen Mayola
Ming Mei Lim
Cheryl Miller
Sudipt Mukherjee
Cherrie (Hui Kuan) Ong
Alisher Rakhmatullayev
Badala Ramkumar
Meenakshi S. Srinivasan
Guo Liang Tan
Florence Tan
Chin Hock Tan
Celestia Tan
Santosh Uchil
Leonard Xiangzhou Ye
Kanglun Sherman Zhou

SUDÁFRICA
Charles Eales
Abubakr Ebrahim
Mitchell Mackay
Thebeetsile Molale
Diane Stinson Van Eeden

SUECIA
Enikö Biró
Karl-Viktor Engstrom

SUIZA
Agricio H. Gomes Ferreira
Phong Quoc Quach
Fernando Vergarajauregui

TAIWÁN
Szu-Chuan Janet Fan
Ricky Hsu
Jui-Chun Huang
Emmy Hsueh-Mei Wang
Hao Jan Wang

TURQUÍA
Berc Aparikyan
Ertug Ekenler
Fatma Tugba Hursitoglu
Z. Fulya Kaptan
Ozgur Ozbayraktar
Özgün Sarıta
Arin Yetgin

UGANDA
Katsigeire Justus

VENEZUELA
José M. Rodríguez Capriles

VIETNAM
Thi Bichha Nguyen

ZIMBABUE
Zivanai Muchenje

Murray Bowen: ALD sigue creciendo

Murray Bowen fue criado en el pueblito de Moore Haven en el condado de Glades, Florida, por padres quienes cumplían tareas de control legal. El condado tenía una población total de 6.500.

Bowen entró a ACAMS en 2008 en el equipo de atención al socio. En la actualidad es un ejecutivo de cuentas en el equipo de ventas y se concentra en las nuevas cuentas de pequeñas empresas, la retención de socios y las renovaciones de suscripción de ACAMS moneylaundering.com.

Antes de entrar a ACAMS, Bowen fue supervisor de elecciones para el condado de Orange en Orlando, Florida, y fue también director de relaciones públicas para dos orquestas. Además, trabajó para una firma de correduría de hipotecas durante ocho años.

ACAMS Today: Ambos de sus padres se desempeñaron en el control legal, ¿nos puede decir en qué capacidad?

Murray Bowen: En realidad me crié en la oficina del alguacil del condado de Glades. Había viviendas adjuntas a la oficina del sheriff y era donde vivía mi familia. Así que supongo que se puede decir que estuve en la oficina del sheriff 24/7. Mi padre era el principal ayudante del sheriff y mi mamá era la administradora de la oficina y la despachadora. En ese momento se trataba de una pequeña fuerza con el sheriff y cinco ayudantes. Tengo un buen número de historias policiales que podría compartir acerca de la vida en un pueblito.

AT: ¿Cómo lo ayudó su participación en el control legal a obtener una mejor comprensión de la lucha antilavado de dinero (ALD)?

MB: No puedo recordar ningún caso de lavado de dinero en mi pueblito, pero sí recuerdo que alguno trató de pasar dinero falso una o dos veces. También, en Moore Haven parecía que había más conducta desordenada, conducción en estado de embriaguez, caza furtiva y arrestos por drogas, es decir, contrabando de marihuana. Por trabajar en ACAMS, ahora sé que la mayoría de estos delitos podría conducir al lavado de dinero y tengo una mejor comprensión de las posibles alertas rojas y los muchos desafíos que enfrentan las autoridades de control legal y los profesionales de la prevención del delito financiero en la lucha contra delitos financieros.

AT: Su trabajo le requiere hablar con los socios durante todo el día, ¿cuáles son algunos de los desafíos que ellos enfrentan en su trabajo diario?

MB: El mayor desafío para nuestros socios es lo ocupados que están investigando y protegiendo a sus respectivas organizaciones de la delincuencia financiera. Debido a su apretada agenda, a veces, el desafío para mí es llegar a hablar con ellos y hacerles saber que ACAMS está aquí para ayudarlos en su lucha contra la delincuencia financiera.

AT: ¿Cuál ha sido la conversación más interesante que ha tenido con un socio?

MB: Yo soy como Vegas: "Lo que pasa en Las Vegas se queda en Las Vegas". En otras palabras, lo que usted me dice queda conmigo.

AT: ¿Cuál diría que es su producto favorito de ACAMS para sus socios y por qué?

MB: Tengo dos favoritos. El primero es AML Foundations, que es para los nuevos profesionales y aquellos que quieran entrar a la industria del antilavado de dinero (ALD). Este programa ofrece los bloques de construcción simples a individuos para comprender los fundamentos del ALD. Además, ofrece asociarse con descuento como parte del paquete, por lo que se aprende algo y obtiene el beneficio de asociarse por un año. El segundo producto es nuestra nueva aula CAMS Virtual Classroom. El aula virtual les da a los participantes una formación práctica de parte de un moderador en vivo y los guía a través de la guía de estudio de CAMS. El CAMS Virtual Classroom también ayuda a cada participante a entender mejor el material y le da una mejor oportunidad de pasar el examen de CAMS al primer intento. Espero poder participar en la clase pronto y rendir el examen CAMS.

AT: ¿Dónde ve usted la industria de ALD en cinco años?

MB: Creciendo, como lo hace ahora. He leído nuestros artículos y alertas tanto en *ACAMS Today* como en ACAMS moneylaundering.com y es aterrador. Cuanto más tratamos de luchar contra el lavado de dinero, el financiamiento del terrorismo y otros delitos financieros, más violaciones en materia de seguridad se llevan a cabo. Parece que siempre hay otro individuo o grupo que trata de aprovecharse del sistema.

AT: Usted es un aficionado de los programas de la televisión, ¿qué considera usted que es su programa favorito de autoridades legales de todos los tiempos?

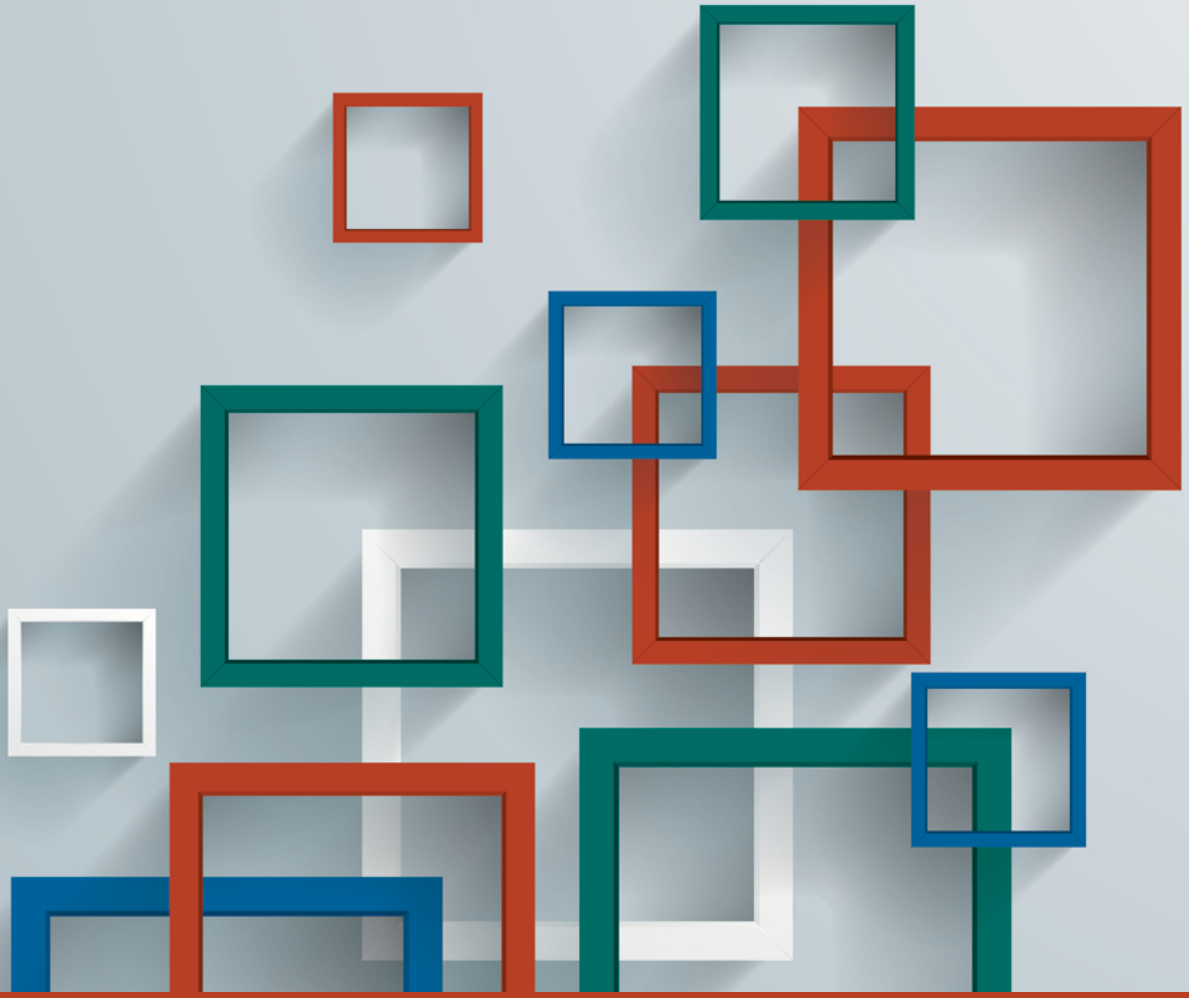
MB: Yo diría *Law & Order*—es un clásico.

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

ACAMS® | AML Foundations

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

EL ACAMS TODAY TOTALMENTE

MÓVIL AMIGABLE Y WEB MÓVIL

Leer *ACAMS Today* se hizo mucho más fácil:

- ✔ Nuevos características
- ✔ Navegación fácil de usar
- ✔ Acceso rápido en cualquier dispositivo
- ✔ Experiencia de uso mejorada

¡Agregue *ACAMS Today* a la pantalla de su dispositivo hoy!

www.acamstoday.org