CUARTA EDICIÓN DE LA APLICACIÓN DE LA LEY

ACAMS® TODAY

La Revista Para los Profesionales en el Campo Antilavado de Dinero

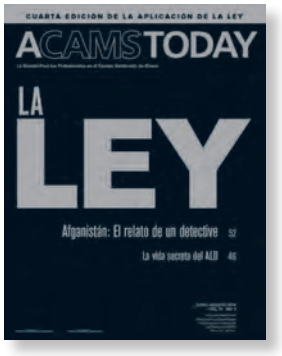
LA LEY

JUNIO–AGOSTO 2014
VOL. 13 NO. 3

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

ACAMS® TODAY

EN LA PORTADA



Afganistán: El relato de un detective
52

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

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

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

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

Fax 1-305-373-5229 ó
1-305-373-7788

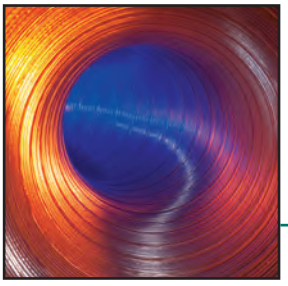
E-mail: info@acams.org

Internet: www.ACAMS.org
www.ACAMS.org/espanol

ACAMS Today — Ganador de los 2014 premios de oro y de plata

The Communicator Awards

Otorgado por el Academy of Interactive and Visual Arts



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

PATRIOT OFFICER®

#1 BSA | AML | ANTI-FRAUD | OFAC | FACTA | SOX | AIBE | EARA | UIGEA Solution

GLOBAL VISION SYSTEMS, INC.

WWW.GV-SYSTEMS.COM

Endorsed By The Largest Bankers Associations and Passed Examinations

THOUSANDS OF TIMES

AMERICAN BANKERS ASSOCIATION ENDORSED

UCEN

PBA Services Corporation

CBA

WBA Wyoming Bankers Association

DBA Delaware Bankers Association

Colorado The Bankers Association

Montana Bankers Association

NMBA New Mexico Bankers Association

NYBA

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

Siempre me he considerado muy patriótica. De hecho, una de mis fiestas favoritas en los Estados Unidos es el cuatro de julio.

Vengo de un pequeño pueblo en el oeste lleno de vaqueros, productos horneados en casa, producciones pueblerinas anuales de musicales bien conocidos y montones de patriotismo. Cuando recuerdo mi experiencia del cuatro de julio en una ciudad pequeña, tengo recuerdos divertidos de desfiles, fuegos artificiales, tartas de manzana y reuniones familiares. Por supuesto que soy la beneficiaria de esos valientes hombres y mujeres que han sacrificado y siguen sacrificando tanto para preservar las libertades que disfruto.

Cuando estaba trabajando en la *Cuarta Edición de ACAMS Today de la Aplicación de la Ley*, me inspiraron los numerosos artículos informativos e interesantes que recibí de expertos en el campo de la prevención de delitos financieros y la palabra patriótico me vino a la mente. Patriótico, por definición, se refiere a alguien leal, dedicado, constante y apasionado por su país. Me gustaría dar un paso más allá y aplicar la palabra a los profesionales de todo el mundo que se dedican a los delitos financieros y al cumplimiento de la ley y que se encuentran en la primera línea de la lucha contra los delincuentes que amenazan nuestros derechos inalienables. Estos profesionales, tanto en el sector público como el privado están luchando constantemente contra los delincuentes que cometen delitos y luego lavan sus fondos ilícitos. El encabezado del artículo, *Afganistán: El relato de un detective* saca a la luz la importancia de la capacitación, las asociaciones y el peligro del papel del que lucha contra delincuentes. El relato de este detective también ilustra la valentía, la camaradería y las posibilidades de una verdadera asociación.

Nuestro segundo titular, *La vida secreta del ALD*, esboza cómo el elemento criminal explota el secreto. El artículo detalla cómo las necesidades de la "S" de la Ley de Secreto Bancario pueden equilibrarse por las instituciones financieras, los reguladores y las fuerzas del orden en el desarrollo de la inteligencia confidencial para el uso efectivo de las investigaciones.

El artículo *Las cuentas de fondos de desvío interestatales—Sacando el dinero de las calles* da luz a esta nueva tendencia de lavado de dinero. Sepa cómo las organizaciones de la droga y el tráfico de personas están utilizando cuentas de desvío interestatales para que sus ganancias ilícitas crucen fronteras a un ritmo rápido y los indicadores de bandera roja de alerta que pueden ayudarlo a detener esta nueva amenaza de lavado de dinero.

Muéstrelo, no lo diga nos da una visión interna de lo que busca un lector de informes de actividades sospechosas (SAR) cuando revisa uno. Este artículo en profundidad muestra cómo escribir SAR útiles que beneficiarán a los investigadores y las fuerzas del orden en su búsqueda de criminales.

El fraude siempre es abundante. El artículo *Combatiendo el fraude de reembolso de impuestos: Las instituciones financieras como capas de defensa* discute la creciente necesidad de identificar y combatir el robo de identidad y fraude de reembolso de impuestos. Entérese de lo que puede hacer como institución financiera para evitar que el fraude fiscal entre en su institución.

Esta cuarta edición especial de aplicación de la ley también contiene entrevistas en profundidad con expertos como Barbara Martinez, Tonja Marshall, Sr. Carmen Pino, Hector X. Colon, Peter Warrack, Dwayne King y Michael Kelly sobre los temas de la trata de personas, el tráfico de personas, el Mercado Negro de Cambio del Peso (BMPE), el maltrato de ancianos, las identidades sintéticas, las alianzas públicas y privadas, el fraude, la confiscación de bienes y mucho más.

Por último, es esa época del año otra vez cuando estamos buscando propuestas para los Premios de Reconocimiento de ACAMS. Asegúrese de proponer su candidato para el *Artículo del Año de ACAMS Today* a editor@acams.org y para *Profesional del Año de ALD de ACAMS* a agonzalez@acams.org. Todas las propuestas deben presentarse antes del 31 de julio del 2014.

Estamos orgullosos de esta edición de la aplicación de la ley, de la amplitud de los temas tratados y del conocimiento compartido de nuestros autores y entrevistados. Esperamos que disfruten de esta edición tanto como nosotros disfrutamos trabajando en ella. También, GRACIAS a la comunidad de aplicación de la ley, a nuestras fuerzas armadas y a los profesionales de la prevención de delitos financieros que se encuentran en constante lucha por nuestra libertad y seguridad.

Karla Monterrosa-Yancey, CAMS
jefa de redacción

CAMS AUDIT

Graduados de CAMS-Audit

BAHAMAS
Andrea Saunders

CANADÁ
Narda Brown

ESTADOS UNIDOS
Svetlana Agayeva
Thomas Alessandro
Robert J. Bradley
John Crouch
Kathe M. Dunne
Sam Adam Elnagdy
David Haghighi
Mary-Jo LaHood
Thomas C. Lorenz
Kathleen O. Smith
Gina Storelli
Mark E. Wolfrey

NUEVA ZELANDIA
Martin Dilly

PUERTO RICO
Victor M. Martinez Cruz

Graduados de CAMS: Febrero–Abril

ARABIA SAUDITA
Yousif Dhiya Al-Dulaijan
Latifa Abdulrahman Alhudaib
Turki Mohammad Al-Madhi

ARUBA
Catherine R.P. Bronswinkel

AUSTRALIA
Thomas Ivan Bonnett
Dane Bowden
John Chevis
Muhammad Saeed
Jacob Scott
Brian Neville Sullivan

BAHAMAS
Nicole Archer
Marcia A. Cooper
Shevette Natasha Nacola Lyles

BAHREIN
Shelly K. Jose
Pankaj Kumar
Mohammed Mattar

BÉLGICA
Dave VanMoppes

BRASIL
Felipe Esteves
Sarah Ryan

CAMERÚN
Ernest Tonka Nkellefac

CANADÁ
Maneesh Agnihotri
Romel Alnazer
Emine Aydin
Michael Baldoni
Duilio Barbaglia
Vivek R. Bhatt
Tammy C. Boe
Horace Bryan
Candy Chan
King Man (Klement) Choi
Oliver Clow
Kevin R. Cmelak
Anthony J. Dissanaike
Abdulai Robert Enakimio
Douglas Fox
Phillip Gellatly
Denise Gouveia
Leo B. de Guzman
Catherine Hardy
Pooran Indar
Ashtona Johnson
Nafees Khurshid
Jiakai Lu
Ivy Lui
Alberto Luis
Kannan Mahadeva
Sh'vaun A. Maher
David Marchbank
Spencer McKay
Lyn Ngu
Jason Nichoslon
Michael Oduro
Stella Osayi Okoh
Guy O'Reilly
Tyler O'Shaughnessy
Ramanujam Padmanabhan
Tushar K. Pain
Benjamin Philippe
Lina Rymar
Premalatha Sarath
Sheeba Sebastian
Ruzanna Shatiryan
Jenny Silva
Leighanne Smith
Joann Sochor
Sam Jaehyung Sohn
Stephen Storey
Judy Myrrh Tan
Catherine Travers
Daniel Udonsak
Asya Vaisman
Caren Wightman
Kwan Pang Wong
Elaine Jie Ling Wu
Qi Ye
Nanda B.M. Yusef
Peng Zhou

CHILE
Eugenie Meijer

CHINA
Beiwei An
Jing Cai
Guoxiang Chen
Haiyan Chen
Min Chen
Xinglei Chen
Zhongtao Cheng
Xin Deng
Yu Deng
Li Dong
Yan Dou
Gang Fang
Jun Feng
Qiang Feng
Shuoshi Feng
Jianrong Gao
Rui Gao
Yan Gao
Wei Geng
Lei Guo
Xiandong Hu
Xiaoling Hu
Chaomin Huang
Jing Huang
Qing Huang
Yishi Huang
Ruicheng Jia
Jia Jin
Su Le
Haiyan Li
Jie Li
Jinmei Li
Wei Li
Xue Li
Yuan Li
He Lian
Di Liu
Wei Liu
Ying Liu
Zhiqiang Liu
Xue Lu
XiaoLan Luo
Jinsong Pan
Jin Qian
Hao Ren
Sun Rui
Rongmei Shi
Yu Jiong (Raymond) Shi
Kai Sun
Lijuan Sun
Ying Sun
Xiuqing Tang
Ming Wan
Dan Wang
Linggang Wang
Qun Wang
Tinghui Wang
Xi Wang
Yan Wang
Yiran Wang
Yuming Wang
Zengke Wang
Kun Wu
Meihua Wu
Xiang Wu
Tingting Xia
Guozan Xie
Jingxiu Xie
Yujun Xin
Biqiong Xiong
Cheng Xu
Jian Xu
Shulin Xu
Xiaoting Xu
Deshun Yang
Ying Yang
Wei Yi
Rong Zhang
Wenjie Zhang
Xunran Zhang
Yan Zhang
Yuanyuan Zhang
Yue Zhang
Shuhua Zhao
Shan Zhong
Hongjuan Zhou
Tianyang Zhou
Wenzhi Zhu
Ya Zhu
Yan Zhu
Yuan Zhu

CURACAO
Stangeline F. Adrien
Priscilla Bueno Guevara

EGIPTO
Mostafa Lotfy El Ashmawy

EL SALVADOR
Lorena Marcela González González

EMIRATOS ÁRABES UNIDOS
Princy Shiju Abraham
Danish Altaf Ahmed
Mohammed Salim Allana
Muhammad Shahid Farid
Mayur Prakash Kank
Hemamalini Krishnan
Sahar Banu Sirajudeen
Pratik Trivedi
Krishnakumar Venkatraman
Maqusood Wangde

ESPAÑA
Miguel Aguado

ESTADOS UNIDOS
Marlyn Abreu
Sandi Acosta
Martin Adams
Rajat Aggarwal
Theolyn L.L. Aimunsun
Katherina Aldmeyer
Nicole Alibayof
Kenneth Allen
Mike Alonso
Afnan K. Altaf
John J. Aman
Roehl Amante
Tomas R. Amidar, Jr.
Karen S. Ampudia
Jason Thomas Andrise
Subramanian Annaswamy
Sonia Araos
Aude Augias
Tara Jomay Avina
Melissa Babin
Zachary R. Baer
Seth Bailey
Donna Baldauf
Bassem Banafa
Maximilian Bargiel
Melanie R. Bargo
Bradley R. Barnes
Michael E. Barnett
Hazen K. Baron
Parminder Batra
Shawn M. Baxter
Elaine Beard
Kieran Beer
Claudia Beltran
Eva Bender
David Bergeron
Marie A. Bianco
Cheri Bilodeau-Barton
Timothy J. Blake
Sharon Blanchette
Joshua Blazer
Brian J. Bolger
Tara Bopp
Ethan Borger
Michael B. Bowman
Michelle Bowsher
Scott Breckheimer
Benjamin Brouillette
James Burns
Jeffrey T. Byrd
Jamessa Nicole Caffey
Kevin J. Carey
Andre Artioli Cavaleiro
Cristina Cea
Sergio Celayo
Daphney Cetoute
Alexander Chan
Xiang Qin Chan
Pushkar Chaudhari
Bo Chen
Diming Chen
William Chen
Xiaoyu Chen
Chavdar I. Chernev
Alice Hei Man Cheung
Bobby Cheung
Brandon M. Childs
Joli Chu
Anthony Claps
Colleen A. Coleman
Jeremy J. Collier
Marta Colomar Garcia
Jo-Ann Copeland
Stefanie Cowden
Aretha Cozma
Terri Crookston
Bridgette Crowe
Nicole H. Cushing
Ann d'Alessandro
Abu Daniel
Debbie Davenport

Sosinna Degefu
Joshua Dellinger
Justin M. Derusha
Scott M. DeRycke
Jessica C. Devereaux
Benny Dharmawan
Juan Carlos Diaz
Joseph P. Dibello
Doreen Dingle
Jacqueline A. DiPaola
John DiSanto
Jeffrey Donovan
John M. Donovan
Peter Dougherty
Stephen J. Douglas
Cindy L. Duffey
Matthew Duffy
Jared Dunn
Marilena Eatman
Alison Edmunds
Patrick Edwards
Sunday E. Eluyemi
Debra Eshbaugh
Mitch Everett
Lindy Falvey
Jeanie Fang
Tracy Fanning
Joseph J. Farlese
Andrew Fast
Stuart Feldhamer
Jonathan C. Feldstein
Lillie E. Fenner
MaryWendell L. Ferguson
Cecilia Fiermonte
Scarlet E. Figueroa
Adam S. Fink
Brian G. Fitzgerald
Ivonne Flores
Madeline Folkman
Lucas P. Forte
Jeremy Foster
Mayya Gabueva
Anthony Gagliardi
Jackie Gaines
John J. Gallagher
Lenny Garcia
Jason Lomar Gardner
Joseph Brien Gately
Dolores Gavcus
Michael Gavrich
Chad Gibble
Leah M. Giese
Sruthi Gollapalli
Altair Gonzalez
Guerlyne Gracia-Bouzi
Osvaldo Gratacos
Jill Grob
Samuel Nobel Grossman
Nicholas Arthur Gunderson
Greg Guthrie
Donna Cook Hall
Karina E. Halperyn
Michael Hannum
Jay Hansen
Brenda Hanson
Jared D. Hanson
Chigusa Hara
Richard Harmel
Rami Hawa
Jessica Hazzard
Elias Hernandez
Mellissa Hettich
Robin Hira
Vicky Ho
Linda A. Hoff
Edgar Holguin
Michael A. Honig
Joshua Horowitz
Spencer Houston
Heng Hsu
Katherine Hulett
Jeong Wook Hwang
Lawrence D. Israel
Leigh Jackson
Drishti D. Jain
Robert Jefferies
Devan Jenkinson
Ben M. Johnson
William H. Johnson
Scott Kaliko
Roy Kantrowitz
Deepak KC
Nicki Keith
Patricia Kenick
Kevin D. Kesterson
Rishaun Khan
John B. King
Peter Klopchic
P. Scott Knight
Kenneth Korsch
Brian M. Krueger
Maura P. Kugler-Vasilescu
Robin Kulas
Neha Kulkarni
Naveen Kumar
Matthew Kuntz
Tara E. Kwiatkowski
Ashley Lam
Erika LaMarch
Nicholas Langenfeld
Michael A. Lanzisera
Henry Lau
Raymond Law
Dayna C. Lederman
Shari Lembach
Bridget A. Lemelle-Phillips
Kristin Leonard
Peter Leroe-Muñoz
Rochelle J. Lester
Ying Y. Li
Julie R. List
Wendy Liu
Adrienne E. Lodge
Monica M. Lojano
Jessie Lopez
Cynthia J. Lopresti
Dennis Lormel
Melanie Louis-Joseph
Eric Lowell Clemonts
Zhao Lu
Royce M. Lugo
Fredrick A. Lutz
Sofya Lysochenko
Peggy Ma
Daniel Mak
Devin G. Mallo
David M. Manek
Thomas E. Manifase
Heather L. Mark
Michael Maroney
Peter Marquardt
Bradley Thomas Martin
Heather Lynn Martin
Kerri D. Martin
Michael Martin
Lise Martina
Omar Martinez
Kevin T. Massiah
Brian Mathews
Erica May
Laura Maytorena
Katie McBrayer
Kourtney Ann McCarty
Sean McCrossan
Megan McNamee
Harold Y. Mendez
Steven Mickelson
Bart Mierzejewski
Brigette K. Miller
Mirela Miraj
Tamara Moiseeva
Alissa Mojica
Frank H. Molteni
Bernard Mooney
Anne Martine Moore
Greyson K. Moore
Patrick J. Moore
Robert Moreiro
Jean Morency
Andrew Muccigrosso
Warren Mui
Allison M. Mulder
Maria Del Carmen Muns
Monica Noemi Murcia
Jinja Murray
Thomas Joseph Nadratowski
Kyle Nelthorpe
Scott Nemeth
Erin Nester
Erik Newberry
Angel Nguyen
TraGiang Nguyen
Jill Niemann
Nicole O'Garro
Eric Ogawa
Pamela A. Ogembo
Fred Olivares
Juan Oliveras
Aaron T.F. Ortiz
Scott Owen
Stephanie Pappaspanos
Zeena Patel
Randy Paul Pearson
Karen Pernia
Todd Petrie
Elyse T. Petruccio
Fitzgerald Philippeaux
Frank J. Pishler
Diane Porter
Alfonso Lopez Portillo Martinez
Daniel Poulos
Rahul Sunil Prabhu
Francine S. Prewitt
Erza Pula
Xiaodan Quan
Rabindranath Ragoonanan
Asif Rahim
Lauren G. Rasmus
Valerie Rattigan
Parker Rauch
Judy Razavi
Leonardo Real
Neha A. Reddy
Peter Reiser
Clay Resnick
Pershaun M. Reynolds
Diliana Reynoso
Damien Sean Rhys
Richard E. Ricot
Andrea Rios
Cortney A. Ritter
Fara Rivera
Lizette Robinson
Michael Roddy
Mary Rodia
Maria A. Rodriguez
Maria E. Rodriguez
Joshua Rogerson
Blanca Rojas
Mindy Romero
Marc Rosner
Theresa Rush
Lawrence Ruttenberg
William Sabate
Christopher Sablich
Ginu Mannakunnil Sabu
Lamis Safa
Ann Sage
Carmen Sandoval
Julio A. Sanjines
Desiree Santiago
Gabriel Sapir
Asif Sardar
Felicite Sare
Leticia Sarmiento
Edouard Sawadogo
Matthew Saxonmeyer
Julie Sbrocco
Mark Schirm
Toni A. Schneider
Jamie Schwab
Daniel Sees
Clayton R. Seifried
Virginia M. Semon-Burley
Nisha Shah
Maryna Shautsova
Lauryn Shay
Jill Sheppard
Victor A. Shier
Catherine Shimota
Sherry (Ya-Ling Hsueh) Shiue
Michelle Simmons
Janet Y. Simms
Lynette Sims
Joshua I. Siniscalchi
Hariharan Sivaramasubramaniam
Cassie L. Skenandore
Thomas M. Slover
Angela Smith
Colin E. Smith
Phillip Sobczak
Kevin P. Sosna
Katherine Spence
Natasha Spence
Christopher Stebbings
Nicholas Stenger
Deborah Stevenson
Crystal Stutler
Melissa Sutherland
Matthew Taggert
Oyetunji A. Taiwo
Lynn Tarantino
John E. Thackeray
April Thatch
Scott Thein
J. Douglas Thompson
Camille Ragadio Tigas
Leonardo A. Tilesio
Derrick Louis Traverzo
Melissa Triplett
Rebecca A. Trujillo
Courtney M. Tucker
Greg Tutelian
Davelon Urbano
Peter Uzee
Andrea Valentin
Luz Velasco
Francisco Ventura
Lori Victory
Edward Virella
Helen Volpert
Jacqueline P. Wade
Nikolaus Walser
William J. Walsh
Noreen Waseem
Joseph C. Wells
Stacy D. West Taylor
Althea T. Weston
Laura A. White
Stephen White
Jeannette Wicks
Brooke Allison Wiener
Bett J. Williams
Azary Witten
Richard J. Wolf
Natasha Woodland
S. Zach Woolley
Rochelle L. Wright
Davendra S. Yadav
Marjorie Yang
Mooi Yap
Bibi Yashin
William Yen
Danielle Young
KaSonya Nichelle Young
Lauren Ziebarth
Teresa Zou

GHANA

Rita Yeboah

GRECIA

Alexandra Eleftheropoulou

HONDURAS

Alba Luz Valladares O'Connor

HONG KONG
Justin Baldacchino
Chee Wai Janet Chan
Chi Fai Chan
Chik Yeung Chan
Fong Chi Chan
Wai Wah Chan
Waiman Chan
Chi Fai Quincy Chan
Cheuk Ming Chang
Wei Chen
Hong To Cheng
Ka Yan Cheng
Lai Mei Cheng
Pui Yan Cheng
Wing Yuen Cheng
Ki Cheung
Pui San Cheung
Rita Cheung
Yik Cheung Dicky Cho
Kar Wing Choi
Yim Yan Lilian Chow
Sin Man Chui
Suet Fun Doo
Dennis Fung
Tin Choi Huang
Hung Keung
Lai Kuen Kylie Keung
Woon Chi Ko
Siu Wai Kong
Yuk Lan Magnolia Kwong
Ngan Ping Lai
Chi Ming Lam
Ka Wai Rebecca Lam
Kei Lam
Lai Ming Lam
Shuk Ching Lam
Fransisca Sari Lau
Jennifer Lau
Mei Kuen Lau
Wai Tai Law
Chi Ho Lee
Paul Lee
Hiu Kong Leung
Po Chun Leung
Cheuk Yin Li
Ming Kwong Li
Chi Sang Lo
Man Un Amanda Lo
Ping Wing Lo
Siu Lung Ma
Tony Mak
Sapna Mangla
Pui Chun Ng
Shuk Fong Ng
Elizabeth A. Pinic
Sui Chun Poon
Mei Wah Shek
Wai Yee Lucia Shiu
Yuk Lan Sit
Yau Chung So
Frances Wai Chun Szeto
Barbara Man Wai Tam
Yiu Yu Francis Tam
Yuen Tung Tam
Siu Loon Henry Tung
Cheuk Yin Wan
Craig C. White
Gloria Chan Wing Chi
Rowena Wong
Shuk Wai Wong
Wan Hing Wong
Wing Yin Wong
Yim Keung Wong
Yuen Tsang Wong
Man Ying Yan
Chi Hung Yau
Ching Mun Anysia Yeung
Ming Hai Ken Yeung
Chi Keung Yim
Ka Yan Yip
Chiho Young
Chen Ping Yu

INDIA
Babu Ashwathappa
Renita Coutinho
Sumit Dhir
Mohammed Mujthahid Masood
Aswathi Nair
Deepa Narasimhan
Bharath HN Rao
Namrata Sood
Vidya Bharati Sundararajan

INDONESIA
Sitti Verny Virnansya Siregar

ISLAS CAIMÁN
Antonette A. Baptist
Reuben Foster
Charmaine McGowan
Allison Clark Morle
Letecia Emmeline Pet
Tristica N. Robinson

ISRAEL
Aaron Jackson

ITALIA
Sara Indelicato

JAMAICA
Austen Douglas-Panther
Tanya Graham Harvey
Fabian Emelio Sanchez

JAPÓN
Shunichi Fukushima
Masahiko Hibino
Yoko Higashikage
Yoji Ichihara
Kyoko Igarashi
Naoko Kawaguchi
Hiromi Morooka
Kazunori Nishimura
Ryohei Ogawa
Atsushi Sakuma
Shuangshuang Wen
Mayumi Yoshino

JORDANIA
Mona Badi Faeq Abu Ghazaleh
Ola Ibrahim Abu Hejleh
Saif Alhawamdeh
Mansour AlKaabnah
Mohammad N. Alkhaldi
Mohannad Alkhalili
Osama Almaghathah
Mamdouh Nayef Mansour AlQhaiwi
Ahmad Mohammad Saleem Al-Rabi
Neven Alrousan
Omar AbdelRahman Alshari
Ashraf Jamil Aqel
Aláa Bani Hani
Maen Barakat
Ramzi Goussous
Rami Abd-Alkarem Hamadh
Luai Husari
Ahmad Omar Ahmad Jaber
Dana Awni Khabbaz
Maria Hanna Masarweh
Adel Mohammed Adel Odeh
Rawan Qaisi
Eman Qasim Issa Rawashdeh
Abdellatif Nabil Samman
Mohammad Yousef

KATAR
Ranya Abou Elhoudas
Shengtian Tang
Ankur D. Vora
Vineet Yash

KENIA
Yvonne Njeri Muturi

KUWAIT
Mona A. Al Saffar
Micheal Adel Adly Zakhary

LETONIA
Kristina Matvejeva

LÍBANO
Ali Abbas
Mario Awad
Houssam Awwad
Omar Baasiri
Nassib Baroudy
Hany Baz
Eliane Chammas
Donna Dagher
Zaher Walid Eido
Wael El Haber
Kamal Abou El Nasr
Wafic Elhinawi
Youmna Fares
Sara Nassar Geadah
Nawal Manneh
Roby Matta
Noura Mikati
Jawad Mohtar
Walid S. Nammour
Rana Rawas
Bassilios Samaha
Joseph Semaan
Randa Sharafeddine
Caroline Yeghia
Tarek Zahran
Gillio Zeinoun

MACAU
Wenting Long

MALASIA
Kang Ching Ee
Kar Yien Lai
Khoo Jean Nee
Pey Sheh (Katrina) Tee
Shelly Vandenberg

MÉXICO
Ivan Veron Esquivel
Karla Rodriguez

NICARAGUA
Aracely Quintana Blandón

NIGERIA
Tunde Bamidele

NUEVA ZELANDIA
Troy Nicholson

PAÍSES BAJOS
Marten De Pagter
Noeme Mennes
Lin Qiu

PAKISTÁN
Muhammad Faraz Haider
Sameer Muhammad Khan
Lubna Naseem
Elvis Smith
Atif Izhar Syed

POLONIA
Lukasz Bunsch
Tomasz Gruszczyk
Lukasz Lecki
Georgios Polyzos
Malgorzata Sarna

PORTUGAL
Ana Sofia Pires Ferreira Lopes
Ana Mello Vieira Santos

PUERTO RICO
Gloria Arlene Hickey Martínez
Wallace R. Ocasio Jimenez
Mariela Ramos
Luis A. Soto
Carlos Reyes Vicente

REINO UNIDO
Olatundun Omotayo Ayinke Abesin
Elisa Marie Adani
Aderemi David Adeyemo
Zade Alnagger
Ross Barrett
Sujana Benchikh
Guido Bendinelli
Benjamin Chapman
Rui Costa
Daniel Couldridge
James A. Dalton
Adetola Gbadebo
Duncan Greatbatch
George O. Gyimah
Samuel Haskins
Mark Patrick Nolan
Norihiro Oyanagi
George Panousopoulos
Derrick Paterson
Soumyadip Rakshit
Micaela Sadati
Amit Singh
Chris Stafford
David Taylor
Samuel Woolard
Liga Zonenberga

REPÚBLICA CHECA
Daniel Bican

REPÚBLICA DOMINICANA
Gianinna Estrella

SINGAPUR
Sobia Amin
Gökçe Arslan
Suk Yen Chung
Natacha Farkas
Craig Fisher
Patrick Matthias Hoehn
Yuan-Chun Huang
Rachel Ya Wen Koh
Ankur Kumar
Jutta Lackner
Marlon Layton
Boon Hau Lim
Hiong Hwee Lim
Say Pean Lim
Ian Loh
Akshay Malhotra
George Choongo Moonga
Preeti Prakash
Monika Roszkowska
Goh Hui Ching Serene
Wui Heck Siong
Odelia Tan
Wayne An Wenzhao
Chun Yee Wong
Jon Yeo
Gideon Young

SRI LANKA
Akila Atapatthu
Nirmal Welikanna

SUDÁFRICA
Gilbert Andersen
Angela Jayne Bates
Jan Bester
Kristin Louise Ellis
Veronika Hruba
Mohale Patrick Matsena
Bethuel Nsibande
Kgaogelo Mercia Ramaboea
Sholane Sathu
Ilze Vorster

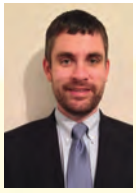
SUECIA
Susannah Borgman Peters

TAIWAN
Aileen Chen-Ching Cheng
Fongmi (Jenny) Chung
Pen-Liang Huang

TRINIDAD Y TOBAGO
Giselle De Verteuil
Jayanti Lutchmedial

TURCAS Y CAICOS
Rebecca Cain

URUGUAY
Stephanie Raciazek



Benjamin Dusenbery, CAMS
Fort Lauderdale, FL, EE.UU.

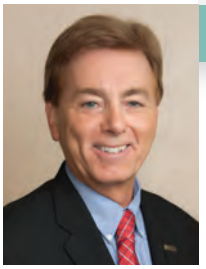
Después de cuatro años de servicio activo en el Cuerpo de Marines de los Estados Unidos, Dusenbery se unió al Departamento de Policía de Fort Lauderdale en 2002. Después de ser ascendido a detective en 2006, se desempeñó en varias unidades especializadas dentro de la División de Investigaciones Especiales, que incluye la unidad de narcóticos que labora en la calle y las principales unidades de narcóticos.

En 2008, Dusenbery fue asignado a la Fuerza de Tarea de Lavado de Dinero del Condado de Broward (MLTF, por sus siglas en inglés), de reciente creación, y todavía sirve en ese cargo. La MLTF es un grupo de trabajo multi-institucional encabezado por la Oficina del Alguacil de Broward y está integrado por agencias federales, estatales y locales de orden público. La MLTF se encarga de la investigación y el enjuiciamiento de los casos complejos de lavado de dinero, las investigaciones de narcóticos a gran escala, la delincuencia organizada, la trata de personas, violaciones financieras, así como otros tipos de delitos graves. Dusenbery también es especialista certificado de antilavado de dinero.

Marie Fulop, M.S., CFE
Fort Myers, FL, EE.UU.

La detective Marie Fulop tiene una maestría en derecho penal con especialización en psicología anormal/ciencias de la conducta. La detective Fulop trabaja actualmente en la Oficina del Sheriff del Condado de Lee, asignada a tiempo completo al Servicio Secreto de los Estados Unidos. Su segundo trabajo es con el Colegio Rasmussen, donde ocupa el cargo de coordinadora y profesora principal de la Escuela de Estudios de Justicia. La detective Fulop ha estado dedicada a la aplicación de la ley por más de 16 años. Pasó 14 de estos 16 años dedicada a las investigaciones delictivas, más específicamente a los casos de lavado de dinero/drogas/fraude.

Ha sido el agente del caso en las causas penales emblemáticas de fraude por lo que recibió distinciones por parte de el FBI y del Servicio Secreto de los Estados Unidos (USSS) por sus logros y las incautaciones en investigaciones federales que resultaron en juicios exitosos. Tiene más de 2.000 horas de formación en la especialidad, por el trabajo con agencias locales, estatales y federales, incluyendo la Drug Enforcement Administration (DEA, por sus siglas en inglés), el FBI, Mariscal de los EE.UU. y USSS. En 2011, la detective Fulop accedió a ser socia de la Asociación de Examinadores Certificados de Fraude (ACFE) y obtuvo su certificación. En 2012, se unió a la Asociación de Especialistas Certificados de la Lucha contra el Lavado de Dinero (ACAMS). La detective Fulop está trabajando diligentemente para lograr su certificación CAMS en los próximos seis meses.



Honrando a las fuerzas del orden

En el punto medio del año 2014, ACAMS se detiene, una vez más, para honrar y reconocer a los valientes hombres y mujeres que sirven a la sociedad como miembros de las fuerzas del orden. En todas partes de la comunidad global de ALD, seguimos desafiados por el terrorismo, el delito organizado, los delincuentes que se aprovechan de las personas mayores y los jóvenes, los estafadores comunes, hackers y gente que simplemente es mala. Nuestros socios en la aplicación de la ley, quienes sacrifican ganancias financieras y muchos otros beneficios para investigar, denunciar y detener a los que se aprovechan de la comunidad son los que se encuentran defendiéndonos. A todos ustedes ACAMS dice "Gracias" y ¡se enorgullece de publicar nuestra Cuarta Edición de la Aplicación de la Ley de *ACAMS Today*!

Temas sobre los cuales reflexionar en esta edición

Nuestra *Cuarta Edición de la Aplicación de la Ley* cubre la gama de temas tomados de los títulos de ALD y del fraude financiero:

- El horrible (y, tristemente, de larga data) delito de la trata de personas;
- Los desafíos únicos de la capacitación de la Policía Nacional de Afganistán;
- La marihuana, el debate en curso sobre la forma de abordar el hecho de que varios estados están despenalizando su venta—con lo que se coloca a los profesionales de ALD y sus instituciones financieras en un dilema;
- Un artículo creativo sobre en realidad mirar su plan de investigación a la inversa para ayudarlo a aumentar sus destrezas investigativas;
- La vieja pregunta sobre cómo escribir un SAR mejor; y
- Entrevistas con los principales líderes de su comunidad.

Déjenos saber lo que piensa de esta edición—si lo lee en papel, en ACAMSToday.org o en la aplicación *ACAMS Today*, *ACAMS Today* ¡es el líder mundial en la publicación de información de ALD! Sus comentarios siempre son bienvenidos.

Una oferta educativa de vanguardia — las Fundaciones de ALD de ACAMS

Como he mencionado antes, ACAMS no se detiene en nuestro compromiso de proporcionar a los miembros las herramientas necesarias para mantenerse a la vanguardia de la continua necesidad de garantizar que el personal obtenga la capacitación pertinente de ALD. En concreto, hemos escuchado su pedido de capacitación integral para el personal de nivel de entrada de ALD, las líneas pertinentes de profesionales de negocios que trabajan con temas de ALD, y el personal de gobierno que necesita más que el conocimiento general de las muchas áreas de lavado de dinero y delitos financieros. ACAMS ahora ofrece "Fundamentos de ALD de ACAMS", un amplio programa en línea con características interesantes de aprendizaje adaptativo que llenarán los vacíos de formación en el mercado y pondrán al estudiante exitoso en la carrera de CAMS o simplemente le dará un conocimiento fuerte de los fundamentos de ALD. No hay oportunidad de aprendizaje comparable que no sólo refuerza el conocimiento operativo de conceptos importantes del empleado, sino que le da acceso a los beneficios que ofrece el ser socio de ACAMS.

Un pedido continuo de diálogo— ¿o molinos de viento?

He pedido en blogs, conferencias y artículos la necesidad de que los que hacen cumplir la ley y los del sector financiero trabajen juntos y tengan un diálogo sincero con la comunidad reguladora sobre cuáles son los objetivos de las leyes diseñadas para abordar el lavado de dinero. Ya sea que tengamos una cumbre, charlas bajo reserva o un debate real, el entorno actual no puede permanecer. Todos compartimos el objetivo de combatir el movimiento de ganancias delictivas—¿quién puede tomar la iniciativa y probarlo?

¡Enhorabuena a la premiada *ACAMS Today!*

Por último, me complace anunciar que ¡la Academy of Interactive and Visual Arts ha adjudicado a *ACAMS Today* "The 2014 Communicator Award" en cinco categorías! ¡Felicidades a Karla Monterrosa-Yancey y su grupo de tareas editorial por este merecido reconocimiento!

John J. Byrne, Esq., CAMS
vicepresidente ejecutivo

HECTOR X. COLON:

EXPLOTANDO A LOS ESTAFADORES Y SUS TRAMAS

ACAMS Today tuvo la oportunidad de hablar con Hector X. Colon, el jefe de unidad de la Unidad de Transparencia Comercial, de Narcóticos y de Operaciones Especiales División Financiera, (División 2), Investigaciones de Seguridad Nacional (HSI), acerca de una gran variedad de temas que van desde el Cambio de Peso del Mercado Negro (BMPE), el maltrato a los mayores, la financiación del terrorismo hasta las monedas virtuales.

En su cargo actual, Colón tiene la supervisión programática de las investigaciones y operaciones de HSI basadas en el comercio de lavado de dinero (BMPE) en todo el mundo. Es el responsable del desarrollo de iniciativas nacionales e internacionales destinadas a identificar, investigar y procesar a los terroristas y las organizaciones delictivas transnacionales que mueven y lavan sus fondos ilícitos a través de tramas complejas que involucran el comercio global. En NTC-I, dirige los esfuerzos de HSI para incrementar la colaboración con CBP a través de todo el continuo de seguridad fronteriza, incluyendo: prohibiciones, investigaciones de HSI y la explotación conjunta de inteligencia. Colon comenzó su carrera de policial federal en 1997 con el ex Servicio de Aduanas de los EE.UU. en San Juan, Puerto Rico, especializándose en delitos financieros, fraude aduanero, delitos cibernéticos e informática forense. Ha servido en una variedad de cargos de liderazgo de HSI en misiones extranjeras y nacionales, incluso el de jefe de la Unidad de delitos de Ilícitos Financieros y ganancias de HSI. Colon también ha representado a HSI en diversos foros nacionales e internacionales, como el Grupo Asesor de la Ley de Secreto Bancario de los EE.UU. (BSAAG) y el Grupo de Acción Financiera Internacional (GAFI).

ACAMS Today: ¿Qué supone esto para el comercio y las aduanas?

Hector Colon: El cambio del peso en el mercado negro, o BMPE, es un método altamente complejo utilizado para mover el valor a nivel internacional utilizando esquemas de TBML como mecanismo de solución. El proceso de BMPE se compone de múltiples tramas financieras y relacionadas con el comercio que trabajan juntas sin problemas para eludir medidas mundiales de antilavado de dinero (ALD) y la aplicación de la ley. Las tramas de BMPE se han convertido en uno de los métodos preferidos de las organizaciones delictivas financieras transnacionales (TCO) para mover valores disfrazando sus orígenes e integrándolos a la economía legítima. El BMPE y el TBML, sirven además para ocultar el origen de las ganancias obtenidas ilícitamente a través de la importación y exportación de productos legítimos — tales como material electrónico — comprado con, o como sustituto de los fondos derivados de actividades delictivas.

El movimiento ilícito de dinero de las organizaciones delictivas se puede clasificar en tres:

- *Operaciones financieras* — alto riesgo de detección debido a su rastro de papel financiero
- *Contrabando de dinero en efectivo* — alto riesgo de detección y costo
- *Comercio* — bajo riesgo de detección debido a la complejidad de la trama

El sistema de comercio internacional proporciona un camuflaje natural para el TBML debido a su complejidad heredada y el alto volumen de transacciones comerciales que se realizan dentro del sistema de comercio internacional. El BMPE también puede ofrecer a las TCO la capacidad de evitar los derechos de importación, impuestos de ventas y de renta, la excesiva regulación y requisitos de información relacionados con el movimiento de, y las transacciones relativas a la moneda, y con frecuencia los tipos de cambio menos favorables asociados a los mecanismos de cambio de divisas formales.

AT: ¿Qué cosas debe buscar un oficial de ALD cuando se trata de un BMPE?

HC: Los siguientes son algunos indicadores básicos de bandera roja de alerta de posible actividad de TBML:

- Dinero en efectivo para pedidos de valor alto
- Productos con precios bien por encima o por debajo del valor de mercado
- Discrepancia entre los elementos y lo ordenado por el cliente
- Transmisiones de empresas efectuadas sin razón aparente
- Financiación por terceros
- Embalaje incompatible con los contenidos
- Tamaño y peso de paquetes incompatibles con contenidos
- Ruta de envío tortuosa o económicamente ilógica

Debe tenerse en cuenta que a medida que los estándares de ALD se hacen más eficaces, otras tramas complejas que abusan de los sistemas internacionales de comercio son cada vez más atractivas para los profesionales o tercerizadores de lavado de dinero. Las TCO prefieren cada vez más los sistemas de TBML que minimicen sus riesgos de detección.

AT: ¿Hay un vínculo establecido entre BMPE y la financiación del terrorismo?

HC: BMPE es sólo uno de los muchos tipos de tramas complejas en el ámbito de TBML que podrían utilizarse para financiar y legitimar las ganancias de actividades ilícitas, para incluir el financiamiento del terrorismo. A principios de este año, al Lebanese Canadian Bank con sede en Beirut (LCB) se le condenó a pagar al gobierno de los EE.UU. $102 millones como parte de un acuerdo al que se llegó porque estaba involucrado en una trama global de lavado de dinero destinada a ayudar al grupo terrorista libanés Hezbollah. Las instituciones financieras libanesas con lazos significativos con Hezbollah habrían cableado fondos desde Líbano a los EE.UU. para comprar y embarcar coches de segunda mano al África Occidental. Los beneficios de las ventas de automóviles usados en África Occidental, así como los ingresos de estupefacientes, fueron luego canalizados de vuelta al Líbano con la ayuda del LCB.

AT: ¿Es BMPE uno de los tipos de casos de ICE más frecuentes considerados recientemente?

HC: BMPE es uno de los muchos tipos de delitos financieros que Investigaciones de Seguridad Nacional (HSI) de Inmigración y Control de Aduanas (ICE) de los EE.UU. investiga todos los días. HSI es un legado del Servicio de Aduanas de los EE.UU. y es el brazo principal de investigación del Departamento de Seguridad Nacional de los EE.UU., con más de 7.000 agentes especiales que llevan a cabo una amplia gama de investigaciones para incluir el movimiento ilícito de mercancías dentro y fuera de los EE.UU., así como el lavado de dinero y otros delitos financieros asociados a tales violaciones. HSI también investiga habitualmente otros delitos que pueden calificar como actividades ilegales específicas como el blanqueo de dinero y los delitos predicados de violaciones del crimen organizado, que incluyen lo siguiente:

- Contrabando/tráfico de narcóticos
- Importación y exportación de contrabando y fraude aduanero
- Contrabando de armas
- Violaciones de exportación asociadas con la mercancía en la Lista de Control de Comercio o la Lista de Municiones de los EE.UU.
- Violaciones relacionadas con la infracción de la propiedad intelectual transfronteriza
- Violaciones que involucran explotación de niños
- Contrabando/trata de personas
- Falsificación de documentos/beneficios de inmigración
- Cleptocracia y malversación de fondos públicos por parte de funcionarios públicos
- Fraude electrónico asociado a la extorsión de fondos por parte de las personas fuera de los EE.UU. (por ejemplo, el fraude de telemercadeo y ardides románticos)

- Empresas de transmisión de dinero que operan sin licencia
- Delitos financieros relacionados con lo cibernético

AT: Casos de maltrato a personas mayores, trata de personas, y moneda virtual ¿han estado en el radar de ICE recientemente, y cuáles son algunas de las tendencias que se ven?

HC: Sí, HSI ha estado investigando la amenaza de lavado de dinero que supone la explotación de los sistemas de monedas virtuales en los últimos cinco años. Hemos estado monitoreando el crecimiento, y el uso ilícito de los dos tipos de sistemas de monedas virtuales: sistemas de divisas virtuales centralizadas como Liberty Reserve o e-gold, y sistemas de monedas virtuales descentralizadas como Bitcoin.

Después de la persecución y desaparición del sistema de moneda virtual e-gold, HSI y sus socios de agencias federales identificaron la tracción de mercado del sistema de moneda virtual Liberty Reserve (ahora difunto). La moneda virtual Liberty Reserve se utiliza principalmente en dos formas: la promoción de las actividades de la delincuencia cibernética, como el comercio con tarjetas de crédito comprometidas y la información de identificación personal (actividades conocidas como cardado o "carding" en inglés) en los mercados negros subterráneos; y, el lavado de las ganancias ilícitas derivadas del cardado y de fraudes online.

Hay docenas de sistemas de moneda digitales como Liberty Reserve, pero hasta que la acción reciente de ejecución, por parte de un grupo de trabajo interinstitucional conjunto incluyendo HSI, IRS, el Servicio Secreto de los EE.UU. y el Fiscal de los EE.UU. para el Distrito Sur de Nueva York, Liberty Reserve fue el líder del mercado. El grupo de tareas de Liberty Reserve arrestó a seis operadores principales y se apoderó del nombre de dominio asociado con este sistema de moneda virtual:

- Liberty Reserve pretendía operar desde Costa Rica.
- Los servidores se encontraban en Europa.
- Los operadores principales eran ciudadanos de los EE.UU. que habían renunciado a su ciudadanía y se convirtieron en ciudadanos costarricenses.
- La operación de imposición involucró una amplia cooperación internacional.
- Aproximadamente $29 millones dólares se han incautado de la operación hasta la fecha.
- HSI Las Vegas y el Centro de Delitos Cibernéticos de HSI originaron el caso.

Desde el derribo de Liberty Reserve, nuevos sistemas de moneda digital se han apresurado a llenar el vacío. Si bien hay muchos sistemas de moneda virtual en el mercado, es prematuro determinar cuál va a convertirse en el líder del mercado. HSI ha aprendido de sus investigaciones en materia de ciberdelincuencia (por ejemplo, el juego, cardado y sitios web en el mercado negro que se dedican al contrabando) que las TCO utilizan la moneda virtual para ocultar y transferir fondos de forma anónima.

Específicamente, HSI ha identificado nuevas tendencias para que los delincuentes utilicen profundas plazas de mercado web para distribuir contrabando, del tipo de drogas, armas, y pornografía infantil. Estos criminales han emigrado a aceptar Bitcoin como forma de pago para promover el lavado de dinero. El uso ilícito de Bitcoin se convirtió en sinónimo de la página web de la droga en el mercado negro, Silk Road. Este sitio web operó dentro de la red "Onion Router" (TOR). En octubre de 2013, el sitio web de Silk Road fue capturado y el operador principal que lo controlaba (conocido como el administrador) fue arrestado en San Francisco por el FBI con el apoyo de HSI.

Como resultado de la investigación de Silk Road, la Oficina del Fiscal de los EE.UU. para el Distrito de Maryland, acusó a John Doe también conocido como "el temible pirata Roberts" de múltiples violaciones incluyendo: conspiración para distribuir una sustancia controlada, Título 21 U.S.C. § 846; intento de asesinato de testigos, Título18 U.S.C. § 1512(a)(1)(C); y uso de las facilidades de comercio en la comisión de asesinato a sueldo, Título 18 U.S.C. § 1958(a). El 1 de octubre del 2013, en colaboración con la Oficina del Fiscal de los EE.UU. para el Distrito Sur de Nueva York, HSI Baltimore consiguió una acusación formal del gran jurado contra el temible pirata Roberts bajo su verdadera identidad de Ross William Ulbricht.

HSI siguió atacando la distribución y venta de contrabando ilícito dentro de mercados profundos de la web. En enero de 2014, una investigación de HSI y el FBI llevó a la identificación de una red de personas que compraron toxinas mortales de estos sitios en línea. Estos vendedores en los mercados profundos de la web aceptan Bitcoin como forma de pago para anonimizar aún más la compra de contrabando. Hasta la fecha, HSI ha realizado varias detenciones en relación con esta investigación.

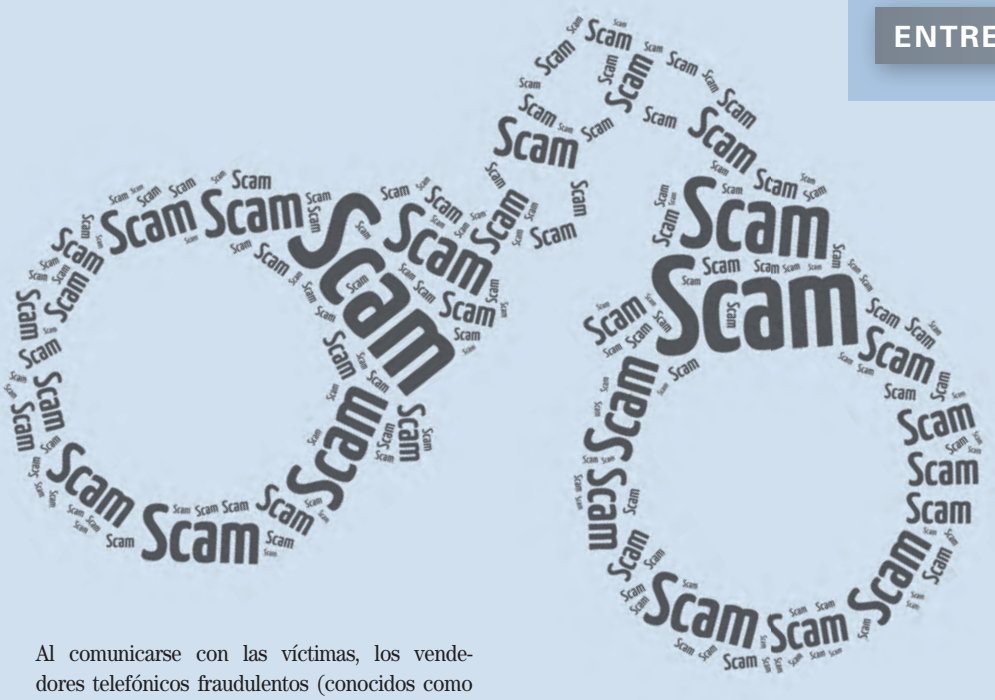
HSI ha puesto en marcha recientemente un programa de economía subterránea digital centrado en la orientación del uso ilícito de moneda virtual asociado con el lavado de dinero y el financiamiento de la delincuencia, así como ha establecido como objetivos los mercados negros subterráneos en línea tales como los utilizados para facilitar el tráfico de drogas, armas, y la pornografía infantil, así como los utilizados para participar en el robo de identidad y de cardado. Este programa se basa en la experiencia operativa de HSI derivado de las investigaciones de Liberty Reserve y Silk Road, y busca identificar las tendencias y metodologías asociadas con el uso ilícito de moneda virtual emergente. Dado que la tecnología y los sistemas de moneda virtual están en constante evolución, es fundamental que la aplicación de la ley de los EE.UU. y de la comunidad reguladora unan sus fuerzas con el sector bancario y las entidades legales que operan en el campo de la moneda virtual para el desarrollo uniforme y procedimientos de colaboración y políticas dirigidas a encontrar e interrumpir a actores delincuentes.

HSI reconoce la grave amenaza del fraude en la comercialización internacional de masas (IMMF) formulada por las TCO que operan desde el África Occidental y las regiones del Hemisferio Occidental, como Canadá, Costa Rica y Jamaica. Las tramas delincuenciales subyacentes implican estafas como el fraude de cuotas por adelantado, las estafas de lotería, telemarketing, compradores misteriosos (mystery shoppers en inglés) y estafas de alquiler de bienes raíces asociadas a instrumentos monetarios fraudulentos.

La IMMF continúa desafiando a los funcionarios de los EE.UU. encargados de hacer cumplir la ley debido a que los actores criminales principales se encuentran a menudo fuera de la jurisdicción de los EE.UU., y, debido a que estos actores siguen evolucionando y adaptándose a nuevas tecnologías y servicios de Internet. Las TCO que participan en IMMF utilizan la banca y el dinero de las remesas tradicionales con regularidad, así como las técnicas de lavado de dinero que emergen de la utilización ilícita de los dispositivos de moneda virtual y de acceso prepago para mover y lavar las ganancias obtenidas ilícitamente.

HSI se centra en la lucha contra la amenaza de la IMMF. La estrategia consiste en tomar un enfoque holístico de la lucha contra las TCO apuntando el de comunicaciones por Internet, el transporte y los servicios de correo urgente y los sistemas financieros que explotan para iniciar y promover sus fraudes.

De acuerdo con la Comisión Federal de Comercio de los EE.UU. (FTC), los consumidores estadounidenses pierden miles de millones de dólares cada año debido al fraude de telemercadeo transfronterizo. Para los ancianos de los EE.UU., que a menudo son los más vulnerables a este tipo de fraude, las pérdidas pueden superar los cientos de millones de dólares al año y en muchos casos supondrán la pérdida de ahorros de toda la vida de la víctima.



Al comunicarse con las víctimas, los vendedores telefónicos fraudulentos (conocidos como "estafadores") normalmente se identifican como abogados, funcionarios de gobierno, la policía, o funcionarios de la empresa de lotería. A las víctimas potenciales se les hace creer que han ganado un sorteo, varios millones de dólares internacionales, cuando en realidad las ganancias son inexistentes. Los estafadores luego les dicen a las víctimas que, a fin de recibir sus ganancias, tienen que pagar una cuota por adelantado, por lo general se describe como impuestos, seguros, o derechos de aduana que se deben pagar para liberar sus ganancias. Las víctimas tienen instrucciones de enviar los fondos a través del correo, mensajería o transferencias de dinero como Western Union o MoneyGram, y a través de dispositivos de acceso prepago, como las tarjetas.

Dentro del IMMF, las TCO, una variedad de socios delincuentes, adquiere un papel muy especializado y participa en estafar a la víctima durante un período prolongado de tiempo. En muchos sistemas, los socios delincuentes asumen funciones especializadas tales como "Jefe de sala", "Abridor", "Cargador", "Corredor" y "Destructor".

Papeles:

- Jefe de sala — gerente de la sala de calderas, que reparte las listas de llamadas
- Abridor — estafador que hace la primera llamada para desarrollar con éxito una relación
- Cargador — estafador que luego intensifica la trama para estafar más dinero
- Corredor — mula que recoge el dinero
- Destructor — estafador que coordina con los corredores para recoger el dinero remitido por cable

La mayoría de los estafadores construyen su credibilidad y confianza presentándose de manera muy elocuente y profesional. Muchas de las víctimas de fraude de telemercadeo son de edad avanzada, que a menudo están aislados y solitarios.

Un subgrupo de víctimas sufre de las primeras etapas de trastornos cognitivos tales como la enfermedad de Alzheimer y la demencia. Los estafadores suelen cultivar relaciones personales con las víctimas. Los estafadores establecen una relación con la víctima, ganan su confianza mediante el empleo de tácticas de ventas comprobadas de telemercadeo. Los estafadores luego explotan esta confianza para manipular a la víctima para que revelen información personal, transfieran fondos, y envíen "regalos".

Informes de las víctimas revelan la naturaleza viciosa de este crimen. Los estafadores a menudo bombardean repetidamente a sus víctimas con llamadas telefónicas sin parar, incluso empleando el abuso verbal para coaccionar a las víctimas. Intimidadas, confusas y agotadas, las víctimas finalmente ceden a las exigencias del vendedor telefónico. Algunas de las víctimas han denunciado amenazas contra su vida y/o la vida de miembros de la familia cuando se resistían al envío de dinero. Los estafadores pueden decirles a las víctimas que la cooperación con la policía podrá causarles la muerte o lesiones a ellos o a sus familiares, lo que puede conducir a que estas tramas queden sin declarar.

En un esfuerzo conjunto para combatir los esquemas de telemercadeo fraudulentos basados en el extranjero, HSI se ha asociado con las autoridades de Canadá y Jamaica para crear dos iniciativas conocidas como Proyecto COLT (Centro de operaciones vinculadas a Telemarketing) y Proyecto JOLT (Operaciones jamaicanas vinculadas al telemercadeo). El enfoque de estas asociaciones es el de identificar, desbaratar y desmantelar las organizaciones que perpetran estas tramas, incautar las ganancias de sus operaciones, y devolver el dinero a las víctimas del fraude de telemercadeo.

El Proyecto de Activos, Dinero y Ganancias de Contrabandistas y Traficantes (STAMP) tiene como objetivo los ingresos ilícitos obtenidos por el tráfico de personas y de las organizaciones de tráfico de personas. Con el fin de desbaratar y desmantelar efectivamente el funcionamiento de estas TCO, HSI está apuntando al mismo tiempo al contrabando, así como a las actividades de financiación y de lavado de dinero de estas TCO. Sumando las sanciones sustanciales asociadas con violaciones de lavado de dinero se aumentan significativamente las penas recibidas por las personas condenadas por el tráfico ilícito de personas y violaciones de tráfico de personas. Además, cuando se rastrea el dinero a menudo este conduce a la cima de una organización criminal y a la incautación y decomiso de activos y las ganancias obtenidas ilícitamente es crucial para el desmantelamiento de la actividad criminal arraigada.

La actividad financiera asociada con el tráfico y la trata de personas es muy diferente de la asociada a otros tipos de delitos. Con el fin de ayudar a los socios de la industria financiera en la identificación de estas transacciones, HSI ha desarrollado indicadores de bandera roja sobre la base de una amplia revisión de los flujos financieros relacionados con el tráfico y la actividad de la trata de personas. Estos indicadores de bandera roja se comparten con socios del sector financiero en las conferencias y durante las sesiones de estrategia conjuntas.

Se necesita una acción dinámica y coordinada para cerrar las organizaciones delictivas de tráfico humano y la trata de personas y la incautación de los fondos que motivan y amplifican los problemas asociados con estas organizaciones es de alta prioridad para HSI. HSI ha tomado un papel de liderazgo entre los organismos encargados de hacer cumplir la ley en todo el mundo proporcionando experiencia en el tema en los foros nacionales e internacionales en los que las tipologías de lavado de activos relacionados con el contrabando de personas y el tráfico humano han pasado a primer plano.

Entrevistado por: Cindy Choi, miembro de ACAMS grupo de trabajo editorial, Toronto, Canadá, cindylmchoi@gmail.com

CUENTAS DE DESVÍO INTERESTATALES

–Sacando el dinero de las calles

En los últimos años, la tendencia de lavado de dinero conocida como "cuentas de desvío interestatales" ha crecido en popularidad sobre todo entre las organizaciones de la droga y las de contrabando de extranjeros. Las cuentas de desvío interestatales, o cuentas de efectivo interestatales, son actualmente uno de los medios más eficientes para que las organizaciones de la droga y las del contrabando de seres humanos puedan mover rápidamente ganancias ilícitas dentro de los EE.UU. (estados de destino) a aquellos estados que limitan con la República de México (estados de origen).[1]

Si bien las cuentas de desvío interestatales no han reemplazado otros medios tradicionales de mover dinero en efectivo, como puede ser el transporte vehicular de moneda a granel, son una evolución de las prácticas de lavado de dinero. Para las organizaciones delictivas, las cuentas de desvío interestatales ofrecen varias ventajas. Las dos ventajas más importantes son el rápido movimiento de dinero a través de grandes distancias con honorarios mínimos y el anonimato de los depositantes ya que los depósitos en efectivo se encuentran generalmente bajo los umbrales de notificación.

Entre los beneficios adicionales de las cuentas de desvío se encuentra la consolidación del volumen físico del dinero en efectivo. Por ejemplo, los depósitos en efectivo pueden consistir en una mezcla de billetes de alta y baja denominación mientras que los retiros posteriores pueden hacerse en denominaciones altas. La disminución del volumen hace que sea más fácil para las organizaciones mover y ocultar cargas en efectivo. Otro de los beneficios es la limpieza literal de los billetes, ya que el dinero en efectivo depositado por una organización de tráfico de drogas (DTO en inglés) puede tener fuertes residuos y olor de estupefacientes, mientras que el efectivo retirado del banco en un estado diferente está limpio y libre de residuo concentrado. Por otra parte, el uso de cuentas de desvío interestatales permite a las organizaciones delictivas evitar los esfuerzos de interdicciones de autopistas, aeropuertos y encomiendas de la policía.

Atributos de cuentas de desvío interestatales

El cliente bancario que abre la cuenta de desvío interestatal suele ser un testaferro de la organización delictiva y por lo general no se involucra en el delito de narcotráfico o el contrabando de personas. En la mayoría de los casos, los titulares de las cuentas pagan una cuota a las organizaciones delictivas para utilizar cuentas existentes o abrir cuentas nuevas. Esta tarifa puede variar desde $200 a $500 por transacción. Los titulares de cuentas pagan por aceptar depósitos, hacer retiros, y entregar las ganancias ilícitas retiradas de la cuenta al representante de la organización delictiva.

Una vez abierta la cuenta, el representante de la organización delictiva comunica el (los) número(s) de cuenta a sus clientes co-conspiradores de todos los EE.UU. Poco después, el cliente conspirador deposita efectivo en la cuenta de la organización, que a su vez, está inmediatamente disponible para ser retirado en el estado de origen. Este método de pago de honorarios de contrabando de extranjeros, o cualquier otro ingreso ilícito, es tan conveniente como ir a las sucursales bancarias locales.

Un análisis de informes de la Ley de Secreto Bancario (BSA) ha identificado que la actividad de la cuenta se asocia a menudo con las cuentas de desvío: depósitos anónimos de fuera del estado hecho en efectivo en varios estados; retiros rápidos de efectivo en cantidades similares a los depósitos en efectivo; uso de boletas de depósito de ventanilla; depósitos y retiros individuales intencionalmente menores a $10.000 (estructuración); acreditaciones limitadas en las cuentas, pocos depósitos que no sean en efectivo (es decir, no hay depósitos de sueldo ni transferencias electrónicas); no hay negocio legítimo evidente; y la actividad de depósito es mayor que los ingresos previstos.

Informes sobre transacciones de divisas (CTR en inglés) se pueden presentar en la actividad de la cuenta de desvío interestatal si varios depósitos suman más de $10.000. Los CTR presentados

[1] Los estados fronterizos se conocen como "estados de origen" porque se encuentran en el origen o punto de tránsito de la mayoría de la actividad de la droga y del contrabando humano en los EE.UU. Con el tiempo, la droga ilegal o los extranjeros pasarán al interior de los EE.UU. a los "estados de destino".

en las cuentas de desvío a menudo indican que múltiples transacciones ocurrieron en sucursales bancarias geográficamente distantes.

Indicadores de banderas rojas de alerta

- Cuenta(s) con múltiples depósitos que son transferidos en breve a otras cuentas;
- Cuentas con una alta actividad sumada de depósitos en dólares, pero con saldos bajos;
- Cuentas con depósitos de múltiples particulares o empresas diferentes;
- Cuentas con múltiples depósitos de varios lugares fuera de la zona de la banca; (por ejemplo, un banco domiciliado en California con depósitos en Illinois y Georgia);
- Cuentas con múltiples depósitos de múltiples orígenes (por ejemplo, depósitos en efectivo, en cajeros automáticos, cheques, transferencias bancarias, etc.);
- Cuentas abiertas en los EE.UU., por personas temporalmente en los EE.UU. con documentos de identidad inmigratorios (como tarjetas de cruce fronterizo), que, a continuación, se usan para transferir fondos de vuelta a México;
- Los depósitos son de inmediato (o dentro de 1 a 2 días) transferidos por cable de la cuenta;
- Cuentas con un número inusualmente alto de rechazos de débito;
- Actividad financiera no acorde con el negocio u ocupación indicados del depositario;
- Cambio brusco en la actividad de la cuenta; y
- Uso de varias instituciones financieras para disfrazar el nexo de los fondos depositados con movimientos a través de fronteras internacionales de los EE.UU.

Ejemplos de casos

Organización de narcotráfico de Waine Vassel

En junio de 2008, HSI Phoenix inició una investigación en relación con un empleado bancario que facilitaba la actividad de "cuenta de desvío interestatal" por una tarifa. La investigación reveló que una cuenta abierta por el empleado del banco a su nombre la usaba una organización de narcotráfico como método principal para mover sus fondos ilícitos en apoyo de su empresa delictiva. Los resultados iniciales de analizar la cuenta del empleado del banco mostraron un patrón de transacciones financieras sospechosas relacionadas con depósitos en efectivo anónimos en instituciones financieras situadas en la costa este de los EE.UU. Retiros de efectivo posteriores fueron hechos por el empleado en Phoenix, Arizona. El DTO utiliza numerosas cuentas bancarias para mover más de $700.000 en ganancias ilícitas procedentes de otros lugares de los EE.UU. a Arizona.

La conspiración se amplió cuando la investigación identificó los miembros de la organización de narcotráfico que operaba un envío de droga y operación de lavado de dinero desde Phoenix, Arizona. Dos de los objetivos de la investigación de HSI Phoenix, Waine Vassel y Anton Holt, jugaron un papel decisivo en el contrabando de miles de kilos de marihuana a través del correo de EE.UU. de Arizona a los estados de la costa este. Vassel y Holt encontraron personas dispuestas a abrir cuentas bancarias y recibir y depositar los fondos ilícitos derivados del contrabando que se vende en los estados de destino. Cada uno de los titulares de cuentas bancarias entonces retiraría el dinero en efectivo en Phoenix y entregaría personalmente el dinero a Vassel, menos honorarios de $300 por transacción.

En abril de 2010, Vassel y Holt fueron condenados a 70 y 36 meses de cárcel, respectivamente, por participar en el contrabando de drogas y la operación de lavado de dinero. Cuatro cómplices más se declararon culpables de violaciones de 18 U.S.C. § 1960, por participar en empresas de transmisión de dinero sin licencia.

Organización de tráfico de drogas de Shawn Falando Smith

En septiembre de 2009, HSI Phoenix recibió información sobre cuentas bancarias que participaban en numerosos depósitos en efectivo de fuera del estado y de retiros por caja posteriores dentro del estado de Arizona. Los depósitos y retiros de las cuentas bancarias se estructuraban para evitar los requisitos de presentación de informes de la BSA. Además, la mayoría de los depósitos se hacían utilizando boletas de depósito de ventanilla lo que lograba un nivel adicional de anonimato. Un análisis más detallado de las cuentas bancarias reveló que un número de individuos desvió más de $2,5 millones en fondos ilícitos a través del sistema financiero. HSI Phoenix observó una discrepancia porque las cuentas bancarias fueron abiertas en sucursales en Phoenix, mientras que la información bancaria mostraba que los titulares de las cuentas residían fuera del estado de Arizona.

HSI Phoenix confirmó que la información personal utilizada para abrir las cuentas bancarias en Phoenix se derivó de víctimas de robo de identidad. El robo de identidad se remonta a Shawn Falando Smith, quien obtuvo copias de los certificados de nacimiento de los varones de la misma edad que las de los que abrían cuentas bancarias en Phoenix de un empleado del condado comprometido en Pennsylvania. Smith y sus co-conspiradores utilizaban los certificados de nacimiento para obtener licencias de conducir de Arizona y luego abrían cuentas bancarias. Los investigadores identificaron a los cinco conspiradores como miembros de una organización de narcotráfico que participaban en una gran operación de tráfico de drogas que utilizaba cuentas bancarias para mover sus fondos a través de los EE.UU. En junio de 2010, todos los sospechosos con excepción de uno de los acusados se declararon culpables y fueron sentenciados a hasta cinco años de prisión por distribución de marihuana, lavado de dinero y robo de identidad.

El camino por seguir

El Departamento de Investigaciones de Seguridad Nacional (HSI en inglés) de Inmigración y Aduana de los EE. UU., ha desarrollado una amplia estrategia nacional para hacer frente a la susceptibilidad de las cuentas de desvío interestatales. Un enfoque integral que abarca la colaboración con la Red Contra los Delitos Financieros (FinCEN) del Departamento del Tesoro de los EE.UU., la industria financiera y el Departamento de Justicia (DOJ) asegurará que se tomará en cuenta esta vulnerabilidad. La estrategia nacional incluye, pero no se limita a lo siguiente:

- Compartir tipologías y lecciones aprendidas con las instituciones financieras;
- Alentar a las instituciones financieras a exigir la identificación de los depósitos en efectivo en cuentas de terceros; e
- Identificar/seguir las cuentas de desvío interestatales basándose en datos de investigación de BSA existentes.

La combinación de las acciones exitosas de ejecución penal, informes presentados según la BSA y el lavado de dinero (ALD), los esfuerzos de cumplimiento de las instituciones financieras fortalecen los sistemas bancarios y obligan a las organizaciones delictivas a buscar otros medios para mover fondos ilícitos. HSI continuará trabajando con las partes interesadas del sector público y privado para identificar las nuevas tendencias y tramas de lavado de dinero y para compartir información, proporcionando indicadores de banderas rojas de alerta, consejos y perspicacia para investigar con mayor eficacia estos ardides delictivos complejos y sofisticados.

Mark A. Witzal, subdirector adjunto, Departamento de Investigaciones de Seguridad Nacional (HSI) de Inmigración y Aduana (ICE) de los EE.UU., Washington, D.C., EE.UU., mark.a.witzal@ice.dhs.gov

Charles Sturt University

Master of Anti-Money Laundering and Counter Terrorist Financing

Charles Sturt University (CSU), in partnership with the Association of Certified Anti-Money Laundering Specialists (ACAMS), offers postgraduate programs that provide specialist anti-money laundering and counter terrorist financing education that will develop the knowledge and skills required to advance your career.

The Master of Anti-Money Laundering and Counter Terrorist Financing (AML-CTF) is the only postgraduate program of its kind being taught at an International university.

The course was developed in consultation with law enforcement, financial regulators, and government agencies with significant input from the finance, banking and corporate sectors in Australia, North America, Europe, Middle East and Asia-Pacific.

This graduate program is delivered by CSU's Australian Graduate School of Policing and Security and incorporates the CAMS certification as an integral part of the coursework required to successfully complete the program. Part-time students can complete the Graduate Certificate in one year, the Graduate Diploma in two years and the Master's degree in three years.

The course is designed to promote best practice in AML-CTF investigation, compliance, prevention and management in the private and public sectors. Subjects are taught via online distance education with interactive sessions and lectures provided by academic,law, criminal justice and industry experts in the AML-CTF field.

STUDY MODE
Distance education

WHEN
Session 1 (March)
Session 2 (July)
Session 3 (Nov)

DURATION
Graduate Certificate: 1 year part-time
Graduate Diploma: 2 years part-time
Master: 3 years part-time

APPLY NOW
www.csu.edu.au/aml

STUDIES COMMENCE IN MARCH, JULY AND NOVEMBER EACH YEAR

Registration is now open. For further information please visit www.csu.edu.au/aml, phone: +61 (2) 993 25212 or email ctung@csu.edu.au.

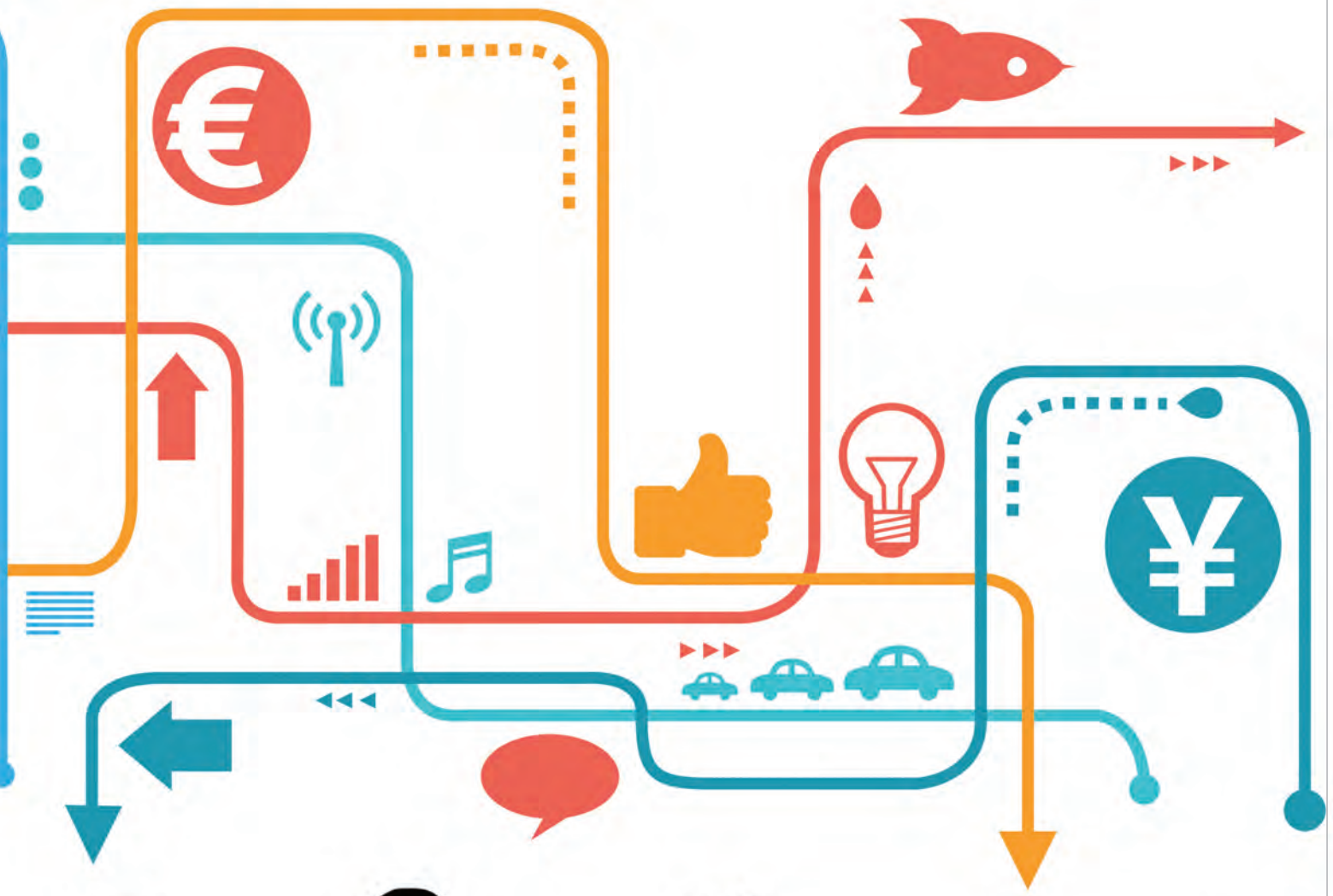
Those who complete the Master Degree through this educational partnership:

- Earn the Certified Anti-Money Laundering Specialist (CAMS) Certification, or if already certified, advanced standing and subject credits in the Master's program.
- Obtain the tools and educational resources to competitively position themselves.
- Contribute to establishing best practices in field, making a lasting impression on the industry.

ACAMS® | Advancing Financial Crime Professionals Worldwide®

El personal de las instituciones financieras:

La primera línea en la lucha contra la trata de personas



La pareja tenía un negocio de alhajas de fantasía que comercializaba desde su casa en Meridian, Idaho, y tenía varias cuentas en las sucursales de Meridian y Boise de dos bancos de cobertura nacional. Enviaban dinero de esas cuentas a los beneficiarios en McAllen y Palmhurst, Texas, en cantidades de $1.000 a $1.700. El marido, posteriormente, hizo numerosos depósitos en las sucursales de bancos dispersos de Wyoming a Alabama. En Idaho, su mujer retiró el dinero poco después de que se acreditaba en una de sus cuentas.[1]

Y el rastro del dinero bien pudo haber terminado, si no fuera por la vigilancia del personal bancario que reportó la actividad financiera la Red Contra los Delitos Financieros (FinCEN). Después de revisar los informes, Investigaciones de Seguridad Nacional (HSI) de Inmigración y Control de Aduanas de los EE.UU. (ICE). inició una investigación y pronto encontró razón para profundizar. Una declaración jurada presentada en una corte federal por un agente especial de ICE HSI detalla lo que encontró y alegó el gobierno; este relato se deriva de la declaración jurada.[2]

El marido y la mujer se encontraban en el país ilegalmente, y la Patrulla Fronteriza de los EE.UU. había detenido al marido y lo había devuelto a su México natal varias veces antes. De manera más alarmante, las transferencias por cable de la pareja en las comunidades fronterizas de Texas, así como a una cuenta en California, fueron enviadas a conocidos traficantes de extranjeros.[3]

TABLA 1. INCIDENTES DE TRATA DE PERSONAS ABIERTOS A LA INVESTIGACIÓN EN LOS EE.UU. POR GRUPOS DE TAREAS FINANCIADOS POR EL GOBIERNO FEDERAL, ENERO 2008 A JUNIO 2010

TIPO DE TRAFICO	CIFRA*	POR CIENTO*
Todos los incidentes	2.515	100,0
Tráfico sexual	2.065	82,1
Prostitución adulta/acto sexual comercial	1.218	48,4
Prostitución o explotación sexual de un menor	1.016	40,4
Labor sexual	142	5,6
Otro	61	2,4
Tráfico Laboral	350	13,9
Labor comercial industrial	132	5,2
Labor industrial no regulada	230	9,1
Otro	26	1,0
Tráfico sospechado	65	2,6
Desconocido	172	6,8

* Las cifras suman más de 2.515 y los porcentajes suman más del 100 por ciento debido a que los incidentes pueden implicar más de un tipo de trata.

Fuente: Banks D and Kyckelhahn T. "Special Report: Characteristics of Suspected Human Trafficking Incidents, 2008 – 2010". NCJ233732. Bureau of Justice Statistics. Office of Justice Programs. U.S. Department of Justice. Accesado el 14 de abril del 2014 en http://www.bjs.gov/content/pub/pdf/cshti0810.pdf.

Trabajando con los registros de instituciones financieras y otras fuentes, el ICE HSI determinó que la pareja les pagaba a contrabandistas para que cruzaran nacionales mexicanos por la frontera. Una vez en los EE.UU., los inmigrantes ilegales le compraban alhajas de fantasía símil-oro al marido, quien luego los llevaba por todo el país en una furgoneta, haciendo que revendieran las joyas en los estacionamientos para pagar los honorarios de los contrabandistas, el costo de la joyería, y el dinero que la pareja invertía en ellos por comida, alojamiento y otros gastos.[4]

La agente especial Stephenie Lord Eisert, jefa de la Unidad de Financiamiento y Ganancias Ilícitas de Delitos de ICE HSI, señala que el caso pone de relieve el papel central del personal de las instituciones financieras en la lucha contra la trata de personas. "El SAR y otros informes que pide la BSA son el alma de nuestro trabajo a la hora de iniciar o ampliar nuestros esfuerzos de investigación", Lord señaló en una reciente entrevista a *ACAMS Today*.[5]

Banderas rojas de alerta de posible trata y tráfico de personas

ICE HSI ha identificado varias actividades y patrones de conducta financieros que pueden indicar que una persona o empresa se encuentra involucrada en el tráfico de personas o la trata, e insta a personal del banco y otros, a tener en cuenta y denunciar esas banderas rojas, que incluyen:[6]

- Depósitos en efectivo estructurados para evitar los informes de transacciones de dinero (CTR), seguido poco después por transferencias electrónicas internacionales salientes;
- Cuentas bancarias de negocios que carecen de los gastos típicos del negocio, o actividad de la cuenta que no se relaciona con el negocio;
- Procesamiento de crédito y débito, por montos uniformes en dólares, cuando dichas cantidades no son habituales para el tipo de negocio;
- Grandes depósitos en efectivo incompatibles con el tipo de negocio;

[1] Declaración jurada presentada para apoyar United States of America vs. Real Property located at 478 West Great Basin Drive, Meridian, Ada County, ID, Case 1:11-cv-00426-REB, United States District Court for the District of Idaho, filed Sept. 13, 2011. Declaración de la Aplicación de Inmigración y Aduana de EE. UU.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Entrevista telefónica de *ACAMS Today* a Agentes Especiales Stephenie Lord Eisert y Michael S. Tutko de la U.S. Immigration and Customs Enforcement, 11 de abril del 2014.
[6] "Project STAMP – Smugglers' and Traffickers' Assets, Monies, and Proceeds". The Cornerstone Report. Agosto del 2013. U.S. Immigration and Customs Enforcement. U.S. Department of Homeland Security. p. 2. Se accedió a él el 12 de abril del 2014 en http://www.ice.gov/doclib/news/library/reports/cornerstone/cornerstone10-1.pdf.

"Los informes SAR y otros informes solicitados de BSA son el alma de nuestro trabajo a la hora de iniciar o ampliar nuestros esfuerzos de investigación".

–Agente especial Stephenie Lord Eisert, jefa de unidad, Unidad de Financiamiento y Ganancias de Delitos, ICE HSI

- Múltiples cuentas establecidas para diferentes empresas, pero con personas con el mismo poder de firma en cada cuenta;
- Uso de las transferencias electrónicas de fondos de cuentas de las empresas para pagar viajes extravagantes y el alquiler de vehículos de alta gama;
- Recepción de numerosas transferencias electrónicas entrantes o cheques personales incompatibles con el tipo de cuenta;
- Transferencias electrónicas de una cuenta a la cuenta de otra empresa cuando las dos entidades carecen de relación comercial aparente;
- Pagos con tarjeta de crédito a los servicios de acompañantes en línea para publicidad, incluidos honorarios pequeños a empresas como Craigslist, así como para empresas publicitarias y sitios anfitriones de la web más caros;
- Grandes pagos a las empresas extranjeras que son incompatibles con la cantidad de producto recibida de ellas;
- Cambio repentino en las prácticas comerciales normales del cliente, tal como un aumento dramático en los depósitos, retiros, o en la fortuna de la que se dispone;
- Depósito de cheques emitidos en cantidades uniformes y con frases aparentemente no aplicables escritas en los comentarios o memorando;
- Transacciones estructuradas de empresas de servicios monetarios (MSB) (múltiples transacciones financieras inferiores a el límite de informes de $3.000 de MSB en el mismo día); y
- Clientes que han denunciado el robo de identidad, ya que muchas empresas delictivas utilizan identidades robadas para facilitar sus actividades.

"La trata de personas, en su núcleo, es un negocio", señala el fiscal de distrito de Manhattan Cyrus R.Vance, Jr., quien ha hecho de este delito una prioridad para su oficina. "Al igual que otras empresas, deja un rastro financiero de papel que se puede controlar y se utiliza para identificar las redes de tráfico", dice Vance, que en abril del 2013 se asoció con Monique Villa, CEO de la Fundación Thomson Reuters con sede en Londres, que convoca un grupo de trabajo internacional grupo sobre los aspectos financieros de la trata de personas.[7]

Tomando un enfoque global, el grupo de tareas integrado por representantes de organizaciones no gubernamentales (ONG) y empresas de servicios financieros, como American Express, Bank of America, Barclays, Citigroup, JPMorgan Chase & Co., TD Bank, Wells Fargo, y Western Union. En enero del 2014, el grupo publicó un informe diseñado para proporcionarles a las instituciones financieras de todo el mundo una guía sobre cómo identificar e informar de las transacciones financieras que pueden ser indicativas de la trata de personas.[8]

Villa, el CEO de la Fundación Thomson Reuters, dijo a *ACAMS Today* que las banderas rojas se citan en el documento confidencial incluyen "fondos de las cuentas de los empleados que remontan al empleador (indicativo de tráfico laboral), transacciones comerciales recurrentes que tienen lugar fuera del horario conocido de operaciones del negocio, transferencias transfronterizas de fondos incompatibles con el objetivo social declarado de los clientes de la institución financiera, y otros que no pueden ser revelados por razones de seguridad. Si queremos tener una oportunidad para debilitar a los traficantes, es esencial que las principales instituciones financieras del mundo se encuentren a bordo".[9]

La trata de personas en números

Como con cualquier actividad ilícita, es extremadamente difícil cuantificar el alcance de la trata de personas, pero la Oficina de las Naciones Unidas contra la Droga y el Delito (UNDOC) estimó en 2012 que la trata de personas genera $32 mil millones al año y atrapa a aproximadamente 2,4 millones de víctimas en todo el mundo en un momento dado.[10,11]

En varios de sus últimos informes anuales sobre la trata de personas, el Departamento de Estado de los EE.UU. (DoS) ha estimado que entre 600.000 y 900.000 personas son traficadas a través de las fronteras internacionales cada año.[12] En 2003, el DoS estimaba que entre 18.000 y 20.000 ciudadanos extranjeros eran objeto de la trata en los EE.UU. cada año, mientras que un informe federal del año siguiente puso la cifra entre 14.500 y 17.500.[13,14] El gobierno no ha publicado estimaciones más recientes, y es importante tener en cuenta que estas cifras se refieren únicamente a los nacionales extranjeros llevados a los EE.UU., y no a los ciudadanos o residentes que son objeto de trata en el país.

Las estadísticas sobre las investigaciones y los enjuiciamientos proporcionan cifras concretas, pero, por supuesto, es imposible saber qué porcentaje de los incidentes de tráfico en general representan estos casos. En el año fiscal 2012, el Departamento de Justicia (DOJ) informó que su grupo de tareas llevó a cabo 753 investigaciones de casos relacionados con la trata de personas — frente a más de 900 investigaciones en el año fiscal 2011, mientras que ICE HSI, que forma parte del Departamento de Seguridad Nacional

[7] "Manhattan DA Cyrus Vance Jr., Thomson Reuters Foundation CEO Monique Villa, Top U.S. Financial Institutions Issue White Paper to Combat Human Trafficking Using Financial Data". Thomson Reuters Foundation. 10 de enero del 2014. Accesado el 20 de marzo del 2014 en http://www.trust.org/item/20140110101411-vphyw/.
[8] Ibid.
[9] Comunicación de correo electrónico a *ACAMS Today*, 15 de abril del 2014.
[10] "Debemos redoblar nuestros esfuerzos para terminar el tráfico humano , dice el Presidente de la Asamblea General de la ONU".United Nations Office on Drugs and Crime. April 10, 2012. Accesado el 13 de abril del 2014 en http://www.unodc.org/lpo-brazil/en/frontpage/2012/04/03-we-must-redouble-efforts-to-end-human-trafficking.html.
[11] "U.N.: 2.4 million human trafficking victims". USAToday.com. 3 de abril del 2012. Accesado el 13 de abril del 2014 en http://usatoday30.usatoday.com/news/world/story/2012-04-03/human-trafficking-sex-UN/53982026/1
[12] "Human Trafficking Statistics". Polaris Project. Accesado el 12 de abril del 2014 en http://www.cicatelli.org/titlex/downloadable/human%20trafficking%20statistics.pdf.
[13] Trafficking in Persons Report. U.S. Department of State. Junio del 2003. Accesado el 15 de abril del 2014 en http://www.state.gov/j/tip/rls/tiprpt/2003/.
[14] Assessment of U.S. Government Efforts to Combat Trafficking in Persons. Junio del 2004. U.S. Department of Justice. Accesado el 13 de abril del 2014 en http://www.justice.gov/archive/ag/annualreports/tr2004/us_assessment_2004.pdf.
[15] "Trafficking in Persons Report". U.S. Department of State. Junio del 2013. Accesado el 15 de abril del 2014 en http://www.state.gov/j/tip/rls/tiprpt/countries/2013/215645.htm.

(DHS), informó investigar 894 casos posiblemente de la trata de personas, frente a los 722 casos del año anterior.[15]

Los fiscales federales aseguraron 138 condenas contra tratantes en el año fiscal 2012, en comparación con 151 condenas del año fiscal anterior. Ciento cinco de las condenas en el año fiscal 2012 involucraban predominantemente el tráfico sexual, mientras que el tráfico laboral fue el delito predominante en los otros 33 casos.[16]

Una revisión del DOJ de incidentes sospechosos de la trata de personas del 2008 hasta mediados del 2010 encontró que, en el transcurso de 30 meses, los grupos de tareas que reciben fondos federales iniciaron investigaciones en 2.515 incidentes sospechosos. El treinta por ciento de los incidentes que se han abierto durante al menos un año, o aproximadamente 750 casos, fueron confirmados como trata de personas, mientras que se confirmó que en el 38 por ciento no se trata de personas, y 32 por ciento quedó abierto al finalizar el período de estudio.[17]

Entre los 389 incidentes confirmados como de trata de personas para los que se disponía de datos amplios, el informe encontró que:[18]

- El 62 por ciento de las víctimas del tráfico laboral tenía 25 años o más, comparado con el 13 por ciento de las víctimas de tráfico sexual.
- Las víctimas de tráfico sexual tenían más probabilidades de ser negras (40 por ciento) o blancas (26 por ciento), en comparación con las víctimas del tráfico laboral, que eran más propensas a ser hispanas (63 por ciento) o asiáticas (17 por ciento).
- El 83 por ciento de las víctimas de tráfico sexual eran ciudadanas de los EE.UU., mientras que el 67 por ciento de las víctimas del tráfico laboral eran indocumentados extranjeros y el 27 por ciento eran extranjeros calificados.

Mientras tanto, el Polaris Project (Proyecto Polaris), una organización sin fines de lucro con sede en Washington, dedicada a la lucha contra la trata de personas, informa que entre diciembre del 2007 y diciembre del 2012, su National Human Resource Center (NHTRC) recibió informes de 9.298 casos singulares de la trata de personas emergiendo de más de 72.000 llamadas, correos electrónicos y presentaciones en su formulario en línea.[19]

El poder que da la asociación

ICE HSI hace hincapié en la importancia de la asociación de los que aplican la ley y la industria financiera en contra del trafico de personas y la trata de personas. La iniciativa Cornerstone de la agencia lleva a cabo investigaciones en una amplia gama de delitos financieros, incluyendo la trata de personas y el contrabando, mientras que su Project STAMP (Activos, Dinero y Ganancias de Contrabandistas y Traficantes) se dedica a la lucha contra las organizaciones delictivas transnacionales (TCO) que participan en esas actividades siguiendo los rastros que crea el dinero.

Lanzado en 2010, Project STAMP es una iniciativa en la que, "HSI colabora con sus socios del sector privado para evaluar cómo las organizaciones [delictivas transnacionales] utilizan el sector financiero en el país y en el extranjero para cobrar por los servicios ilegales y compartir estos métodos con la comunidad financiera para cerrar vulnerabilidades explotables".[20]

Lord señaló que, "Durante el próximo año, vamos a reunirnos con los miembros de la industria bancaria y la comunidad financiera mayor para compartir con ellos las más recientes tipologías y los flujos financieros que hemos identificado. Proporcionaremos más detalle que nunca antes".[21]

Antes de esa reunión, Lord y el agente especial Michael S. Tutko, jefe de sección de la unidad de Contrabando y Tráfico Humano de ICE HSI, enfatizó a *ACAMS Today* que es importante que el personal de la industria financiera aprecie la distinción entre el trafico de personas [contrabando] y la trata de personas, y esté al tanto de las tendencias y los factores asociados con cada uno.[22]

Tutko explicó que el contrabando consiste en traer personas a los EE.UU., violando las leyes de inmigración, y también puede conllevar albergar extranjeros una vez que están en el país y transportarlos dentro de los EE.UU.; la trata involucra la explotación de las personas, ya sean extranjeros llevados a los EE.UU. para ese fin o que ya viven aquí como ciudadanos o residentes. La mayor parte del tráfico se caracteriza por ser tráfico sexual o laboral. El tráfico sexual implica

[16] Ibid.
[17] Banks D and Kyckelhahn T. "Special Report: Characteristics of Suspected Human Trafficking Incidents, 2008 – 2010". NCJ233732. Bureau of Justice Statistics. Office of Justice Programs. U.S. Department of Justice. Accesado el 14 de abril del 2014 en http://www.bjs.gov/content/pub/pdf/cshti0810.pdf.
[18] Ibid.
[19] "Human Trafficking Trends in the United States". The Polaris Project. Accesado el 13 de abril del 2014 at http://www.polarisproject.org/resources/hotline-statistics/human-trafficking-trends-in-the-united-states.
[20] "Project STAMP – Smugglers' and Traffickers' Assets, Monies, and Proceeds". The Cornerstone Report. Agosto del 2013. U.S. Immigration and Customs Enforcement. U.S. Department of Homeland Security. p. 2. Accesado el 12 de abril del 2014 en http://www.ice.gov/doclib/news/library/reports/cornerstone/cornerstone10-1.pdf.
[21] *ACAMS Today* telephone interview with U.S. Immigration and Customs Enforcement Special Agents Stephenie Lord Eisert and Michael S. Tutko, 11 de abril del 2014.
[22] Ibid.

el uso de la fuerza, la coacción o el fraude para inducir a un adulto a participar en actos sexuales comerciales, o transportar a un menor de edad al país o en el país para el comercio sexual. El tráfico laboral, por su parte, implica el uso de fraude, la fuerza o la coacción para inducir a una persona a trabajar en la servidumbre involuntaria, peonaje, servidumbre por deudas, o condiciones que podrían considerarse esclavitud.[23]

Lord señaló que, "En el pasado, los contrabandistas solían retener a la gente en casas seguras cerca del punto en el que habían entrado en los EE.UU. hasta satisfacer la deuda de contrabando. Como resultado, muchas de las transacciones financieras indicativas de contrabando involucraban los MSB o bancos en Texas, Arizona y el sur de California. Ahora estamos viendo más una huella nacional. Los extranjeros son trasladados a sus destinos finales dentro de los EE.UU., y desde esos lugares, los depósitos anónimos en efectivo se hacen en las ventanillas de la sucursal local de un banco con oficinas en todo el país. Un intermediario del contrabandista entonces retira el dinero de la cuenta domiciliada en otro lugar en los EE.UU".[24]

La agente especial de ICE HSI añadió que las cuentas canalizadoras interestatales que facilitan este enfoque están recibiendo mayor escrutinio por parte de los agentes federales del orden público, y alabó a las instituciones financieras por trabajar para combatir el uso de este tipo de cuentas para fines delictivos. Como ejemplo, señaló que JPMorgan Chase está impidiendo que se hagan depósitos por ventanilla de personas no pre-identificadas como asociadas con una cuenta en particular.[25]

Los agentes de ICE HSI también observaron que, si bien el trafico y la trata de personas puede involucrar extranjeros desde cualquier parte del mundo, muchos de los casos recientes se han centrado en gente traída a los EE.UU. desde México y en otras partes de Centroamérica, así como de Asia del Sur y el Este de Asia. Del mismo modo, las agencias gubernamentales y organizaciones sin fines de lucro que luchan contra la trata notan que si bien una amplia variedad de industrias puede dar cobertura a la delincuencia, las empresas que pueden justificar una vigilancia especial incluyen salones de belleza, salones de masajes, clubes de striptease, agencias de viajes, servicios que reclutan y colocan niñeras y otros trabajadores domésticos, y las entidades que emplean trabajadores agrícolas y otros trabajadores manuales.[27,28]

Lord añadió que era importante que la gente que trabaja en los bancos y otras empresas de servicios financieros no subestimen la importancia de su contribución a la lucha contra la trata de personas. "Entiendo que el personal del banco a menudo se pregunte qué pasa después de haber presentado un informe, si su esfuerzo realmente hace una diferencia. Si hay una cosa que podría transmitir, es que se revisó cada SAR. Tenemos equipos dedicados a ese esfuerzo. En algunos casos, se inició una investigación debido a un SAR en especial o porque varios informes relacionados con un individuo o negocio acumulan y sugieren cierto patrón de actividad. En otros casos, se inicia una investigación por otra razón, y nos basamos en los informes como parte de la investigación. Pero independientemente de que los informes nos llevan a abrir una investigación, o contribuyen a una ya en marcha, son fundamentales para el éxito que hemos tenido en la lucha contra la trata de personas y otros delitos".

Tom Garry, CAMS, socio de ACAMS Grupo especial de edición, presidente de Exponent Communications, Hawthorne, NJ, EE.UU., thomasmgarry@gmail.com

Cómo se puede colaborar con ICE HSI para combatir la trata de personas?

Como parte de su esfuerzo para colaborar con la comunidad financiera en la lucha contra la trata de personas (HT), Investigaciones de Seguridad Nacional (HSI) de Aplicación de Inmigración y Aduana de los EE.UU. (ICE) invita a los bancos y otras empresas de servicios financieros a participar en su programa Cornerstone de varias maneras, incluyendo:

1. **Asociarse** — Hacerse socio del sector privado contactando al agente local de la oficina HSI Especial a Cargo (SAC) para programar una presentación Cornerstone para su empresa u organización;
2. **Informar** — Informar actividad comercial y empresariales sospechosas contactando a su oficina local de HSI SAC o llamando al 1-66-DHS-2-ICE; y
3. **Anotarse** — Anótese para recibir el boletín trimestral de HSI, The Cornerstone Report, para estar al día sobre los nuevos desarrollos en los delitos de fraude financiero y comercial. Usted puede anotarse para recibir el boletín de noticias en http://www.ice.gov/cornerstone/.

[23] Ibid.
[24] Ibid
[25] Ibid
[26] Ibid.
[27] "Trafficking in Persons Report". U.S. Department of State. Junio del 2013. Accesado el 15 de abril del 2014 en http://www.state.gov/j/tip/rls/tiprpt/countries/2013/215645.htm.
[28] "Human Trafficking Trends in the United States". The Polaris Project. Accesado el 13 de abril del 2014 en http://www.polarisproject.org/resources/hotline-statistics/human-trafficking-trends-in-the-united-states.

MALTRATO DE ANCIANOS:

Salir de las sombras al centro de atención de la aplicación de la ley

El maltrato de ancianos ha sido durante mucho tiempo un crimen sin denuncias. Pero los reguladores, los organismos policiales y los fiscales están volcando su atención a este crimen y sacándolo de las sombras para que sea más fácil que los ancianos víctimas denuncien el delito y busquen justicia. Mediante la comprensión de por qué las víctimas son renuentes a denunciar el delito y de cómo construir un caso cuando se trata de víctimas de edades avanzadas y, a menudo frágiles, los agentes encargados de hacer cumplir la ley pueden hacer que las sombras se alejen aún más.

El maltrato de ancianos puede ser físico, mental, sexual o financiero, pero este artículo se centra en la explotación económica de las personas mayores. Este es el tipo de maltrato que el personal del antilavado de dinero (ALD) y las agencias de las autoridades que aplican la ley que se ocupan de fraudes y delitos financieros tienen más probabilidades de encontrar.

Encendiendo el proyector

Se tomó un paso importante en la presentación de informes y la lucha contra el maltrato de ancianos en febrero del 2011, cuando la Red de Contra los Delitos Financieros (FinCEN) publicó un *Aviso a las instituciones financieras sobre la presentación de informes de actividad sospechosa relacionada con la explotación financiera de los mayores.* La advertencia incluye una lista de banderas rojas de alerta que podrían indicar maltrato financiero de ancianos y pidió también que el término "explotación financiera del anciano" se incluyera en las narraciones de los informes de actividades sospechosas (SAR) que notifican el crimen.

El asesor dijo que, "el análisis de los SAR que informan sobre la explotación financiera de ancianos puede proporcionar información crítica sobre fraudes específicos y tendencias potenciales, y puede poner de relieve los abusos perpetrados contra los ancianos". Ambas instituciones financieras responsables de la presentación de SAR y agentes de la ley que utilizan la información proporcionada en los documentos se benefician de analizar los datos y de estar familiarizados con las banderas rojas de maltrato a personas mayores. Las banderas rojas mencionadas por FinCEN incluyen:[1]

- Grandes retiros frecuentes de cuentas financieras, incluyendo retiros máximos diarios en moneda de un cajero automático;
- Súbita actividad insuficiente de fondos;
- Transacciones de débito incoherentes con el comportamiento pasado de la persona;
- Envío por cable o intentos de hacerlo por grandes cantidades de dinero;
- Cierre de cuentas sin considerar sanciones; y
- Cambio repentino de la gestión financiera del cliente anciano; por ejemplo, el individuo cambia el poder a un miembro diferente de la familia o a alguien nuevo.

Las estadísticas publicadas en la entrega de mayo del 2013 de *SAR Activity Review—Trends, Tips & Issues* de FinCEN muestran que el asesor está haciendo una diferencia. FinCEN informó que durante el período de seis meses antes del asesoramiento, se presentaron 806 SAR con los términos "explotación financiera de un anciano" y "maltrato financiero de ancianos" en comparación con 2.161 SAR, durante los seis meses siguientes a la consulta.[2]

El informe también analiza los tipos de explotación financiera reportada y encontró que los crímenes fueron más a menudo perpetrados por un familiar o un cuidador de la víctima. Este hecho es una de las razones que subyacen a tantos crímenes de abuso de ancianos no se denuncian.

Por qué las víctimas no denuncian

Aunque los más de los casos se reportan y procesan, muchos todavía permanecen en las sombras. El Centro Nacional sobre el Maltrato de Ancianos (NCEA, por sus siglas en inglés) informa que un estudio llevado a cabo "estima que sólo uno de cada 14 casos de maltrato a personas mayores llega a conocimiento de las autoridades" y que el Estudio de Prevalencia del Maltrato de Mayores del Estado de Nueva York encontró que "por cada caso conocido por los programas y agencias, 24 eran desconocidos".[3]

La comprensión de las razones por las que los ancianos víctimas guardan silencio puede ayudar a los agentes del orden público durante una investigación. Las razones más comunes son:

- El delito fue perpetrado por alguien que la víctima conoce y en quien confía y la víctima teme que la denuncia del delito enviará a su ser querido a la cárcel;
- El miedo a las represalias por parte del perpetrador;
- La vergüenza, en los casos en que la víctima fue engañada por una estafa y cayó en la trampa;
- Si el autor es el cuidador principal de la víctima, el miedo a que la víctima tendrá que mudarse a un centro de atención sin el cuidador;
- Si el agresor es un miembro de la familia con quien la víctima vive, la víctima teme perder su casa; y/o
- La víctima está cognitivamente alterada y no puede informar del maltrato.

Abordar estas preocupaciones durante una entrevista e investigación puede hacer que sea más fácil para las personas de edad víctimizadas proporcionen información. Si es apropiado y aceptable en su estado, busque un defensor legal para la víctima.

La construcción de un caso mejor

Las mismas razones que impiden que las víctimas denuncien también hacen que sea difícil para las fuerzas del orden armar un caso y para que los fiscales lo lleven a los tribunales. Saber cómo trabajar con las víctimas de edad avanzada para construir su caso es esencial.

En su folleto de 46 páginas *Prosecuting Elder Abuse Cases Basic Tools and Strategies (Enjuiciamiento de casos de maltrato de ancianos: herramientas básicas y estrategias)*, el Centro Nacional para Tribunales Estatales (NCSC) ofrece orientación detallada tanto a las fuerzas del orden como a los fiscales.[4] En el folleto, el NCSC recomienda que pruebas y testimonios se recojan y conserven "usando métodos que mejoren la probabilidad de admisibilidad en un juicio si el anciano no pueda o quiera atestiguar". El folleto también recomienda que se reúnan el investigador y la víctima en la casa de ésta y que hable con la víctima de uno-a-uno para asegurarse de que la víctima está separada del agresor y posibles testigos del delito.[5]

Además, para aliviar los temores y hacer que el anciano víctima se sienta más cómodo al hablar del delito, la *Guía de capacitación sobre el maltrato de mayores* de la ciudad de Nueva York asesora a los investigadores así:[6]

- Pida permiso para sentarse cerca de la víctima.
- Siéntese a nivel visual con la persona durante la entrevista.
- Recuerde que las personas mayores pueden necesitar tiempo para procesar y responder una pregunta. Asegúrese de darles el tiempo que necesitan. Al hacer una pregunta, hable despacio y con claridad.
- Haga una pregunta a la vez.
- Mantenga las armas fuera de la vista.
- Diríjase a la persona por su apellido.
- Deje que la víctima sepa que su principal preocupación es su bienestar.

Conclusión

El maltrato de ancianos es un delito horrible que está pasando a la vanguardia de los esfuerzos de aplicación de la ley. Aunque se han dado pasos para investigar y enjuiciar estos delitos, todavía hay demasiados que no llegan a comunicarse. El maltrato de ancianos es un delito que deberíamos todos, ya sea personal de cumplimiento responsable de informar, agentes encargados de hacer cumplir la ley responsables de la investigación o fiscales responsables de llevar a juicio, estar buscando y estar dispuestos a hacer nuestra parte para combatirlo.

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

[1] Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation. FinCEN, February 22, 2011. http://www.fincen.gov/statutes_regs/guidance/html/fin-2011-a003.html

[2] SAR Activity Review – Trends, Tips& Issues, FinCEN, May 2013 http://www.fincen.gov/news_room/rp/files/sar_tti_23.pdf

[3] National Center on Elder Abuse, http://www.ncea.aoa.gov/Library/Data/index.aspx

[4] *Prosecuting Elder Abuse Cases Basic Tools and Strategies* National Center for State Courts, http://www.eldersandcourts.org/Elder-Abuse/~/media/Microsites/Files/cec/Prosecution%20Guide.ashx

[5] National Center on Elder Abuse, http://www.ncea.aoa.gov/Library/Data/index.aspx

[6] Interviewing Elderly Victims and Witnesses, NYC Elder Abuse Training Project, 2004, www.NYC.gov

Customised analysis for risk assessment and documentation

I N P U T

Company financials | Company descriptions | Financial strength data | Beneficial owners | PEPs & Sanctions | Directors & managers | Adverse data | Original documents | Adverse news | Exchanges | Share-holdings & subsidiaries | Regulators

Valuable compliance critical datasets

compliance catalyst

- Streamline your on-boarding process
- Analyses and ranks risk
- Screens across corporate groups
- Automates processes
- Provides an audit trail
- Saves you time and improves your efficiency

You can:

- Add attachments
- Capture screen grabs
- Prioritise your research resource
- Annotate
- Create customised models and processes
- Manage your workflow
- Get a dashboard view on the status of your research

A purpose built platform

Your bespoke Compliance Documentation

Professional, secure hard copy and electronic reporting

O U T P U T

Compliance Catalyst is a process and data driven compliance tool. Combining company information from Bureau van Dijk with other compliance-critical data sets, it automates steps in your on-boarding process, analysing various types of potential risk.

BUREAU VAN DIJK

bvdinfo.com/compliance

bvd@bvdinfo.com 020 7549 5000

Renacimiento del FRAUDE

Goran Bogicevic / Shutterstock.com

Como ex agente especial de Investigación Criminal (CI) del IRS, estuve en el negocio de la caza de defraudadores, grandes estafadores y ladrones de cuello blanco. El deporte no era para los detectives financieramente débiles de corazón. Aquellos dignos de captura y enjuiciamiento camuflaban bien senderos de dinero falso con astucia, encanto y un grueso barniz. Como cazadores dedicados, estudiamos y tratamos de predecir su comportamiento, buscamos sus cotos de caza y los acechamos pacientemente antes de que cometieran otro crimen financiero. La satisfacción personal de que ya no victimizaría a otros era el preciado trofeo por agarrar a un gran estafador.

Descontando la horrible experiencia de sufrir robos o asaltos, el robo de los ahorros por alguien en quien se pensaba que se podía confiar, a menudo deja una cicatriz emocional muy profunda. En mi experiencia he visto que estas víctimas se sienten perseguidas por el resto de sus vidas, y rara vez se recuperan económica o psicológicamente.

Durante los años de agente especial y más tarde como líder de alto rango en la organización, me he puesto más a tono con la actividad de los estafadores. Como sucede con la mayor parte de los que se encuentran en esta línea de trabajo, se empieza a desarrollar un sexto sentido. Digo esto para calificar lo que voy a decirle: La gente puede llegar a hartarse. No puedo evitar quedar influido por los años de forzar ciertas miradas. Admito que puedo haber desarrollado un prejuicio de etiquetar individuos como defraudadores. Por lo tanto, sea usted el juez si mis observaciones se hacen a través del prisma del escepticismo.

Me han causado alarma varias tendencias convergentes recientes: En primer lugar, el avance exponencial de las oportunidades para que un defraudador encuentre presas y pueda reproducirse; en segundo lugar, el crecimiento explosivo en el tamaño y la cantidad de casos delictivos de fraude; y en tercer lugar, el grupo de recursos en rápida disminución de los investigadores y fiscales en la tarea de luchar contra los delitos financieros sofisticados. Nos encontramos en un renacimiento del fraude en el que nunca ha sido más fácil cometer robos financieros y salirse con la suya.

Abundan las oportunidades

Dejando un cajón de caja registradora sin llave deja claramente un negocio abierto al delito de peculado. Con el fraude, a veces nuestros cajones de cajas registradoras quedan muy abiertos por credulidad, avaricia o desesperación. Donde existen oportunidades, cometer fraude puede ser más fácil de lo que uno cree. Hubo un caso en mi oficina hace tiempo en que un hombre puso un anuncio en el diario que la publicidad si usted le enviaba $50 él le enviaría un paquete educativo que le enseñaría cómo ganar $1.000 por semana. Varias víctimas le enviaron cheques y, como había prometido, el estafador les mandó el secreto para el éxito: una breve carta diciéndoles que pusieran un anuncio en el diario pidiéndole a la gente que les enviara $50 como él hacía.

Los EE.UU. han tenido una larga historia de estafadores que venden ardides y medicamentos falsos. Hasta finales de 1990, estos estafadores tenían limitaciones de ladrillo y mortero que limitaban hasta dónde su ardid podía extenderse. Por ejemplo, un ardid de telemarketing se limitaba al tamaño de la sala de calderas; un envío postal masivo de una inexistente cura para el dolor se vio limitada por el coste de envío y de la correspondencia y un publirreportaje que proponía minas de oro falsas tenía una barrera empinada dado el costo de producción y el tiempo de aire de la televisión.

Pero la popularidad general de Internet cambió todo. Ahora existen oportunidades inimaginables que hacen que el costo de engañar a las víctimas resulta mucho más barato y se puede hacer en el anonimato del ciberespacio. Además, las características de los autores del fraude (engaño y encanto) pueden atenuarse vastamente. Cuando se trata de Internet, los estafadores pueden presentarse como un negocio bien establecido, usando sólo un diseño de web bien hecho.

El Internet ha permitido los fenómenos de *micro fraude* donde ahora resulta muy rentable estafar a cientos de miles por pequeñas cantidades. Mi oficina trabajó en un caso en que el estafador estafó a cientos por millones de dólares de muchos individuos cada uno de los cuales perdió entre 25 a 150 dólares. Imagine las posibilidades del anuncio de la estafa del diario que mencioné antes, cuando se la transfiere a correos electrónicos no deseados y utilizando sitios web que permiten el anonimato. Y con esta nueva presencia cibernética global, los defraudadores pueden llegar a las víctimas en cualquier lugar del mundo desde la comodidad de su cibercafé. Con el Internet el mundo es su campo de acción.

Nuestro afán de hacer que las transacciones sean convenientes y sin problemas a través de la tecnología ha abierto nuevas oportunidades que los estafadores están explotando enérgicamente. El robo de identidad es un claro ejemplo de esto. Además del fraude de tarjetas de crédito, miles de millones de dólares se han pagado en los últimos años a los ladrones que roban la identidad y número de seguro social de los contribuyentes desprevenidos y luego presentan declaraciones de impuestos en línea. Se ha vuelto tan lucrativo que las pandillas y otros grupos delictivos lo han convertido sin reparo en una de sus fuentes de ingresos principales. Lo que lo hace atractivo y seguro para los

ladrones es que los reembolsos se pueden recibir en las tarjetas de débito prepagas por lo que no hay rastro del dinero en los bancos.

El IRS está haciendo un buen trabajo en combatir el problema, pero nunca ha experimentado tal epidemia de delitos relacionados con el robo de identidad. Y todo esto es principalmente el resultado de que los funcionarios electos esperan que los reembolsos sean convenientemente pagados en el breve período de 24 a 48 horas. Además, el IRS no es la única agencia gubernamental en sufrir el robo de identidad de manera épica. Cualquier programa de gobierno local, estatal o federal que paga los fondos de utilización de tarjetas de débito prepagas ha sufrido ataques de los ladrones de identidad. Logramos capturar un pequeño grupo de individuos que fueron capaces de obtener 4 millones de dólares en beneficios de desempleo falsos todos pagados sobre las tarjetas prepagas.

Además de las consideraciones tecnológicas y de conveniencia, los cambios demográficos también abren nuevas oportunidades. A medida que la población envejece, los *baby boomers* se jubilan con ahorros menores de lo que imaginaron y por desesperación algunos buscan oportunidades de inversión no convencionales más enérgicas. A medida que las personas envejecen se vuelven más confiadas y olvidadizas y todo esto le resulta favorable para mejorar las oportunidades de los estafadores.

Ataques de defraudadores zombis

Cuando comencé la carrera, los grandes casos no se entregaban en bandeja de plata. Uno tenía que trabajar para ello, profundizar y levantar un buen número de rocas financieras. El desarrollo del caso constituía la orden del día para ser un buen agente especial. Pero ha habido un cambio notable en los últimos años. Los agentes ya no necesitan buscar constantemente bajo piedras incrustadas profundamente para encontrar una pista de calidad. Esto se debe a que los grandes casos han sido saliendo de debajo de las piedras últimamente.

Justo antes de jubilarme, el valor agregado de las investigaciones bajo mi dirección en los últimos años se acercó a mil millones de dólares. Muchos de estos casos superaron los $10 millones y hubo unos cuantos por más de $200 millones. La inflación no puede explicar la enorme variación en el inventario de una oficina de tamaño similar hace apenas una década. En todo el país, referencias, consejos y súplicas apasionadas de las víctimas están llegando a los investigadores de delitos de cuello blanco mucho más rápidamente de lo que pueden ingresar. Digan que estoy harto, pero algo anda mal en las carreteras financieras de los EE.UU. Es casi como si hubiera un levantamiento de zombis defraudadores.

Las limitaciones presupuestarias a nivel local, estatal y federal también entran en juego en esto. Hay menos investigadores y fiscales con experiencia en delitos financieros sofisticados que en años anteriores. Por ejemplo, la CI del IRS se está acercando a los niveles de dotación de personal de 1970. Esto debería ser una señal de alerta porque los agentes especiales del IRS a menudo son invocados por los fiscales federales para construir las investigaciones financieras más sofisticadas.

Para gestionar el inventario desbordante de delitos financieros con menores recursos, muchas pistas potenciales que se habrían trabajado hace años se pasan por alto por otras mayores. Los fiscales están obligados a establecer criterios más elevados en dólares como un medio para garantizar que los delincuentes de mayor impacto sean juzgados. Los resultados son desconcertantes. No es raro que un defraudador de un cuarto de millón de dólares sea devuelto al mundo de la estafa por ser una pesca demasiado pequeña en muchas ciudades importantes dado el límite del tamaño de la pesca del investigador financiero. En algunas áreas, si el fraude es por menos de un millón de dólares existe la posibilidad de que no será procesado si los peces gordos ya están en el trasmallo del barco.

Tenga en cuenta que toma mucho más tiempo pescar y montar en la pared de la fiscalía los casos de cuello blanco sofisticados. El esfuerzo es más parecido a la pesca marina en alta mar que la pesca del bagre con red. Estos grandes casos son enormes sumideros de recursos y a menudo toma todo un equipo de agentes y abogados para llevarlos a juicio. Con una prioridad para garantizar la seguridad pública, muchos departamentos de policía locales y estatales más pequeños no pueden financiar las unidades de investigación de delitos de cuello blanco adecuados, por lo que los ceden a las agencias penales federales.

Los romanos tienen un dicho: *El dinero es como el agua de mar. Cuanto más se bebe, más sed da.* Los estafadores vívidamente comprueban este axioma. A diferencia de los criminales violentos hay una alta tasa de reincidencia a medida que los estafadores envejecen. A menudo se hacen más atroces y rapaces en sus robos financieros, tratando de calmar su sed de codicia. No es raro ver los esquemas de Ponzi perpetrados por personas de setenta años e incluso algunos de ochenta.

Racionalización

Lo que impide que la mayoría de nosotros cometamos fraude es nuestra brújula moral. Es revelador que los estudios sobre el engaño demuestran que una porción significativa de entre nosotros se saldría del camino ético si pudiéramos racionalizar la acción. El factor importante en la racionalización tiene que ver con la mentalidad del grupo. Si usted percibe que todos lo hacen, se siente más cómodo racionalizando su acción como un comportamiento aceptable. La crisis de las hipotecas se basó en parte en el hecho de que mucha gente racionalizó que estaba bien presentar un préstamo hipotecario hinchado con datos financieros ficticios. En su mente todo el mundo lo estaba haciendo y nadie se metió en problemas por ello. A medida que más personas se salen con la suya, habrá aquellos que racionalizan que está bien seguir al grupo, sobre todo si está impulsado por la desesperación financiera.

La racionalización es a menudo mayor si una persona no tiene ningún apego emocional a la víctima. Aquí es donde se pone de miedo. Como ya he mencionado, el Internet ha abierto enormes oportunidades no sólo para los estafadores de casa, sino también para los grupos extranjeros nefastos como los terroristas, las organizaciones delictivas transnacionales y las cleptocracias, a las que no les podría importar menos el modo de vida de las personas. Nuestros enemigos también están involucrados en la guerra financiera.

¿Qué significa esto para el cumplimiento del ALD?

Con las fuertes multas recientes por cientos de millones a las instituciones financieras, el gobierno ha dejado en claro que lo que espera de los programas de ALD es detectar e informar sobre los delitos financieros: el fraude. Las fuerzas del orden no pueden mantenerse al día con el crecimiento exponencial de los casos de delincuencia financiera; por lo tanto, a las instituciones financieras se les pide hacer más en la lucha contra el fraude financiero. Esto significa que los programas de ALD tendrán que ser reestructurados y las instituciones financieras, sin duda, se enfrentarán a nuevos retos y expectativas.

La Ley de Secreto Bancario (BSA, por sus siglas en inglés) fue creada en la década de 1970 para monitorear y reportar las transacciones financieras que se producen en la economía subterránea de dinero en efectivo, no bancarizado. Gran parte del aparato del ALD se centra en la detección de la actividad tradicional sospechosa basada en el uso de efectivo. El mundo delictivo ha cambiado enormemente desde entonces. La mayoría de los delitos financieros significativos no se basan en el uso de efectivo. Los estafadores a menudo no aprovechan las técnicas de lavado de activos basados en efectivo utilizadas por los cárteles y otras organizaciones de narcotráfico. Por ejemplo, las instituciones financieras están sufriendo una ola de estafadores que intentan compensar operaciones de crédito o débito en relación con una multitud de ardides de fraudes. Y hay estafadores que sólo utilizan las instituciones financieras simplemente para disfrutar de sus fondos no en efectivo en lugar de lavar el dinero.

Así que, cuando se trata de detectar a los defraudadores es principalmente acerca de los protocolos de diligencia debida y se trata de mantenerse al tanto de las últimas tramas de fraude. Hay un mito que albergan muchas personas: Sólo los tontos, codiciosos y crédulos resultan estafados. Les aseguro que no es mi experiencia en la carrera de representante de la ley. Los estafadores están codificados genéticamente para ser encantadores totales, maestros en armar mentiras que parecen grabadas en piedra. He visto a médicos, abogados, ingenieros y profesores universitarios caer en su engaño. Si estos profesionales de alto nivel pueden ser presa, imagine lo difícil que será para el personal de ALD detectar su fraude.

Hay un alto grado de subjetividad en evaluar si una persona participa en un fraude, en especial si hay una gruesa capa protectora de sofisticación. En el futuro, tenemos que lidiar con el hecho, no vamos a atraparlos a todos. Las grietas en la pared del ardid sólo se harán patentes mucho más tarde en la maniobra de fraude y, a menudo después de que ha habido una notificación pública de la condena.

Incluso contactar a las víctimas para verificar el fraude podría ser menos fructífero de lo que uno se imagina. No es raro que una víctima que pierde fondos importantes pueda estar en un estado de denegación, incluso después de que se le dice que hay una investigación penal en curso. Como mecanismo de defensa, algunos se negaron a encarar y admitir que fueron engañados. Lo he visto incluso con profesionales de alto nivel. También hay ocasiones en que el estafador hace ofertas laterales a víctimas desesperadas. Las víctimas se comprometen a dar fe de los méritos de la inversión a cambio de que se le devuelva su dinero.

No es raro que los empresarios deseosos de inversión acepten situaciones cuando se enfrentan a la realidad económica, sobre todo si están disfrutando de la buena vida. Esto sucede a menudo cuando hay crisis económica de la inversión subyacente. La crisis de las hipotecas incubó una gran cantidad de escenarios de aceptación. Las personas que tenían que decirles a los inversionistas que perdieron todo continuaron aceptando contribuciones de inversión. Esta situación puede ser particularmente difícil para el cumplimiento de ALD debido a que la diligencia debida inicial habría dado como resultado un perfil legítimo.

Usted tiene que conocer las tramas para detectar las tramas. Debido a que la tecnología ha aumentado la velocidad de creación de nuevas estafas, los departamentos de ALD se enfrentan al reto hercúleo de cómo ofrecer efectivamente capacitación en las tendencias de fraude emergentes. Aquí es donde la policía tiene que intervenir y proporcionar de forma proactiva el reconocimiento de la situación de fraude. Los profesionales de ALD se encuentran en desventaja en la identificación de fraudes si no están informados sobre la mecánica detallada de las tramas actuales. Una cosa es decirle a alguien cómo montar un reloj; otra cosa es desmontarlo y mostrarle cómo encaja cada pieza. Esto ya está ocurriendo en cierta medida en muchas ciudades con grupos de tareas de fraude financiero que contactan las instituciones financieras. Las restricciones presupuestarias obstaculizaron considerablemente la capacidad de la policía para asistir a las conferencias de la industria para compartir su experiencia en la materia. Para mitigar esto, quizá capítulos locales de ACAMS también podrían servir como una plataforma para acoger la policía local, estatal y federal para que puedan perfilar casos y tendencias recientes.

Conclusión

Durante el último año he participado en controles de la realidad con colegas como un medio para medir mi nivel de hartazgo. Invariablemente mi observación refleja la suya: Muchos de nosotros creemos que nunca ha habido un momento en que las posibilidades de que uno sea víctima de fraude son tan grandes. Ante esto, todos tenemos que tener conciencia de la situación de nuestro entorno financiero, no sólo para nosotros sino también para nuestros familiares y amigos, especialmente los más ancianos, que podrían ser más vulnerables. Los tiburones financieros son bastante sigilosos como para nadar en aguas tranquilas y poco profundas sin ser detectados. Esto se me demostró de manera dolorosa recientemente.

No hace mucho, recibí una llamada de un primo que me informaba que mi tía anciana había perdido todo su fondo de jubilación a manos de un estafador. La trama atrapó a miles de víctimas de edad avanzada que perdieron sus ahorros de toda la vida a manos de lo que ellos pensaban que era una inversión prudente y segura que ofrecía una rentabilidad razonable de alguien de confianza durante años. A medida que iba preguntándole a mi primo sobre lo sucedido, me di cuenta dolorosamente de que los estafadores les habían hecho una buena jugada, habían cubierto sus huellas y apenas habían dejado pequeñas aberturas para un juicio rápido y abarcador. Era un escenario que he visto una y otra vez, pero ahora dio en el blanco. El plan involucró más de medio mil millones de dólares y, probablemente fue el mayor del estado.

Mi conjetura es que el mismo subterfugio sofisticado utilizado en las víctimas para mantenerlos a raya también se aplicó a las intuiciones financieras. La historia se incrusta profundamente en mi creencia de que esto le puede pasar a cualquiera y a cualquier institución financiera. No importa lo mucho que construimos nuestros programas para detectar el fraude financiero, los estafadores depredadores ingeniosos siempre encontrarán la manera de no quedar atrapados en las redes. Y, entonces, me vuelvo aún más harto; nunca seremos capaces de construir la ratonera perfecta para el ratón defraudador.

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

Luchando contra el fraude de reembolso de impuestos: Las instituciones financieras como estructuras defensivas

A medida que la temporada de impuestos de 2014 llega a su fin, la División de Investigación Criminal del Servicio de Impuestos Internos (IRS-CI) ha reconocido la necesidad creciente de identificar y combatir el robo de identidad y el fraude de reembolso de impuestos. "El robo de identidad es uno de los delitos de mayor crecimiento en todo el país, y el fraude de reembolso causado por el robo de identidad es uno de los mayores desafíos que enfrenta el IRS", dijo el Comisionado del IRS John Koskinen.[1] El fraude de reembolso se produce cuando se roba o compra un número de seguro social, o una lista de números; se presenta una declaración de impuestos falsa, por lo general al inicio de la temporada de presentación de las declaraciones; y un reembolso se envía por correo a una dirección accesible a las personas involucradas en el plan, se envía a un banco, o se carga en una tarjeta prepaga.[1] En los últimos años, ha surgido un nexo entre el fraude de reembolso y las formas más tradicionales de delincuencia, como el narcotráfico, porque los individuos y las redes ven la rentabilidad de este tipo de delito altamente lucrativo y de riesgo relativamente bajo.

De acuerdo con un informe del Inspector General del Tesoro para la Administración Tributaria (TIGTA) de septiembre de 2013, el IRS emitió más de $3,6 mil millones en reembolsos potencialmente fraudulentos en el año fiscal 2011.[2] En mayo de 2012, el Inspector General del Tesoro J. Russell George informó a los Subcomités de la Cámara de Maneras y Medios sobre Vigilancia y Seguridad Social que los criminales que presentan declaraciones de impuestos fraudulentas robando identidades de los consumidores podrían ingresar un estimado de $26 mil millones en los próximos cinco años.[3] A la luz de un aumento del fraude de reembolso, el IRS y el Departamento de Justicia están incrementando sus esfuerzos para luchar contra esta forma de robo de identidad. En el año fiscal 2013, el IRS inició aproximadamente 1.492 investigaciones penales relacionadas a los robos de identidad, un aumento del 66 por ciento sobre las investigaciones iniciadas en el año fiscal 2012. Desde enero de 2014, el Departamento de Investigación Delictiva del IRS ha iniciado 295 nuevas investigaciones de robo de identidad, lo que aumenta el número de casos activos a más de 1.800.[4]

El 24 de febrero del 2014, el Departamento de Justicia emitió un comunicado de prensa destacando sus esfuerzos de aplicación más recientes y su compromiso de proseguir la persecución del delito de Fraude de Reembolso de Robo de Identidad (SIRF en inglés). En el año fiscal 2013, el Departamento de Justicia presentó más de 580 autos de procesamiento de más de 580 acusados de delitos relacionados con el SIRF.[5] Como los planes de reembolso de impuestos se hacen cada vez más frecuentes y sofisticados, las instituciones financieras deben tener en cuenta los indicadores de fraude de reembolso de impuestos y aumentar los esfuerzos para reportar sospechas de delito por parte de sus clientes, así como rechazar reembolsos potencialmente fraudulentos.

¿Qué pueden hacer los proveedores de servicios financieros?

Las instituciones financieras son fundamentales para identificar el fraude de devolución de impuestos, ya que a menudo proporcionan los medios para la negociación o el depósito de fondos. Los negocios de servicios monetarios (MSB) pueden ser la primera línea de defensa en la detección del fraude de reembolso por medio de reembolsos hechos en papel, aunque, en algunos casos, ellos mismos pueden estar involucrados en los sistemas de devolución. Los delincuentes pueden cobrar las devoluciones de impuestos a los MSB como una manera de recibir dinero en efectivo rápidamente, evitando los bancos. Los MSB deben tener consciencia de las banderas rojas de alerta, que pueden indicar fraude de reembolso de impuestos y deben garantizar en consecuencia que se presenten informes de actividades sospechosas universales (USAR). Los MSB deben mostrar cautela ante clientes que cobran un gran volumen de cheques de reembolso, clientes que cobran cheques de reembolso en efectivo en nombre de varios individuos con la misma dirección, así como ante la devolución de impuestos emitidos en el mismo monto en dólares para algún individuo en un estado muy lejos de la ubicación del MSB. Los delincuentes pueden enviar los cheques de reembolso para múltiples individuos a la misma dirección o a direcciones cercanas, a veces en connivencia con los trabajadores postales que trabajan ciertas rutas.[6] También pueden viajar a otro estado a fin de utilizar un MSB específico. Los delincuentes también pueden utilizar la información financiera similar en la presentación de devolución de impuestos, lo que resulta en reembolsos que son iguales o son casi por la misma cantidad en dólares. Los MSB deben reconocer similitudes entre direcciones y deben mostrarse cautelosos ante las personas que acompañan a los clientes, así como frente a los clientes que presenten identificación dudosa. Al completar informes de actividades sospechosas (SAR) cuando hay sospecha de fraude de reembolso, los MSB deben asegurarse de que utilizan el término "fraude de reembolso de impuestos" en la sección narrativa. También pueden querer alertar a la Oficina de Investigación Criminal del IRS local sobre la actividad sospechosa.

Los bancos también son fundamentales para identificar posibles fraudes de reembolso del Tesoro hechos por individuos y clientes del MSB y deberían devolver los reembolsos cuestionables al IRS. Durante la temporada de impuestos de 2013, más de $245 mil millones de los $301 mil millones en reembolsos se emitieron a través de depósito directo.[7] A medida que el número de devoluciones de impuestos por medio de depósitos directos y tarjetas prepagas aumenta, los bancos probablemente verán un aumento en el potencial de fraude de reembolso a través de las cuentas

[1] Comunicado de prensa del Department of Justice http://www.justice.gov/opa/pr/2014/February/14-tax-193.html>
[2] TIGTA Report < http://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.pdf>
[3] Testimony of The Honorable J. Russell George, Treasury Inspector General for Tax Administration <http://www.treasury.gov/tigta/congress/congress_05082012.pdf>
[4] Comunicado de Prensa de IRS, IR-2014-50, <http://www.irs.gov/uac/Newsroom/IRS-Intensifies-Work-on-Identity-Theft-and-Refund-Fraud;–Criminal-Investigation-Enforcement-Actions-Underway-Across-the-Nation>
[5] Comunicado de Prensa del Department of Justice Press http://www.justice.gov/opa/pr/2014/February/14-tax-193.html>
[6] "Former U.S. Postal Service Mail Carrier Sentenced to Prison for Role in Stolen Identity Refund Fraud Scheme", <http://www.justice.gov/opa/pr/2013/October/13-tax-1164.html>
[7] IRS 2013 Filing Season Statistics see <http://www.irs.gov/PUP/newsroom/12-27-2013.pdf>

bancarias de los clientes. Los bancos deben reconocer las banderas rojas de la Red Contra los Delitos Financieros (FinCEN), que pueden ser indicativas de fraude de reembolso, y deberían considerar devolver reembolsos de depósitos directos, así como deberían alertar a las oficinas del IRS locales cuando hay sospecha de fraude de reembolsos de impuestos.[8] Según lo recomendado por TIGTA, las instituciones financieras deberían rechazar depósitos directos de reembolsos realizados en cuentas que pertenecen a personas cuyo nombre no coincide con el que aparece en la declaración de impuestos. Estos reembolsos deben reenviarse al IRS que a su vez enviará una notificación al contribuyente cuyo nombre no es el mismo de la declaración.[9] Por otra parte, las instituciones financieras deberían considerar desarrollar una manera de autenticar la identidad de las personas que utilizan tarjetas de débito, ya que el IRS no ha desarrollado una manera de identificar los depósitos directos de la devolución de impuestos a las cuentas asociadas a una tarjeta de débito. Los bancos también deberían limitar el número de devoluciones de impuestos a la misma cuenta bancaria o tarjeta de débito con el fin de reducir la posibilidad de fraude.

Los oficiales de cumplimiento deben estar al tanto de los posibles vínculos entre el fraude de reembolso y otras formas de delincuencia, y deben asegurarse de que los SAR describen todas las actividades sospechosas, cuando sea aplicable. Por ejemplo, si varias devoluciones de impuestos se depositan en la cuenta de un cliente, y la actividad de desvío, que es a menudo indicativa de tráfico de drogas, se lleva a cabo en la misma cuenta, esta actividad debe reportarse y caracterizarse por lo menos como robo de identidad y lavado de dinero. Esta información podría ser un catalizador para una nueva investigación, o podría ayudar a los investigadores para presentar cargos penales adicionales contra uno o más individuos.

Por último, los bancos deben asegurarse de informar actividades sospechosas relacionadas con clientes de MSB que pueden depositar declaraciones de impuestos fraudulentas de terceros. Aunque el depósito de cheques de terceros está en consonancia con el modelo de negocio de los MSB, los bancos deben asegurarse de presentar SAR cuando reciben múltiples cheques del Tesoro de sus clientes de MSB en las mismas cantidades o cantidades similares y/o que tienen la misma dirección.

¿De qué manera los datos relacionados con la devolución SAR ayudan a los investigadores?

La información proporcionada en los SAR es inteligencia valiosa para los investigadores financieros que llevan a cabo las investigaciones penales. Información tal como los importes y las direcciones que figuran en los reembolsos de impuestos, así como la frecuencia de la actividad, puede ser aprovechada por las fuerzas del orden y puede conducir a un mayor desarrollo de un caso. La información sobre posibles conexiones entre los clientes también es útil para los que aplican la ley y puede permitir identificar redes de personas que pueden estar trabajando juntas como parte de un plan más amplio. Los detalles relativos al cargo de un cliente y sus negocios, en particular las empresas de preparación de impuestos, pueden también ayudar y apoyar en casos de las autoridades de control legal. En febrero y agosto de 2013, tres empleados de "Nothing But Taxes" (Nada Mas Pero Los Impuestos, en español), una empresa de preparación de impuestos en Durham, Carolina del Norte, fueron condenados a prisión federal por delitos relacionados con la preparación de declaraciones de impuestos falsas y fraude de identidad. Otros dos empleados de "Nothing But Taxes" están a la espera de sentencia. Del mismo modo, el dueño de "Angie's Tax Service" en Baton Rouge, LA, fue sentenciado a 132 meses de prisión federal por fraude electrónico, declaraciones falsas, suscribir declaraciones de impuestos falsas y robo de identidad agravado. Se ignora si datos de FinCEN se utilizaron por las fuerzas del orden en estas investigaciones, pero los detalles con respecto a los sospechosos y sus transacciones, y si está disponible, han podido ayudar en gran medida a los investigadores en este caso.

Melissa Babin, CAMS, asociada de Booz Allen Hamilton y analista financiera senior de anti-lavado de dinero (AML) (FININT) para un cliente del gobierno EE.UU., Babin_melissa@bah.com

[8] For a list of red flags, see FinCEN Advisory FIN-2013-A001, <http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-A001.html>
[9] TIGTA Report < http://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.pdf>

Más baches en el camino del **Bitcoin**: ¿Es este el *fin* del *principio?*

La velocidad del cambio en moneda virtual es grande. Los artículos que se escriben sobre ella de inmediato requieren revisiones. El modelo de Wikipedia de mensajes actualizados continuamente es quizás el medio ideal para escribir sobre las monedas virtuales. Esto es especialmente cierto en el caso de Mt. Gox, bolsa de Bitcoin con sede en Japón, que cesó sus operaciones en febrero de 2014, cuando anunció que habían desaparecido unos 850.000 bitcoins de los clientes y de sus propias reservas (el valor estimado en el momento fue de $450 millones y equivalía a 6 por ciento de la oferta mundial de bitcoins). A pesar de que desde entonces ha "encontrado" 200.000 bitcoins perdidos, Mt. Gox inició su liquidación en abril.

Al igual que muchas empresas de nueva creación, el concepto detrás de Mt. Gox consistía en satisfacer una necesidad del mercado, en este caso la bolsa de Bitcoin. Después de leer sobre Bitcoin en 2010, el programador y empresario digital Jed McCaleb entendió que el mercado Bitcoin necesitaba un sitio donde los participantes pudieran intercambiar bitcoins y moneda fiduciaria. Entonces escribió el código de un sitio web de intercambio y lo emparejó con un nombre de dominio que poseía llamado Mt. Gox (mtgox.com). Mt. Gox deriva del nombre de Magic the Gathering Online Exchange, un mercado en línea para comerciar tarjetas de juegos de fantasía.

Mt. Gox fue un éxito inmediato entre los primeros adoptadores de Bitcoin. Pocos meses después de ir en vivo, el intercambio estaba procesando cientos de órdenes, que estaban tomando más y más del tiempo de McCaleb para centrarse en las operaciones diarias y lo alejaban de desarrollar mejoras en el código inicial. En 2011, McCaleb vendió una participación mayoritaria en Mt.Gox a otro programador, Mark Karpelès, quien se convirtió en el director general (CEO).

Bajo la dirección del Karpelès, Mt.Gox continuó creciendo y para abril de 2013, Mt. Gox representaba aproximadamente el 70 por ciento del mercado de Bitcoin. Sin embargo, los problemas con la gestión y la plataforma de negociación eran continuos desafíos a las operaciones generales. Como cuando en junio de 2011, un hackeo requirió cerrar el sitio durante unos días y resultó en la pérdida de aproximadamente $8,7 millones de dólares en bitcoins.

En mayo de 2013, se le emitió una orden de incautación a Dwolla, un procesador de pagos para el comercio electrónico en línea con sede en Iowa, para las cuentas de Mutum Sigillum LLC, subsidiaria de Mt. Gox en los EE.UU. En aquel entonces, los consumidores podían comprar bitcoins mediante un depósito con Dwolla, y luego los fondos se enviaban a Mt. Gox para la compra real del bitcoin. Después de una extensa cobertura de prensa, en junio de 2013, Mt. Gox se anotó en la Red Contra los Delitos Financieros (FinCEN) y siguió funcionando como la bolsa líder de moneda digital en el mundo. Las grietas en el modelo comercial de Mt. Gox empeoraron cuando Dwolla, en octubre, finalizó la actividad de cambio de divisas con sus clientes virtuales debido a la incertidumbre y la confusión en torno a las monedas virtuales.

En aquel momento, el negocio de Mt. Gox luchaba por sobrevivir. La compañía cedió $5 millones a los agentes federales de los EE.UU. porque la empresa no estaba anotada como empresa de servicios monetarios (MSB) y un ex socio de negocios, CoinLab estaba demandando a la compañía por $75 millones. Mt.Gox luego presentó una contrademanda por $5 millones BTC que CoinLab supuestamente mantenía para Mt. Gox. Los clientes estadounidenses pronto empezaron a quejarse de los largos retrasos para retirar dólares de Mt. Gox. Si bien Mt. Gox se mantuvo como la bolsa prominente, las noticias en la comunidad de Bitcoin empezaban a extenderse sobre si Mt. Gox se podía mantener a flote. Los problemas continuaron y en febrero de 2014, la empresa simplemente les dejó de pagar a los clientes en bitcoins alegando que había un defecto en la moneda digital. Y entonces llegó la noticia de que Mt. Gox había sido hackeado y perdió 850.000 bitcoins. Lo que una vez fue la mayor bolsa de Bitcoin estaba cerrada.

De acuerdo con los informes en línea, los hackers habían estado sacando (skimming en inglés) dinero de Mt. Gox desde 2011. Los informes afirman que había una fuga entre el monedero caliente de Mt. Gox y su almacenamiento en frío. El almacenamiento en frío eran las reservas de Bitcoin de Mt. Gox y que tenían que estar no en línea sino fuera de línea para su custodia. Parece que los hackers tuvieron acceso a las claves de propiedad sobre Bitcoin en el almacenamiento en frío y sin conciencia de los administradores. Almacenamiento caliente se refiere al mantenimiento de teclas Bitcoin conectadas a Internet, mientras que el almacenamiento en frío es cuando los fondos están fuera de línea. Esto nos lleva a la pregunta: En una empresa cuya operación entera consiste en la protección de datos y la seguridad de la programación, ¿cómo podría no haber notado la infracción durante tanto tiempo? ¿Es de extrañar que los consumidores y los inversionistas perdieran toda confianza en Mt. Gox?

Como consecuencia de que Bitcoin es un nuevo medio de intercambio, los clientes de Mt. Gox carecen de recurso o tienen poco a su alcance para tratar de recuperar sus inversiones en Bitcoin. En este momento de la vida de la moneda virtual, hay poca o ninguna protección al consumidor. Las monedas virtuales exponen a los consumidores al riesgo de robo digital o fraude, y las carteras de divisas virtuales no tienen la seguridad de una cuenta de banco asegurado por la FDIC. Sin embargo, es bien conocido en los círculos de divisas digitales que Bitcoin es un producto e inversión de alto riesgo. Además, los inversores especulativos en Bitcoin no tienen las protecciones que se ofrecen a los inversores de los productos tradicionales. Para las monedas virtuales que obtienen una mayor aceptación, es necesario que haya mejorado la protección de los consumidores y de los inversores. Esto puede retirar gran parte de lo los conceptos iniciales en cuanto al anonimato y la no regulación. Lo más probable es que Mt. Gox se convierta en el niño modelo para la regulación mejorada, en especial la protección del consumidor.

El CEO de puesta en marcha y oficial de cumplimiento de bitcoin acusado de lavado de dinero

En enero de 2014, vimos la detención de Charlie Shrem, vicepresidente de la Fundación Bitcoin, cofundador y director ejecutivo, de BitInstant, y uno de los defensores más prominentes de Bitcoin. El caso federal contra Shrem está relacionado con su interacción con el residente de Florida Robert Faiella (conocido también como BTCKing), distribuidor de bitcoin que operó en el mercado Silk Road, ya desaparecido. La denuncia penal federal le señala a Shrem tres acusaciones: operar una empresa de transferencia de dinero sin la licencia adecuada, conspiración para cometer lavado de dinero, y la omisión intencional de presentar informes de actividades sospechosas (SARs).

Según la denuncia, Faiella recibió órdenes para Bitcoin de usuarios de Silk Road para completar sus transacciones en el sitio. La empresa de Faiella requería que Bitcoin y, según se alega, él entonces hacía pedidos directamente a Shrem en BitInstant quien, a su vez, transfería bitcoins a cuentas controladas por Faiella. Entonces los bitcoins se revendían a los clientes de Silk Road con un margen de ganancia.

BitInstant era una pequeña operación con un equipo de sólo cuatro personas, por lo que los papeles y responsabilidades de las oficinas de frente al público y las de la trastienda se compartían. Una de las responsabilidades de Shrem era supervisar el programa de cumplimiento de antilavado de dinero (ALD) de BitInstant. Según la denuncia federal, Shrem también estaba interactuando directamente con los clientes y él personalmente procesaba las órdenes de cambio de BTCKing incluso cuando muchas órdenes estaban por encima del umbral diario de $1.000 y aprobaba las anulaciones. Por otra parte, según la investigación del gobierno, se alega que Shrem ayudó a BTCKing proporcionando instrucciones sobre cómo eludir las políticas de ALD de BitInstant y los disparadores de banderas rojas (por ejemplo, depósitos estructurados).

Al final, la demanda alega que Shrem y Faiella vendieron más de $1 millón de bitcoins a usuarios de Silk Road, quienes luego utilizaban esos bitcoins para comprar estupefacientes y otras mercancías ilícitas y servicios. En abril de 2014, tanto Shrem como Faiella fueron acusados en una corte federal de Nueva York.

Este caso es un ejemplo de los desafíos a los que se enfrentan todas las instituciones financieras al tratar de mantener un programa de cumplimiento sólido. No importa lo bueno de las políticas y los controles, esos procedimientos se pueden inutilizar por los propietarios y empleados dispuestos a hacer caso omiso de las normas y reglamentos que rigen el ALD. Una buena práctica de ALD para proteger nuestras firmas contra el abuso consiste en marcar la pauta de adhesión a una cultura de cumplimiento.

Los buenos controles internos y una cultura ética fuerte y robusta minimizarán el riesgo de lavado de dinero. Pero incluso el programa de ALD más

sólido se puede evitar. Como se vio con BitInstant, una empresa con un programa de ALD manifiesto en su sitio, sufrió la subversión de sus controles internos y su sistema de control de parte de un miembro del personal en connivencia con un cliente y que tenía autoridad para anular el sistema de control interno. Este es el quid del caso federal contra Shrem.

Para que Bitcoin y otras monedas virtuales obtuvieran mayor aceptación, la adhesión a las directrices de ALD recomendadas por la FinCEN y otros reguladores deben implementarse y seguirse. La ley lo requiere y también lo hacen las instituciones financieras con cuentas bancarias. Las organizaciones deben mantener una sólida cultura de ética empresarial y cumplimiento como parte de sus valores corporativos. Cuanto más ese tono se desarrolla y se practica, más posibilidades hay de que las violaciones de procedimiento y los riesgos de fraude internos se reducirán.

Escrutinio de las transferencias de par a par

El interés en el comercio de Bitcoin y de prevenir que se utilice para realizar actividades ilícitas también está ocurriendo a nivel de estado de los EE.UU. En diciembre de 2013, detectives de Florida iniciaron una investigación de lavado de dinero con moneda digital. Los detectives estatales accedieron a la página web https://localbitcoin.com para obtener una lista de los operadores más cercanos a la ubicación del usuario. Localbitcoins.com es uno de los últimos sitios que permiten a los usuarios de bitcoins comerciar de forma anónima.

Los usuarios se relacionan entre sí a través de un canal de par a par donde los comerciantes de Bitcoin establecen correspondencias con compradores. Los usuarios luego se reúnen personalmente o en línea para intercambiar bitcoins por moneda fiduciaria, una operación financiera que está fuera del sistema financiero tradicional. Por ejemplo, la persona A quiere comprar bitcoins de la persona B. Se ponen de acuerdo en un precio y se reúnen en una cafetería local. La persona A ya mantiene un instrumento financiero o dinero en efectivo, entonces pasa el mismo a la persona B. La persona B entonces transfiere los bitcoins de su monedero digital al monedero digital de la persona A. Ahora, la persona B tiene dinero fiduciario en el bolsillo y la persona A tiene bitcoins en su monedero digital.

En Florida, los detectives notaron varios puestos de localbitcoins.com de un comerciante con el alias de "michelhack". Michelhack tenía al menos 100 operaciones confirmadas en los últimos seis meses de 2013 que involucraron más de 150 bitcoins (valor estimado de 110.000 dólares). Un agente encubierto contactó a michelhack e inicialmente le compró un bitcoin por $1.000, que incluía una tasa de 17 por ciento. Nota: Las tasas de cambio en línea son tradicionalmente más bajas que el valor de calle; sin embargo, los intercambios de dinero fiduciario a bitcoin o viceversa se encuentran contemplados por la guía de FinCEN y se consideran MSB, por lo tanto la disponibilidad de intercambios conformes en línea en los EE.UU. es pequeña.

Se confirmó que michelhack era un alias vinculado a Michell Abner Espinoza. Los investigadores se fijaron si el nombre de Espinoza aparecía en la Oficina de Regulación Financiera de Florida o en la base de datos de MSB de FinCEN para determinar si él se había registrado como MSB. Se reveló que Espinoza no estaba en ninguna de las listas.

Para investigar más en profundidad, las autoridades de control legal realizaron otra operación (por valor de $500). En el momento de la transacción, el agente encubierto le dijo a michelhack que quería comprar 30.000 dólares en bitcoins para comprar información sobre línea de tarjetas de crédito robadas. Espinoza declaró que podía dar cabida a la orden y se fijó una fecha y hora para la transacción. Paralelamente a la investigación sobre Espinoza, los detectives encubiertos también estaban inspeccionando a otro comerciante de bitcoins en localbitcoins.com que tenía el alias de "proy33". Proy33 fue posteriormente identificado como Pascal Reid, quien también fue detenido en febrero durante una transacción de $30.000. En total, Espinoza y Reid fueron acusados de operar una MSB sin licencia y de dos penas cada uno de lavado de dinero en moneda digital.

Según la policía, Espinoza y Reid violaban las leyes de la Florida que regulan los transmisores de dinero y estatutos de lavado de dinero. La ley prohíbe el envío de dinero o instrumentos de pago en moneda superiores a $300 pero menos de $20.000 en un período de 12 meses. Los estatutos de ALD de la Florida prohíben el comercio o negocio en la moneda por más de $10.000. Los juicios de Espinoza y de Reid aún están pendientes. Sin embargo, sus abogados sostienen que sus clientes no hicieron nada ilegal ya que la ley estatal no cubre las monedas digitales.

¿Los baches en el camino son para mejor?

Los casos identificados anteriormente son golpes adicionales en la carretera de Bitcoin y se pueden agregar a las vulnerabilidades del ecosistema Bitcoin según lo ilustra el caso de Silk Road. Sin embargo, el ecosistema, y en particular la Fundación Bitcoin, ha reconocido la importancia del cumplimiento de la Ley de Secreto Bancario/antilavado de dinero (BSA/AML) como una necesidad para seguir actuando. Los primeros en adoptar allanaron el camino para que Bitcoin se integrara completamente, pero a lo mejor no son los únicos en hacer progresar esta moneda virtual. La regulación está ayudando a forjar las reglas del camino, los inversores están reconociendo que el cumplimiento es parte de la ecuación de la financiación, las empresas que se inician reconocen que el ALD es un componente de valor añadido a la actividad empresarial y que garantiza una mejor protección de los consumidores. Por otra parte, todas las partes tienen una mejor comprensión de que los programas de ALD robustos ayudan a las empresas iniciales de moneda virtual a obtener relaciones bancarias y más amplia legitimidad comercial. Por supuesto que no todo está resuelto; se están dando cambios para mejor.

Muchos reguladores y jurisdicciones están haciendo sus deberes. Están tratando de entender el concepto de Bitcoin y de otras monedas virtuales: ¿Cómo pueden las monedas virtuales ser instrumentos positivos para los servicios financieros más amplios?; ¿cuáles son sus riesgos?, incluidos los riesgos de lavado de dinero, y, si el enorme potencial de las monedas virtuales presentes puede satisfacerse dentro de los lineamientos de una infraestructura financiera sólida. ¿Las monedas virtuales bajarán los costos de transacción, incrementarán acceso al capital, y llevarán los servicios financieros a muchos individuos no bancarizados en todo el mundo? Las nuevas regulaciones y la adaptación de la normativa existente a los nuevos productos y servicios pueden no ir al ritmo que quiere el ecosistema de la moneda virtual; sin embargo, se están moviendo.

Las autoridades de control legal han adoptado una postura dura, probablemente es así como se debe; sin embargo, los reguladores también han declarado en repetidas ocasiones que no van a socavar la innovación. Los reguladores prefieren reconocer que hay reglas definidas que deben ser incluidas en la innovación. Con una mayor adopción podemos esperar ver el refinamiento de la regulación, así como el perfeccionamiento del protocolo de Bitcoin. Existe una demanda significativa de entidades legítimas en el ecosistema para realizar transacciones, gastar e invertir en Bitcoin. Cuanto más fuerte sea, las empresas mejor dirigidas (es demasiado pronto para hablar de la "segunda generación") ya se están construyendo. Ellas están en modo sigilo y están entrando en línea pronto. El cambio es dinámico y en el mundo de Bitcoin ya es necesario actualizar este artículo.

Brian Stoeckert, CAMS, CFE, director general, director de estrategia de CoinComply, Nueva York, NY, EE.UU., bstoeckert@coincomply.com

Timothy O'Brien, MBA, consultor, Nueva York, NY, EE.UU., timothykobrien@outlook.com

FinScan®
Powered by Innovative Systems

Industrial Strength Offerings for

Sanctions & PEP Screening, KYC / CIP and Identity Verification

Handles Unlimited Record Volumes

100% SaaS Up-time

Verified Disaster Recovery Plan

Data Centers in US, Canada, Germany, Cayman Islands

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

12 billion+ hosted transactions per year

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

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

- Integrates smoothly with all leading third-party PEP databases
- Helps ensure the accuracy and validity of SWIFT and other payment transaction processing
- Provides sanctions lists and 24/7/365 list management service
- Automates review process through integrated case management tool
- Facilitates customer onboarding
- Provides automated I.D. document authentication via integration with scanners
- Screens available in English, Spanish, French, German, and more
- Plus many other features, including document attachment

www.finscan.com

FinScan®
Powered by Innovative Systems

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

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

TORONTO • MEXICO CITY • FRANKFURT

Construyendo una mejor alianza

ACAMS Today habló con el detective Michael Kelly, con el detective Constable Dwayne King y con Peter Warrack, director de la FIU de ALD del Bank of Montreal Financial Group, sobre la importancia de las alianzas entre instituciones financieras (FI) y las autoridades que aplican la ley (LE) y sus experiencias en el campo de la prevención de delitos financieros.

El detective Michael Kelly se graduó de la Universidad de Waterloo, como licenciado en ciencias políticas. Después de graduarse, escribió columnas editoriales de un periódico antes de que lo contratara el Servicio de Policía de Toronto en 2001.

El detective Kelly ha estado investigando los delitos financieros durante siete años y lleva cuatro años asignado a la Alianza Estratégica de Toronto. La finalidad de la Alianza es una estrategia combinada de aplicación de la investigación de la comercialización engañosa en o procedente de la provincia de Ontario o transfronteriza. Los socios de la agencia de ejecución son: Servicio de Policía de Toronto, la Oficina de Competencia de Canadá, la Real Policía Montada de Canadá, el Ministerio de Servicios al Consumidor de Ontario, el Ministerio de Hacienda y en los EE.UU., la Comisión Federal de Comercio y Servicio de Inspección Postal de los EE.UU.

En 2010 el detective Kelly recibió el *Premio de Aplicación de la Ley de los Bancos Canadienses* por investigar la creación de cientos de identidades sintéticas, conocido más tarde como Project Mouse (Proyecto Mouse en español).

El detective Constable Dwayne King labora con el Servicio de Policía de Toronto. Tiene 25 años de experiencia en la Policía de Toronto. Con los años, ha ocupado diversos cargos dentro del servicio. Durante 10 años fue investigador de accidentes; desde allí se trasladó a un cargo uniformado de primera línea por tres años. Después pasó cinco años como investigador importante de violaciones de domicilios y robos. Durante los últimos seis años, el detective King ha trabajado en la Unidad de Delitos Financieros de la Sección de Confiscación de Activos como investigador de confiscación de activos/ganancias del delito/lavado de dinero. Es experto tribunalicio en dinero en efectivo, uso lícito vs ilícito de efectivo y lavado de dinero. Ha sido designado Especialista Certificado de Antilavado de dinero (CAMS). El detective King ha sido el investigador principal en ganancias de delitos/confiscación de activos en varias investigaciones criminales en varias jurisdicciones importantes. El detective King es instructor en la Escuela de Policía de Canadá, la Escuela de Policía de Ontario y la Escuela de Policía de Toronto en las áreas de Ganancias del Delito, Lavado de dinero y Delitos contra la propiedad. En 2012, también fundó una empresa denominada Anti Money Laundering Training Specialist (AMLTS) [Entrenamiento de Especialistas en Antilavado de dinero]. Su empresa se centra en la capacitación de primera línea en la lucha contra el lavado de dinero.

Peter Warrack actualmente es director de la FIU de ALD del Bank of Montreal Financial Group (BMO FG). Anteriormente trabajó como gerente senior de inteligencia y luego jefe de investigaciones de ALD en el Royal Bank of Canada (RBC) al cual había ingresado en 2002 viniendo de la policía de Irlanda del Norte, donde se desempeñó como detective senior.

Desde que llegó a Canadá, Warrack ha sido un defensor de las investigaciones conjuntas de control/fuerzas del orden y ha participado activamente con la policía en la distribución legal de información y las mejores prácticas, lo que ha dado lugar a detenciones y la interdicción de la delincuencia.

Warrack con frecuencia hace presentaciones orales y publicas sobre temas como la inteligencia, el fraude y el blanqueo de dinero y se le menciona a menudo como un académico práctico. La contribución de Warrack a la industria de ALD fue reconocida por sus colegas en 2011 cuando recibió el Premio *ACAMS de Profesional de ALD del Año*.

ACAMS Today: ¿Cómo aplica su experiencia de LE a su posición actual?

Peter Warrack: Mediante la aplicación de la mentalidad de un enfoque proactivo, en el enfoque de inteligencia de mi trabajo actual, que incluye la colaboración de alianzas entre la LE y el sector privado. Las alianzas no son sólo una cuestión de intercambiar tarjetas de visita en una conferencia, sino en realidad se trata de ser proactivos y hacer que estas alianzas sucedan. Se necesita trabajar para establecer y reforzar relaciones. Por último, la aplicación de los principios de gestión de la investigación que se utilizan en LE al trabajo que se hace en el sector público.

AT: ¿Cuál es la clave para tener un proceso de investigaciones exitosas?

PW: Mi mundo es, por supuesto, el del ALD, pero no se puede tener lavado de dinero sin un delito subyacente que da lugar a la generación de las ganancias del delito. Aquí es donde entra la LE—los mundos de Mike y de Dwayne. Trabajar juntos en alianzas (es decir, las instituciones financieras y las autoridades de control legal) y el intercambio de información aumenta la posibilidad de interceptar con éxito la delincuencia y lograr el enjuiciamiento de los delincuentes. Quizás lo más importante desde un punto de vista financiero, trabajando juntos legalmente y de forma proactiva el intercambio de información de tendencias y la inteligencia ayuda a prevenir que en primer lugar el crimen ocurra. La clave es trabajar juntos.

AT: ¿Qué pasos se han dado para hacer alianzas exitosas entre los sectores público y privado?

PW: Las alianzas no suceden por arte de magia. Toma esfuerzo sostenido llegar a los asociados de las fuerzas del orden y verdaderamente establecer una red de contactos y llegar a conocerse unos a otros, no sólo llamar cuando se necesita algo, ya que se tiene la tarjeta de otro obtenida en una conferencia. Tampoco se trata sólo de compartir información; también compartimos las mejores prácticas (por ejemplo, las capacidades analíticas y de gestión de la investigación).

AT: ¿Cómo pueden los sectores público y privado garantizar que el intercambio de información está sucediendo en todas las industrias?

PW: Ambas partes necesitan líderes apasionados por establecer contactos, a veces cruzando barreras imaginarias. Las conferencias deberían atraer a un público más amplio de lo obvio, en mi banco con frecuencia traen oradores invitados de fuera del mundo de la aplicación de la ley y viceversa. Recientemente, gracias a Dwayne, tres de mis investigadores acudieron al Curso de Confiscación de Bienes de la Policía de Toronto; hicieron nuevos contactos, aprendieron mucho de LE y también contribuyeron en ayudar a los de la LE a entender el mundo del ALD.

AT: En su puesto actual, ¿cuál es el tipo más común de actividad delictiva que ve a diario en su institución financiera?

PW: Sin lugar a dudas el fraude en muchas de sus formas, por ejemplo, la absorción de cuentas, ardides románticos, fraudes de inversión, fraude hipotecario y evasión fiscal.

AT: ¿Qué tipo de formación reciben en su departamento de cumplimiento para hacer frente al fraude?

PW: Llevamos a cabo entrenamiento frecuente y extenso para entender en primer lugar el delito de lavado de dinero, cómo funciona, usando y debatiendo numerosos ejemplos y, de igual importancia, llevamos a cabo una amplia formación para comprender los delitos precedentes subyacentes. Lo llamamos las cuatro etapas de lavado de dinero –ganancias, colocación, estratificación e integración. La capacitación también incluye la legislación actual cambiante y el desarrollo de los acontecimientos mundiales. Tenemos la suerte de tener dos compañeros dedicados al aprendizaje de nuestra universidad corporativa y también un desarrollador de temas en línea. Nuestra formación es una mezcla de actividad en línea, pre-lecturas y el aprendizaje colectivo en clase. Nos tomamos muy en serio la formación.

En la foto: Peter Warrack

AT: ¿Cómo se involucró en el ALD y la prevención de delitos financieros?

Dwayne King: Se me acercó un detective sargento de confianza que me dijo que esta sería una gran oportunidad. Este es un campo maravilloso y me gusta trabajar en el campo del ALD. Es increíble lo que podemos hacer como agentes de policía para desbaratar organizaciones delictivas una vez que tenemos el conocimiento.

AT: ¿Cuál es el mayor caso de confiscación que ha manejado?

DK: Yo trabajo en la LE municipal, por lo normalmente nuestros casos son más pequeños. Dicho esto, he tenido varios casos grandes de hasta $5 millones en activos e ingresos en efectivo. El caso que me gustaría destacar es un caso de extorsión de Toronto del este. Fue una operación de usura donde el prestamista usaba la publicidad en un diario y se aprovechaba de los drogadictos y adictos al juego. El usurero estaba cobrando a estas víctimas 10 por ciento del principal como tasa de interés sobre una base semanal. Si usted pidió prestado 5.000 dólares tenía que pagar $500 en interés por semana hasta que se pagaba la cantidad total y el interés nunca variaba. Cuando los prestatarios ya no podían pagar sus deudas fueron agredidos y sus vidas amenazadas. De hecho, uno de los beneficiarios de los préstamos se vio obligado a empezar a trabajar para el prestamista con el fin de pagar su préstamo de $3.000. Trabajó para el prestamista durante casi un año y dejó de trabajar para él porque logramos detener al delincuente. Esta investigación nos llamó la atención, porque una de las víctimas había pedido dinero prestado para pagar los gastos médicos de su esposa y después de un año de pagarle más de 30.000 dólares al usurero, la víctima se mudó, pero el usurero lo encontró y el usurero exigió otros $10.000 o amenazó con lastimar a la esposa e hijos de la víctima. Como resultado, la víctima fue a la policía y esa fue la forma en que nos involucramos, lo que finalmente llevó a la detención del usurero. El usurero fue declarado culpable y se le ordenó reembolsar a sus víctimas y que renunciara a más de 100.000 dólares, como ganancias del delito. La víctima que le había pagado al prestamista $30.000 terminó recuperando su dinero.

AT: ¿Qué pueden hacer las instituciones financieras para ayudar en casos de decomiso de activos?

DK: STR y SAR son absolutamente invaluables para los casos de decomiso de activos. Por ejemplo, el caso que mencioné antes sobre el usurero, originalmente no podíamos ligar a la mujer al caso, pero a causa de un SAR presentado nos enteramos de que estaba depositando grandes cantidades de dinero en efectivo, algunos de ellas tanto como $80.000 en una sola vez. Como resultado del STR, pudimos vincularla al blanqueo real de los activos delictivos, fue arrestada y acusada de blanqueo de ganancias del delito y la posesión de ganancias de delito.

Como me ocupo más de instituciones financieras, ya sea en mi papel de policía o de entrenador, he aprendido que las instituciones financieras no reciben ninguna información sobre lo que ocurre con los informes sobre transacciones sospechosas que presentan. Creo que la retroalimentación de los FI sobre los resultados de sus informes sobre transacciones sospechosas ayudaría a ganar y aumentar el interés de las FI de y, aun más importante, de sus empleados. Como oficial de policía creo que es importante, cuando sea posible, dar algún tipo de información a la FI que presentó el STR.

Por último, el fomento de relaciones positivas entre los LE y los FI nos ayudará a todos nosotros. Todos estamos luchando en la misma batalla contra el blanqueo de dinero y la financiación del terrorismo.

AT: Usted entrena a profesionales de la ley, ¿cuál es la pregunta más común que hacen durante los entrenamientos?

DK: Muchas personas vienen a mis entrenamientos sin ningún conocimiento de lavado de dinero o las ganancias de la investigación de delitos y sus primeros pensamientos son "¿Puedo hacer esto?" Al principio, mi objetivo es tratar de romper el estereotipo de que las ganancias de investigaciones de delitos son demasiado trabajo o están fuera del ámbito de las capacidades de cualquier oficial de policía.

AT: ¿Cuál es el mejor consejo que ha recibido para avanzar en su carrera?

DK: Nunca rechaces el entrenamiento y nunca dejes que el miedo te impida hacer algo. Comenzar algo desconocido o nuevo puede ser intimidante, pero hace seis años no sabía nada sobre el ALD o de las Investigaciones de Ganancias del Delito y ahora estoy ofreciendo formación en esos campos. Yo no soy más inteligente que cualquier otro oficial de la policía; sólo que ahora tengo la formación que no tenía antes.

AT: ¿Cómo se involucró en el ALD y en la prevención de delitos financieros?

Michael Kelly: De manera totalmente accidental. Durante un violento altercado con un individuo me golpeé la cabeza contra una mesa que estaba atornillada al suelo, lo que resultó en una lesión grave en la cabeza. Después de varios meses, estaba volviendo al trabajo de a poco y me ubicaron en la oficina de fraudes para continuar

con la recuperación. A medida que mejoraba empecé a ayudar con las investigaciones y resultó que era bastante bueno en ello. Volví a la labor de primera línea por alrededor de un año y medio y cuando una vacante en la oficina de fraude surgió, pedí el cargo, y el resto es historia. Creo que es justo decir que, en mi caso, empecé a investigar el fraude después de un fuerte golpe en la cabeza.

AT: ¿Cómo han ayudado las Alianzas Estratégicas de Toronto a frustrar la comercialización masiva engañosa?

MK: La Asociación Estratégica de Toronto nació como una respuesta directa a los desafíos jurisdiccionales. La mayoría de las tramas de marketing masivo operan deliberadamente cruzando fronteras para hacer que los intentos de detección, interceptación y de aplicación sean más difíciles.

Las tramas de fraude implican típicamente víctima(s), delincuente(s), medios de comunicación y el envío de dinero. La posesión inicial de la información se reparte entre varias agencias del orden público/de gobierno y las partes interesadas del sector privado en los diferentes países. Todas las investigaciones, en su forma más básica, son la búsqueda, recopilación y análisis de dicha información.

Aliarse con grupos de ambos lados de la frontera inmediatamente rompe muchas de las barreras que previamente habían interferido con el flujo de esa información. El resultado ha sido una investigación más exhaustiva, más eficiente y que, en un caso, se ha traducido en una erradicación completa de un problema.

De 2003 a 2009 los investigadores del Servicio Postal de los EE.UU se enteraron de que un gran número de víctimas del fraude en los EE.UU. estaban enviando dinero al área de Toronto a través de una empresa de transferencia de dinero. Los miembros de la Alianza Estratégica de Toronto obtuvieron autorizaciones judiciales y llevaron a cabo la vigilancia física que reveló que las transferencias de múltiples víctimas estaban siendo "agrupadas" en grandes pagos individuales a los individuos que operaban puntos de venta corruptos del mismo negocio de transferencia de dinero. Aproximadamente $100 millones fraudulentos fueron identificados y los operadores fueron posteriormente extraditados a los EE.UU., donde se declararon culpables y recibieron largas penas de prisión.

La investigación fue tan completa que el servicio de transferencia de dinero aceptó la confiscación de $100 millones en un acuerdo de enjuiciamiento diferido por su papel en la facilitación de las transacciones. No ha habido ningún punto de salida corrupto identificado en el área de Toronto, en los casi cinco años después de la investigación.

AT: ¿Qué consejo le daría a otros profesionales que están comenzando a formar alianzas de los sectores público y privado?

MK: La formación inicial de las asociaciones es a menudo un ejercicio de persistencia. La verdad es que en casi todas las alianzas va a haber organizaciones con intereses que compiten entre sí, ya sea directa o indirectamente. Todas las partes necesitan que se les recuerde que su base de unión está en enfrentar un problema o desafío común.

En una presentación que sintetiza nuestra investigación sobre las identidades sintéticas (Project Mouse) utilizamos una foto de Franklin Delano Roosevelt, Churchill y Stalin sentados con los otros. Destacamos que al igual que con los hombres en esa imagen, los actores que reunimos tenían intereses en conflicto y, en algunos casos, desprecio por el otro. Pero esas diferencias se dejaron de lado en el fomento de la investigación, que más tarde beneficiaría a todas las partes interesadas.

Al final del día, las asociaciones nacen por necesidad; si una sola persona o grupo pudiera lidiar con el problema por sí solo ya lo habría hecho. Paradójicamente, es pensando y actuando colectivamente que todos nos beneficiamos al máximo de forma individual.

AT: ¿Puede hablarnos de su investigación de identidades sintéticas?

MK: El Project Mouse fue una investigación que inicialmente descubrió 125 identidades sintéticas respaldadas por identificación emitida por el gobierno. Estas identidades no pertenecían a personas reales, fueron simplemente creadas a través de diversas lagunas en los sistemas de gobierno y del sector privado, que se supone deben proteger contra este tipo de cosas.

Desde el principio nos dimos cuenta de que estas identidades presentaban un riesgo significativo para las fuerzas del orden, las burocracias del gobierno y la industria privada. También sabíamos que si dejábamos cualquier aspecto de ellas sin tocar, serían explotadas y como oficiales de policía tenemos el deber de prevenir la delincuencia.

En un esfuerzo por racionalizar la investigación y mitigar los daños, identificamos grupos de interés y los invitamos a asistir a una conferencia de caso en la que expusimos lo que habíamos encontrado, porqué era peligroso para todos nosotros y lo que esperábamos de todos ellos a medida que avanzábamos. No todo el mundo estaba entusiasmado por participar en un primer momento pero

En la foto: Dwayne King y una moto que se recuperó de una escena de crimen.

probablemente no haya una frase más motivadora que "siéntase libre de perder tanto dinero (o la confianza del público) como quiera".

Al final, después de meses de colaboración y de compartir, nuestra lista aumentó a más de 1.000 nombres y pudimos limitar severamente las pérdidas sufridas por los grupos de interés del sector privado. Esto por cierto retiró cientos de millones de dólares de las manos del grupo extranjero de delito organizado que respaldaba la operación, que a su vez fue una gran victoria para la seguridad pública.

AT: ¿Cuál fue la pieza central de la información que llevó a cerrar el sindicato de identidad sintética?

MK: No estoy seguro de que hubiera una sola pieza de información que haya logrado esto, sino más bien hubo confluencia de muchas cosas.

Muy tempranamente otro servicio de la policía arrestó a un hombre que era el rostro de una de las falsas identidades que habíamos identificado. En el momento de su detención se encontraba en posesión de la documentación que nos permitió identificar dónde/cuándo/cómo se creó la identidad sintética.

Ante nuestra sorpresa, nos enteramos a través de uno de nuestros grupos de interés del sector privado de que la identidad había existido en el

papel durante aproximadamente dos años antes de obtener la licencia de conducir. La identidad había sido creada a través de una puerta trasera en cómo se crean y controlan los perfiles de crédito. Luego supimos que el grupo detrás de él estaba muy organizado, era muy sofisticado y estaba bien financiado, y era muy paciente.

Pero creo que la táctica más efectiva en retrospectiva fue también la final. Al compartir nombres, direcciones y otra información con todos nuestros grupos de interés nuestra lista creció por diez mediante la asociación de esos datos.

El grupo criminal fue cuidadoso de no dejar todos sus huevos en una sola canasta, así que tuvimos que reunir todas nuestras canastas y contarnos unos a otros lo que estábamos buscando. Y creo que este es el beneficio final de las alianzas público-privadas: la capacidad de identificar más fácilmente los huevos malos y tratar con ellos en consecuencia.

AT: ¿Tiene algún consejo sobre cómo las instituciones financieras pueden aprender a identificar las identidades sintéticas tan pronto llegan a sus instituciones?

MK: Las instituciones financieras se encuentran un poco en desventaja porque el personal de primera línea no tiene la capacidad de sondear las distintas burocracias gubernamentales con el fin de verificar la identidad/identificación de una persona. La verdad sea dicha, las propias burocracias a menudo no tienen la capacidad de compartir esta información con los demás tampoco. Este sigue siendo el obstáculo principal.

Esto significa que las instituciones financieras tienen que protegerse a sí mismas mediante la adopción de una visión más crítica de la información frente a ellas. Por ejemplo, si un nuevo cliente da un apartamento de dos piezas como dirección, asegúrese de que otras veinte personas no están pretendiendo vivir en esa misma dirección también. Utilice los mapas en línea con capacidades de "vista de la calle" para confirmar que realmente existe una dirección. Si un cliente le da una dirección particular en la Ciudad de Toronto y el número de teléfono de su casa con un código de área de Montreal, esto también estaría diciendo algo.

Cuando entra una ola de nuevos clientes y todos dicen trabajar para la misma empresa, mire esa empresa más de cerca. En Project Mouse teníamos decenas de personas presuntamente trabajando para la misma compañía de camiones; si los bancos se hubieran molestado en mirar se habrían dado cuenta de que esta compañía de camiones aparentemente logró aparcar su flota dentro de los acogedores confines de un apartamento de soltero en un edificio de Toronto de gran altura. Si hubieran mirado aún más de cerca, se habrían dado cuenta de que una gran empresa constructora que supuestamente empleó decenas más se encuentra en el mismo piso de soltero.

Otra cosa que encontramos fueron cientos de activaciones de tarjetas de crédito que se realizaban desde el mismo teléfono. Pudimos identificar la mayoría de nuestras identidades sintéticas utilizando técnicas muy sencillas, de sentido común, junto con análisis básicos (dirección, empleador, número de teléfono, etc.). La tecnología y los programas avanzados son una gran herramienta, pero el exceso de confianza en ellos a menudo crea la apatía y hace que la gente pase por alto los fundamentos.

En nuestro caso se trataba de un cajero de banco de primera línea que reconoció que esa misma persona había abierto dos cuentas bancarias con nombres diferentes, lo que comenzó toda nuestra investigación. No se necesitaba una herramienta de tecnología costosa o formación amplia para reconocer que un individuo no puede abrir cuentas bancarias con nombres diferentes.

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

¡Una idea novedosa!

Cuando el sol comienza a subir, los oficiales se alinean delante del concreto y acero. Clavan los ojos en un trozo de cartón que tienen enfrente. Escuchan de un altavoz: "Encárguense". Dentro de un segundo, se oye un sonido metálico que gira y una botella con forma de papel que una vez fue una delgada pieza de cartón se hace ahora visible delante de cada oficial. Con precisión exacta, los oficiales sacan la pistola de su funda, apuntan a la botella y hacen seis rondas de fuego. Los agentes de policía de todo el mundo asisten a la formación de armas de fuego por obligación. ¿Para qué? Para asegurarse de que den en el blanco cuando se requiera o para protegerlo a usted. El entrenamiento es lo único que realmente separa la vida de la muerte.

El entrenamiento de los agentes durante un año consta de tirar, manejar persiguiendo a otro, primeros auxilios, asuntos legales, testimonios ante los tribunales y una serie de temas de capacitación (es decir, grupos desviados, lucha en tierra, etc.). Una vez que un oficial decide su trayectoria profesional dentro del departamento, él o ella va a buscar una capacitación más formal para el camino elegido. Ciertos departamentos harán una presentación pública en forma de una Academia de Policía para Ciudadanos para mostrar cómo se entrenan todos los agentes.

¿Qué tipo de entrenamiento le ofrece su institución?

Con la *13ª Conferencia Anual Financiera y de ALD* acercándose rápidamente, le recomiendo que asista. Cuando hablo con los oficiales y los grupos de la comunidad acerca de la marihuana, les pido que miren siempre y piensen en la totalidad. Sí, sólo es marihuana, pero ¿cuántas personas han muerto a causa de plantarla o venderla? Sí, sólo es una multa por velocidad, pero si te hace ir más despacio puede salvar una vida. Sí, sólo es un informe de actividades sospechosas (SAR), pero la presentación de manera adecuada podría conducir a la captura de un terrorista, un depredador de niños o a localizar a una persona desaparecida.

El entrenamiento agudiza nuestras habilidades en nuestros campos respectivos. Tanto si se trata de reconocer a alguien que acaba de entrar en su institución financiera para cobrar un cheque fraudulento o reconociendo que ciertos depósitos se hacen en un tiempo determinado de la semana, lo que indica apuestas ilegales provenientes de eventos deportivos.

He asistido a muchas conferencias de ACAMS por años y creo que el éxito de la Unidad de Lavado de Dinero, Investigaciones Especiales/Drogas del Departamento de Policía del Condado de Fairfax, se puede atribuir a las clases que hemos tenido y los contactos que hemos logrado en las conferencias. Por lo tanto, no entre a una clase con la actitud o la impresión de que usted no va a aprender nada. En vez, comparta sus experiencias para que otros puedan aprender de lo que usted sabe.

Una unidad de aplicación de la ley dedicada al lavado de dinero, local o federal, está diseñada para seguir, rastrear e incautar los activos ilícitos derivados de actos ilegales. La capacitación actualizada por parte de las fuerzas del orden y el sector privado es una necesidad si se quiere tener éxito. Nuestra Unidad se creó en 2004. Asistimos a nuestra primera conferencia de ACAMS en octubre de 2006. Me enorgullece decir que los contactos que hemos hecho a través de los años y la información que ha sido compartida durante las conferencias a las que hemos asistido han ayudado en la incautación de varios millones de dólares de ganancias ilegales. Si desea escuchar las historias de cada caso, pues tendrá que venir a conocernos.

Unidad de Lavado de Dinero, Investigaciones Especiales/Drogas del Departamento de Policía del Condado de Fairfax se asoció a ACAMS el año pasado y llevó a cabo una presentación sobre la marihuana y el lavado de dinero. Cada uno de los miembros del equipo habló durante la presentación. Compartimos cómo hacemos una investigación y al final me quedé contento ya que el grupo nos habló de nuevas formas de identificar, por medio de registros financieros, las casas cultivadoras de marihuana.

Alianzas, redes y entrenamiento

Siempre he hablado muy bien de ACAMS, ya que es un grupo que reúne tanto los sectores financieros como los de cumplimiento de la ley. Proporcionan una excelente capacitación en diferentes ámbitos para ambos sectores y nos dicen que trabajemos juntos. Es en estos eventos de contactos en los que nuestra Unidad de Lavado de Dinero quiere conocerlo a usted. Puedo seguir infinitamente sobre los casos que hemos procesado con éxito porque hemos hecho varios contactos con las instituciones financieras en un evento de contacto. Venga a conocernos en el próximo evento o mejor aún contacte a un grupo de la policía que le quede cerca y dígales de la conferencia, invítelos, conózcalos aprendan unos de otros y capturen a algunos de los malos.

No puedo destacar lo suficiente la importancia de mirar la totalidad cuando se trata de entrenarse. Así que, cuando usted se encuentre en una fría sala de capacitación y piensa en cuánto tiempo tomará la capacitación, reevalúe la situación, y preséntese a la persona de al lado y deje que sepa lo entusiasmado que se encuentra por participar en la clase. Lo que aprenda y transmita a sus colegas podría salvar la institución de pasar vergüenza, obviar multas penales o civiles, o usted puede incluso aprender a salvar a un niño de la explotación o salvar una vida.

El entrenamiento hace la diferencia entre el éxito y el fracaso, y en mi profesión podría significar la vida o la muerte, pero en su profesión puede significar rescatar y salvar vidas sin siquiera saberlo.

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

Analytics
for banking

Detect and deter money launderers.

SAS® Anti-Money Laundering delivers dynamic risk assessment, so you investigate only meaningful alerts. High-performance analytics and multiple detection methods offer you complete protection and enable you to meet compliance demands with greater speed and accuracy than ever before.

Read the paper
sas.com/alert

sas
THE POWER TO KNOW®

La vida secreta del ALD

Tal vez no haya más insistencia sobre ningún otro aspecto de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) que en la necesidad del secreto. Se trata de la "S" de BSA que es el único aspecto del ALD en el que a todos los sectores de las instituciones financieras, los reguladores y las fuerzas del orden se les capacita constantemente, advierte una y muchas veces francamente y se les amenaza con consecuencias draconianas si lo violan. Por desgracia, la formación y orientación en esta área se dedica casi exclusivamente a las precauciones y advertencias sobre la protección de la información secreta con poca o ninguna orientación sobre cómo utilizar la información secreta o confidencial en el fomento de una investigación.

Los informes de actividades sospechosas (SARs, por sus siglas en inglés) constituyen un buen ejemplo, pero de ninguna manera son un ejemplo exclusivo, sobre el equilibrio que hay que mantener entre la necesidad de recolección de inteligencia, la información secreta y confidencial y su uso eventual en una investigación o acción de aplicación efectiva. Muchos investigadores han experimentado la situación kafkiana de la inteligencia recogida para un propósito definido, sin embargo, los que recogen la inteligencia son los que la consideran demasiado reservada, sensible o valiosa para usarla con ese propósito. Una tendencia reciente en la formación y discusiones de Equipos de Revisión de SAR es cómo conseguir un mejor y más completo cumplimiento de las citaciones hechas a las instituciones financieras. Con demasiada frecuencia, elementos tales como documentos de BSA/ALD, comunicaciones internas y datos de transacciones específicas que pueden impactar de manera sustancial las investigaciones son o no enviados o intencionalmente retenidos debido a preocupaciones de confidencialidad, a pesar de las citaciones.

No es de extrañar que haya renuencia a proporcionar información. De hecho, existen serias consecuencias para las revelaciones indebidas. Casi todas las revelaciones apropiadas se definen bajo los parámetros de uso oficial. A los agentes policiales se les disciplina de manera rutinaria, deja cesantes e incluso se les inician procesos penales por hacer controles de licencia para amigos, socios o por otras razones no oficiales. Los arrestos de celebridades rutinariamente producen acceso indebido por parte de investigadores a los datos de la Red Contra los Delitos Financieros (FinCEN), estos que simplemente alcanzan el nivel de "chisme". El acceso a datos confidenciales es raramente una autoridad comprehensiva. No sólo el personal de instituciones financieras se enfrenta a sanciones similares por divulgar asuntos de BSA indebidos, sino que la propia institución también podría enfrentar sanciones por el monitoreo o la formación insuficiente de su personal.

Sin embargo, también hay consecuencias serias por no hacer revelaciones apropiadas. Más allá de los muchos ejemplos de las instituciones financieras sancionadas por no informar de actividades sospechosas, incumplir intencionalmente el alcance y las demandas de una citación u orden judicial también puede tener las mismas consecuencias graves. En la mayoría de las investigaciones federales, mentirles a los agentes puede ser un delito en sí mismo. Los testigos que proporcionan respuestas falsas o engañosas pueden encontrarse con acusaciones a pesar de que no eran los objetos de la investigación.

Cuando se trata de información financiera, en primer lugar debemos considerar el fuerte deseo de proteger celosamente nuestra privacidad financiera. Se teme a menudo la exposición de la información financiera a la sociedad mucho más que los secretos de alcoba. Esto se refiere tanto a las relaciones personales como a las de negocios. A las personas que compran pequeñas empresas regularmente se les presenta el "informe de ingresos gravables" seguido por el "guiño, guiño, cabeceo, cabeceo" de lo que el negocio realmente hace. Las apariencias externas son generalmente muy engañosas. A menudo hay una riqueza considerable detrás de fachadas modestas y mucha quiebra tras los muros de las mansiones. La BSA comienza ya en un mundo donde este tipo de subterfugio es común.

Los datos de BSA o de FinCEN deben ponerse en contexto. Los canallas han aprendido a explotar nuestra renuencia a profundizar en los asuntos financieros. Ellos saben cómo mantener las cosas fuera de contexto. Muchos han sido traicionados por un amigo o socio que ha presentado una situación financiera simpática y aparentemente honesta que luego resultó falsa. El lamento que normalmente sigue al descubrimiento fraudulento es no haber prestado atención a las señales de advertencia. Esas señales de advertencia raramente se encontraban en los números de la superficie. Los investigadores de ALD no pueden permitirse el lujo de distraerse con los números de superficie si quieren ser eficaces. Esos son los números que el culpable quiere que vea. Usted quiere los números que no quiere que vea.

> Los investigadores de ALD no pueden permitirse el lujo de distraerse con los números de superficie si quieren ser eficaces

La BSA, principalmente a través de los SAR, ahora obliga a las instituciones financieras a actuar como informantes. Este es un papel que no siempre conocen y sobre el cual existen incertidumbres. Los informantes han estado tradicionalmente muy conectados directamente a su(s) investigador(es). El SAR crea un vínculo indirecto en el que el veto de la "credibilidad y fiabilidad", que es un elemento crucial en una relación tradicional informante/investigador, puede ser aún más confuso. Aunque la existencia de un SAR se basa en el secreto y la confidencialidad que por lo general sólo se aplica a revelar o exponer la existencia de ese SAR. Las personas y la información identificada o verificada a través de una investigación basada en un SAR no tienen garantía de confidencialidad. La existencia del SAR es el único secreto protegido.

Tomemos por ejemplo un cajero a quien un cliente le pregunta "¿Cuánto dinero puedo depositar antes de informarle al IRS?" Como respuesta el cajero le proporciona al cliente un folleto sobre los informes de transacción monetaria (CTR, por sus siglas en inglés) tras lo cual el cliente hace un depósito de $9.900 en efectivo. El cajero informa de esto al director y, finalmente, el informe se abre paso para llegar al departamento de BSA/ALD. La revisión de BSA/ALD refleja que este cliente hace una serie de depósitos parecidos después de este encuentro. Desde este momento un SAR se convertirá en un informante confidencial diciéndoles a los que aplican la ley que este cliente puede estar cometiendo la violación delictiva de la estructuración y el cajero puede ser testigo de ese delito. El SAR no garantiza protegerse de una

investigación, ya sea para el cliente o el cajero. Hace todo lo contrario en la prestación de una pista para un investigador.

Si se investiga lo informado, el investigador querría entrevistar personalmente a los testigos identificables, que incluirían a este cajero. Sin embargo, esto no significa que el nombre del relator ahora pasa al dominio público. Los investigadores raramente identifican a sus testigos abiertamente en este tipo de investigaciones. Hay investigaciones de integridad y otras consideraciones, para incluir las preocupaciones del cajero, que hacen que sea prudente mantener reserva mayormente hasta la conclusión de la investigación. Puede haber necesidad de divulgar información sobre las investigaciones a lo largo del camino, pero rara vez se extiende a ser un documento público y abierto.

Aunque los investigadores construyen un caso con un juicio potencial en mente, ellos, como el cajero, están tratando de hacer que sea el resultado más improbable. No es ningún secreto que la mayoría de los casos son juzgados sin un juicio formal. Las ofertas de negociación y otros acuerdos son la conclusión más frecuente para la gran mayoría de los casos penales. En esta paradoja, sin embargo, mientras mejor esté preparado el testigo para un juicio, menos probable es que vaya a pasar. El trabajo de investigación descuidada puede crear problemas de juicio fácilmente evitables.

Una investigación exitosa de ALD generalmente es el resultado de la fusión de la información de una gran cantidad de fuentes. Las tramas de lavado de dinero, por su propia naturaleza, tienen múltiples capas, a menudo sin relación directa evidente entre sí. Fuera de la totalidad de la investigación, los testigos o involucrados en los diversos elementos pueden no ser conscientes de cómo sus papeles (a veces aparentemente menores) impactan la investigación en general. Tampoco es raro que en una investigación de ALD que los testigos hayan tenido tratos positivos o interacciones con el culpable. Ellos pueden ser renuentes e incluso estar a la defensiva ante cualquier inferencia nefasta que se pueda hacer sobre el culpable. El lavado de dinero es sólo una forma de fraude y sin una víctima manifiesta. La mayoría de los estafadores han aprendido a ser muy encantadores cuando tienen que serlo.

Cualquier tendencia a retener información en una investigación de buena fe que está en marcha es perjudicial para esa investigación. Aunque una llamada airada documentada sobre una comisión bancaria al servicio del cliente puede ser vista por ese departamento como irrelevante y sin interés para una citación de ALD recibida por la institución financiera; de hecho podría ser un indicador clave de las discrepancias que el investigador había identificado en el caso. Al igual que muchas otras investigaciones, serán los detalles de menor importancia que el culpable no tuvo en cuenta lo que desmontará su credibilidad. Recuerde, no es raro que los culpables finjan emociones para desviar o bloquear una investigación.

El campo de ALD tiene muchos componentes. Cuando se lleva a cabo una investigación de buena fe de lavado de dinero es necesario que haya una fusión de todos los secretos de todos los componentes para que la investigación sea exhaustiva y completa. Para ello es necesario que su posición en el ALD esté conectada en red correctamente con todos los demás componentes que puedan tener un impacto en dicha investigación. Los esfuerzos de aplicación externos necesitan saber que su información y contribución al ALD existe. Su vida secreta de ALD no debe ser un secreto.

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

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

Los inspectores postales redoblan esfuerzos para impedir *el lavado de dinero*

Oldrich / Shutterstock.com

Hay una pequeña agencia que está propinando un gran golpe en la lucha contra el lavado de dinero: Conozca el Servicio de Inspección Postal de los EE.UU. (USPIS).

Los agentes de USPIS son inspectores postales federales, que constituyen el brazo de aplicación de la ley, prevención del delito y seguridad del Servicio Postal de los EE.UU. (USPS). Los inspectores llevan armas de fuego, hacen arrestos, ejecutan órdenes de búsqueda federales y entregan citaciones. Aplican unas 200 leyes federales que cubren los delitos que implican el uso fraudulento del correo de los EE.UU. y del sistema postal.

Los inspectores postales no sólo trabajan para asegurar que los negocios estadounidenses puedan enviar de forma segura fondos e información a través del correo, sino que también aseguran que los clientes postales pueden encomendar su correspondencia con USPS y que los empleados postales puedan trabajar en un ambiente seguro.

> Un público informado es la primera línea de defensa contra el fraude en el correo

La agencia lleva a cabo estas metas a través de la aplicación, la investigación y, tal vez de igual importancia, con las campañas nacionales de sensibilización de los consumidores, financiadas por las multas cobradas a delincuentes condenados por maniobras fraudulentas. Basados en la creencia de que un público informado es la primera línea de defensa contra el fraude en el correo, los inspectores organizan eventos en distintas comunidades y oficinas de correos para llamar la atención a las tendencias de fraude actuales. Hacen presentaciones y distribuyen literatura con consejos sobre alertas de fraude para ayudar a los estadounidenses a convertirse en consumidores más inteligentes y mejorar sus conocimientos sobre la forma de combatir los fraudes.

Bajo el Título 18 U.S.C. 1956 y 1957, los inspectores postales investigan a delincuentes que hacen mal uso de los giros postales del servicio postal para blanquear fondos ilícitos, evaden impuestos o evitan los requisitos de generación de informes federales violando así la Ley de Control del Lavado de Dinero (MLCA) y la Ley de Secreto Bancario (BSA). La venta ilegal de drogas, el fraude electrónico, el robo de identidad, la trata de personas, y las ventas de mercancías falsificadas todos dependen del lavado de dinero—y todos son delitos que los inspectores investigan diariamente. Es para lo que fueron contratados.

Como inspector postal y director del programa, tengo a honra dirigir el programa nacional del Servicio de Inspección Postal para las investigaciones de lavado de dinero (MLI en inglés).

El éxito en la investigación

Un buen ejemplo de nuestro trabajo de MLI es un caso de Nueva York, donde nos centramos en una red de narcotráfico colombiana que estaba usando el Cambio de Peso del Mercado Negro (BMPE) y giros postales para lavar su dinero en efectivo.

El BMPE es un sistema internacional de lavado de dinero de drogas complejo. Depende de los servicios de un "corredor de peso", que coordina el intercambio de bienes (se compra en los EE.UU. con el dinero de la droga), que se introducen de contrabando en Colombia y se venden por pesos en el mercado negro. El BMPE convierte narcodólares a pesos sin cambiar la moneda.

Teníamos una pista de un "pitufo" (lavador de dinero) de una red colombiana de narcotráfico. Lo rastreamos cuando hacía compras estructuradas de giros postales, comprando dos o tres por valor de menos de $1.000 cada uno, en las 22 Oficinas de Correos en Long Island y Queens, NY. Incautamos 26 cuentas de negocios que el pitufo usaba para depositar los giros postales.

Fue una investigación difícil, ya que algunas de las cuentas de las empresas que utilizaba el BMPE también se utilizaban en empresas legítimas. Los inspectores estudiaron minuciosamente los documentos de innumerables fuentes para enlazar las cuentas a ganancias de la droga y para demostrar la participación en las actividades del BMPE.

Establecimos correspondencias entre las fechas y lugares de compra de giros postales con registros de correo electrónico obtenidas mediante orden de allanamiento. Los correos electrónicos del agente de pesos al pitufo contenían instrucciones sobre cuánto dinero de la droga debería pasarse a giros postales y cuáles empresas de BMPE deberían recibir las órdenes de pago. También identificamos encomiendas que usaba el pitufo para enviar las órdenes de pago a las empresas BMPE.

En última instancia rastreamos e incautamos miles de dólares en ganancias de la droga que habían sido repartidos entre 26 cuentas de BMPE. Arrestamos al pitufo y al corredor de pesos, cada uno de los cuales se declaró culpable de infringir el Título 18 U.S.C. 1956, sobre lavado de dinero.

Alcance postal vasto

Las ventas de giros postales han disminuido a medida que otras formas de pago electrónico siguen creciendo. Pero como dicen, todo es relativo. El USPS vendió más de 102 millones de órdenes de pago el año pasado, y en promedio vende cerca de 350.000 órdenes de pago en un día determinado.

Lo que definitivamente no está disminuyendo es la actividad sospechosa con giros postales. Se ha incrementado hasta en un 30 por ciento en los últimos tres años. Los delincuentes que buscan una forma fácil de lavar su dinero sucio a menudo recurren a los giros postales del USPS, instituciones financieras u otros puntos de venta. Sólo unos pocos miles de dólares en giros postales en cada punto pueden transformar sus ganancias mal habidas en efectivo limpio o al menos eso creen. No cuentan con la vigilancia de nuestra agencia o los numerosos controles del USPS.

El sistema de punto de venta utilizado por el USPS para transacciones al por menor está integrado con el sistema de cumplimiento de BSA del USPS, que es parte de la Oficina de Cumplimiento del USPS, una entidad separada y distinta del Servicio de Inspección. El sistema de monitoreo de la Oficina de Cumplimiento ayuda a garantizar que toda la información requerida se recoge de las operaciones hechas con instrumentos financieros postales que cumplen con el umbral de registro.

Todos los meses generamos y analizamos informes de transacciones de giros postales sospechosos para detectar la posible estructuración. Clasificamos los resultados en territorios por inspector y los enviamos a los jefes de equipo de MLI en esas áreas. Ellos profundizan las operaciones concretas para desarrollar pistas del caso.

Constantemente extraemos datos disponibles para atrapar la posible estructuración en las oficinas de correos. Los mapas de calor (una representación gráfica de los datos en la que los valores se muestran con colores) nos ayudan a aislar las ubicaciones de las operaciones sospechosas.

La formación es clave

Crucial para el éxito del USPS es este hecho: Los giros postales son vendidos por empleados de carrera, no están tercerizados. Esto se traduce en una fuerza de trabajo estable de personal minorista especializado.

Anualmente, miembros minoristas en oficinas de correos de todo el país reciben capacitación obligatoria de cumplimiento de BSA desarrollada e implementada por la Oficina de Cumplimiento de BSA del USPS. Todos los asociados minoristas responsables de ventas de giros postales son educados a fondo en todos los aspectos de cumplimiento de la BSA. Además, empleados del sector minorista, que manejan más de 989 millones de visitas de clientes a las instalaciones postales cada año, están capacitados para observar y reportar cualquier transacción que consideren sospechosa.

Estos empleados son la clave para el programa de cumplimiento de correos y una razón importante por la que el USPS tiene un historial de cumplimiento excelente.

La cooperación importa

Con 31.135 oficinas de correos de venta al público que operan en todo el país seis días a la semana, y $21 mil millones en giros postales que se venden cada año, la investigación de operaciones financieras sospechosas no es tarea fácil. Entonces, ¿cómo protegen los inspectores y el USPS al público estadounidense?

Trabajamos en estrecha colaboración con la Oficina de Cumplimiento de BSA del USPS, que tiene funciones específicas y diferenciadas del Servicio de Inspección Postal.

El objetivo común de las dos oficinas requiere que mantengan abiertas las líneas de comunicación, asegurando que los inspectores postales reciban toda la información que sea legalmente admisible necesaria para realizar investigaciones de alta calidad de las ventas de giros postales estructurados y de lavado de dinero.

Además de los informes mensuales que difundo a nuestras unidades de campo para generar pistas potenciales, los inspectores van a las oficinas de correos para encontrarse uno a uno con los asociados minoristas—los empleados en la primera línea que interactúan diariamente con los clientes. Esa relación proporciona una valiosa fuente de inteligencia que puede acelerar las investigaciones haciéndolas el objetivo en la fuente misma.

Una visita de un inspector puede conducir a notificaciones de las operaciones sospechosas en el mismo día, así como las descripciones, imágenes de vídeo de los sospechosos y, si un empleado de correos puede conseguirlo de forma segura, el número de placa del auto de un sospechoso.

Un enfoque renovado

Nuestra agencia está intensificando su atención a las investigaciones de lavado de dinero, aumentando los recursos en esta área por más de 40 por ciento este año fiscal.

Bajo la dirección del jefe inspector postal, estoy añadiendo nuevas actividades de divulgación para construir una red fuerte con nuestras oficinas en todo el país. He estado visitando los equipos de liderazgo de campo para transmitir la importancia del programa y hacer hincapié en el potencial de importantes investigaciones, procesadas por el gobierno federal.

Varias de nuestras oficinas en el terreno han dedicado recursos nuevos al programa de MLI. Clases de capacitación de investigación se han programado para los empleados del Servicio de Inspección hasta fin de año. La instrucción en el aula se centra en los diferentes métodos de lavado de dinero y muestra cómo los inspectores y analistas pueden hacer para construir casos efectivos.

Los cuatro instructores que construyeron nuestro curso de MLI son investigadores de lavado de dinero veteranos que tienen un total combinado de 50 años de experiencia en el campo. Proporcionan a cada inspector estudiante una formación que navega a través de las muchas bases de datos disponibles en el curso de una investigación postal.

Cada sesión termina de la misma manera: Los estudiantes desarrollan una pista real de estructuración delictiva, por lo que su último bloque de ocho horas se encuentra totalmente dedicado al desarrollo de casos en profundidad. Los estudiantes profundizan en los datos bajo la tutela de instructores. Al completar la clase, están dispuestos a desarrollar sus propias pistas de lavado de dinero.

Para una visión adicional, nuestros inspectores de MLI se unen a los asistentes en el Seminario de Investigación Financiera anual de la Sección de Confiscación de Bienes y Lavado de Dinero del Departamento de Justicia. Comprende asistencia legal y política para el personal de la fuerza pública, con énfasis en la mecánica de las investigaciones financieras—cómo rastrear dinero.

Casos de estructuración fuertes conducen a la exposición de una amplia gama de actividades ilícitas. Es un método único y eficaz de formación de los investigadores.

Movilización de recursos

Como una de las agencias de la ley federales más pequeños, el USPIS bien entiende el valor de la obtención de recursos mediante la colaboración con otras agencias. Los inspectores han contactado Fiscalías de los EE.UU. con la intención de unirse a las Fuerzas de Tareas de Informes de Actividades Sospechosas (SAR) locales, pasándoles datos de inteligencia, o simplemente ofreciendo un punto de contacto para casos de lavado de dinero relacionados con los giros postales. Su misión, como siempre, es la protección del USPS y sus clientes.

Los inspectores postales reúnen inteligencia útil de SAR sobre transacciones de giros postales sospechosas para descubrir las actividades sustanciales de estructuración o de lavado. Y su experiencia ha demostrado que los sospechosos que estructuran los giros postales son propensos a la estructuración de otras marcas de giros postales también.

Los inspectores pueden examinar la actividad de un solo SAR y, mediante la comprobación de múltiples bases de datos, vincularlo a muchas órdenes de pago relacionadas. Si bien sólo un pequeño porcentaje de todos los giros postales están vinculados a un SAR, en total aún representa una inmensa cantidad de datos que los inspectores minan con fines de investigación.

Ese es un buen argumento para una mayor cooperación a través de organismos y empresas de servicios financieros (MSB). Mientras más organismos y MSB colaboran y comparten datos, más difícil será para los delincuentes ocultar sus ganancias fraudulentas.

Robert Sheehan, gerente del programa de inspector postal, Servicio de Inspección Postal de los EE.UU., Washington, D.C., EE.UU., RBSheehan@uspis.gov

> It's kind of fun to do the impossible.
>
> — Walt Disney

With **SAFE Advanced Solutions®**, SBS helps clients do the impossible every day.

Our patented methodology for risk ranking large databases and probabilistic alert scoring determine the severity and probability of each alert to return only the most relevant, most accurate matches. That means no mountains of low quality or false positive alerts to investigate. And more time to focus on what is important — the highest risk, most likely to be true matches.

SAFE Advanced Solutions dramatically improves the efficiency of your AML and compliance operation while mitigating risk.

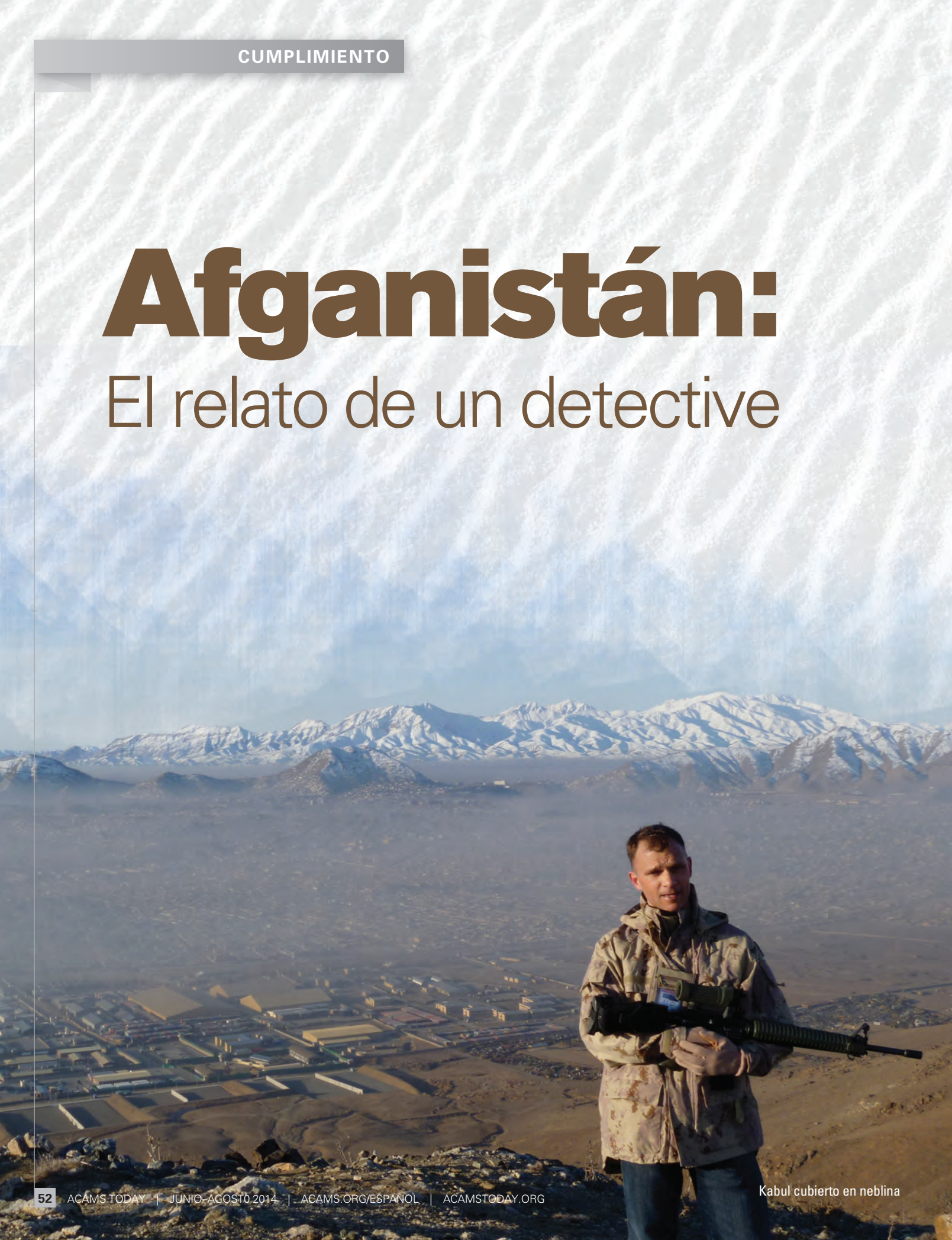
Let us show you how much fun it can be to do the impossible and achieve the lowest hit rate on the planet. Contact us at **sales@safe-banking.com** or **+1 631-547-5400.**

SBS®
SAFE BANKING SYSTEMS

www.safe-banking.com

Afganistán:

El relato de un detective



Kabul cubierto en neblina

El sol aún no había alcanzado su cenit en el horizonte cuando nos bajamos del autobús de la terminal a la pista del Aeropuerto Internacional de Dubai. Nos estábamos preparando para el tramo final de nuestro largo vuelo de Ottawa, Ontario, Canadá a Kandahar, Afganistán. Fue a mediados de febrero de 2011 y yo era uno de los cerca de 20 agentes de policía canadienses que se habían ofrecido, o, en mi caso, enérgicamente solicitado, formar parte de la Misión de Policía de Canadá en Afganistán. Nuestro pequeño grupo representaba media docena de agentes de policía municipal diferentes de todo Canadá, así como de la Real Policía Montada de Canadá (RCMP). Habíamos pasado juntos las últimas seis semanas de entrenamiento y asistencia a reuniones de información en la Escuela de Policía de Canadá en Ottawa, y la Base de las Fuerzas Canadienses en Kingston, Ontario. Mientras tomábamos nuestros asientos en la parte delantera del avión de pasajeros afgano para ir a nuestra misión de nueve meses, nuestro espíritu y entusiasmo eran altos; pero, la verdad, también había un poco de ansiedad.

La tripulación cerró la puerta con llave mientras nos acomodamos e hizo balance de la aeronave. Decir que este avión ya había tenido su época de gloria constituía un eufemismo. "Así que", me dije a mí mismo, "aquí es donde los aviones vienen a morir". Me reaseguré a mí mismo que el piloto era probablemente tan experimentado como este viejo avión. No pasaba nada. Entonces, llegó un golpeteo desde el exterior de la puerta de la cabina. La azafata corrió hacia la puerta y la abrió. Santo cielo, era el piloto, ¡había quedado fuera de su propio avión! Mis colegas y yo nos miramos con desconcierto nervioso, hallándolo tanto cómico como preocupante. Los agentes de policía tienen un sentido del humor bastante negro; es un filtro crítico necesario para ayudar a los oficiales de policía jóvenes a llegar hasta la jubilación. Algunos de nosotros se rieron diciendo que un piloto que quedaba afuera de su propio avión antes del despegue era como un oficial que iba al atraco a un banco dejando su pistola en el casillero. El piloto también se rió entre dientes mientras luchaba para asegurar la puerta de la cabina. Después de bajar el pestillo a golpes con una barra de metal y de maldecir diciendo que el avión era más viejo que él, ninguno de nosotros se reía.

Si usted no sabía que había agentes de policía canadienses trabajando en Afganistán sin duda nadie se lo enrostraría. De hecho, la mayoría de los canadienses ni siquiera sabe que estamos allá. Pero, hemos estado en Afganistán desde 2005. Hasta esta misión, casi todos los canadienses habían sido asignados a trabajar en Kandahar, principalmente con el ejército canadiense. Su misión se había centrado en el fortalecimiento de la capacidad de la Policía Nacional Afgana (ANP) de primera línea. Sus misiones incluyeron instruir en habilidades básicas de policía como el tiro, la colocación de esposas, la instrucción sobre estado de derecho, las relaciones entre la policía y los ciudadanos, y similares; todas cosas bastante estándar para un recluta de la policía. Por supuesto, Afganistán es todo menos estándar y el trabajo de ellos era peligroso y estresante.

Cuando peleé hasta lograr que me aceptaran en esta misión esperaba que me ubicaran en el Equipo de Reconstrucción Provincial (PRT) que opera desde Kandahar. Me había familiarizado con el PRT cuando estudiaba en la Universidad de Norwich en Northfield, Vermont y estaba ansioso de ser parte de uno. Sin embargo, un par de semanas antes de irnos de Canadá nuestra

misión cambió. El Contingente de la Policía de Canadá pasaría de proporcionar formación básica a la ANP en Kandahar a una misión más amplia y estratégica en Kabul. Canadá no tenía un proyecto de policía firme en Kabul y nuestro contingente se extendería por toda la ciudad para apoyar una serie de iniciativas de policía internacionales.

Después de pasar un par de días en Kandahar y dejar a tres de nuestros colegas para concluir la misión, el resto de nosotros voló hacia el norte de Kabul y de inmediato se dedicó a sus tareas. Algunos miembros fueron a la Misión-Afganistán de Entrenamiento de la OTAN (NTM-A) en Camp Eggers, unos a la Misión de Policía de la Unión Europea (EUPOL), uno fue a la Fuerza de Tareas de Delitos Mayores del FBI y yo fui a la Célula de Amenaza de Finanzas de Afganistán (ATFC). Es justo decir que este nombramiento será por siempre el mejor trabajo que he tenido.

La labor y la estructura organizativa de la ATFC han sido bien documentadas en los medios de comunicación estadounidenses y la ATFC ha sido recientemente galardonada con el Premio a la Unidad Meritoria Conjunta.[1] En pocas palabras, la ATFC está liderada por la Administración de Control de Drogas de los EE.UU. (DEA) y tiene dos componentes: el elemento militar dirigido por el Departamento de Defensa de los EE.UU. y el componente de aplicación de la ley liderado por el Departamento del Tesoro de los EE.UU. Me asignaron del lado de las autoridades de control legal y tuve la suerte de ser el primer canadiense del grupo. No estoy muy familiarizado con el funcionamiento del lado militar, pero sí sé que si yo fuera un financista terrorista sospechoso en cualquier lugar en Afganistán me gustaría que mi archivo fuera gestionado por el lado de las fuerzas del orden. El ejército de los EE.UU. es excepcional y sus archivos tienden a concluirse de manera diferente que las investigaciones policiales.

El lado de las fuerzas del orden era una unidad verdaderamente integrada con representación de la casi totalidad de las agencias de la policía federal de los Estados Unidos. Había agentes de la DEA, agentes del FBI, del Departamento del Tesoro, del Servicio de Impuestos Internos, del Departamento de Seguridad Nacional, así como analistas militares de los EE.UU. y de una empresa civil contratada. Los policías son más o menos lo mismo en todas partes de América del Norte y en muchas maneras están todos cortados de la misma tela. Inmediatamente me sentí como en casa con mis primos americanos. Nos reímos de las mismas cosas, compartimos muchas experiencias similares, y todos nos sentimos cómodos con las investigaciones. La DEA me trató como uno de los suyos y yo estaba muy mimado y agradecido por su hospitalidad.

Parte de lo que hicimos del lado de las autoridades de control legal (LE) de la ATFC fue trabajar en estrecha colaboración con un grupo especializado de investigadores de la ANP. Estos oficiales de la ANP fueron especialmente seleccionados y se les examinaba de forma continua. Ellos no eran reflejo del oficial típico de la ANP. Sabían leer y escribir, tenían conocimientos de informática y tenían habilidades de investigación superiores a la media. Un par de ellos eran policías verdaderamente inteligentes y audaces. Trabajaban en un edificio muy cerca de mi campamento y en los próximos nueve meses pasaría muchas horas laborales con ellos y en algunos casos hicimos amistad. La comunicación era un problema, pero sólo para mí. Su dari era impecable y el mío era francamente horrible. Así, cada vez que nos encontrábamos, siempre utilicé un traductor. Por supuesto, esto ralentiza todo el proceso, pero es la única manera de hacer las cosas.

La tarea que me asignó mi supervisor de la DEA era sencilla: Establecer un programa de capacitación de delitos financieros para los investigadores de la ANP e informarlos sobre la delincuencia financiera específica y el financiamiento del terrorismo.

Comencé por colaborar con el supervisor de la ANP e hice una encuesta de evaluación de necesidades junto a él. Quería saber qué destrezas pensaba que necesitaban sus hombres (y eran todos hombres) y con qué prioridad. Yo hice lo mismo con los propios investigadores de la ANP. También consulté a los comandantes de la DEA y mis compañeros investigadores de ATFC. Rápidamente urdí una planificación sólida y un programa de entrenamiento. Al igual que muchos comandantes de la policía, el supervisor de ANP se mostró reacio a que su pequeño grupo de oficiales dedicara dos o tres semanas a un curso largo. Había mucho trabajo que hacer y estar en un salón de clases por tanto tiempo no era una opción viable. Supuse que las sesiones de formación modular más cortas pero más frecuentes serían un buen equilibrio.

Organicé una serie de talleres de capacitación para los investigadores de la ANP. Construí lecciones y presentaciones sobre los estados financieros básicos y el antilavado de dinero. Contacté a mi propio servicio de policía, colegas de la Policía Montada, y de la Asociación de Examinadores Certificados de Fraude (ACFE), para un poco de ayuda con este material (por

Ken Brander enfrente de la Embajada de los EE.UU.

desgracia, yo aún no estaba enterado de la existencia de ACAMS). El ATFC aprovechó la influencia de su agregado de la Red Contra los Delitos Financieros (FinCEN) y pudimos organizar para que la Unidad de Inteligencia Financiera de Afganistán (FinTRACA) proporcionara una sesión también. Recibí ayuda de mis colegas de la policía canadiense en las misiones de EUPOL y NTM-A para el resto. La misión EUPOL me proporcionó los servicios de dos oficiales de policía alemanes para llevar a cabo una serie de tres talleres de entrevistas e interrogatorios. A través de la NTM-A tuve la oportunidad de que un fiscal afgano presentara un taller sobre la ley afgana y su relación con el lavado de dinero y el financiamiento del terrorismo. Lo crea o no, Afganistán ha promulgado una muy severa legislación nacional sobre el lavado de dinero y la financiación del terrorismo desde 2001, y la mayor parte de ella era noticia nueva para los oficiales de la ANP. El taller era en dari, así que probablemente fue el taller más eficaz e importante de la serie. Para los últimos dos meses de mi misión (con mucha ayuda de EUPOL) pude reunir todas estas lecciones en un manual y construir un curso avanzado de tres días sobre Delitos Financieros aprobado por el Ministerio del Interior afgano (MOI).

Desafíos enfrentados

Todo esto suena bastante rutinario y, en muchos aspectos, lo era. No había nada terriblemente emocionante o dinámico sobre esta parte del trabajo. Eran las pequeñas cosas en el camino que realmente presentaban desafíos. Por ejemplo, los estados de cuenta bancarios producidos por la mayoría de las instituciones financieras afganas están en idioma inglés. Es evidente que esto plantea un problema para los investigadores de la ANP que no pueden leer ese

[1] http://www.justice.gov/dea/pubs/pressrel/pr020812.html Accesado el 30 de marzo del 2014.

En la foto: Mercado hawala en Kabul

idioma. Además, la mayoría de los afganos no utilizan los servicios de las instituciones financieras y los términos bancarios no son muy bien conocidos por ellos. Como resultado, la lección comenzó con un glosario que definía términos como "créditos" y "débitos".

La segunda parte de mi tarea consistía en guiar y aconsejar a mi par de la ANP sobre determinados delitos financieros y de financiamiento del terrorismo en Afganistán. Durante mi misión, el fraude del Banco de Kabul fue el elefante gigante en la habitación. Este fraude bancario había sido bien informado y en 2011 amenazó con desestabilizar todo el esfuerzo de los aliados.[2] El relato breve es que unos pocos ejecutivos muy bien conectados en el Banco de Kabul se auto-adjudicaron alrededor de $800 millones en préstamos fraudulentos del banco y enviaron grandes cantidades de ese dinero al extranjero. Estos ejecutivos eran ellos mismos, o eran hermanos y allegados de la elite militar, política y tribal de Afganistán. Peor aún, los fondos que se robaron habían sido depositados por donantes internacionales, incluyendo los EE.UU. y eran las nóminas de la policía, el ejército y los maestros de Afganistán.

Mi pequeño pedazo del fraude del Banco de Kabul involucraba a un empresario afgano que lavaba dinero para uno de los ejecutivos del Banco de Kabul que cometió el fraude. No fue una investigación especialmente complicada. Pudimos obtener las autorizaciones judiciales para ver documentos bancarios y en poco tiempo pudimos seguir la pista del dinero, ya que fue robado del banco, depositado en las cuentas de la compañía de un ejecutivo del banco, y luego estructurado en capas en las cuentas del lavador de dinero, en la cuenta de la empresa de servicios monetarios (MSB) del New Ansari Exchange y luego enviado offshore a la cuenta de la Green Leaf Trading Company en Dubai.

El uso del New Ansari Exchange por parte de nuestro lavador de dinero para transferir el producto del delito del fraude del Banco de Kabul fue significativo. El New Ansari Exchange se originó en Kandahar, en la década de 1990. Este MSB trabajó con los talibanes transfiriendo ganancias de la economía del opio y después de 2001 desarrolló relaciones con los EE.UU., las Naciones Unidas y la OTAN. Los propietarios de la New Ansari diversificaron sus operaciones y fundaron el Afghan United Bank. Entre 2007 y 2010, este MSB transfirió $3,18 mil millones de Afganistán al extranjero y se convirtió en objeto de una investigación.

Cuando estudiaba las cuentas pude determinar que en el transcurso de unos pocos meses en 2008 nuestro lavador de dinero había estructurado por lo menos $27 millones para la compañía del ejecutivo bancario. En algunas ocasiones estructuraba varios depósitos muy grandes en su cuenta el mismo día y luego transfería de inmediato más de $1 millón a New Ansari. Durante esos mismos pocos meses estructuró más de $18 millones a través de Nueva Ansari. Ese dinero se abrió camino hasta Dubai. Tampoco se esforzó en ocultar sus huellas. Sospecho que era extremadamente confiado y no sentía la necesidad de ser cauteloso. Estaba lavando dinero para los asociados que se sentaban a la Mesa Presidencial de Afganistán. El tipo era un pez gordo con seguridad, pero la trama de lavado de dinero en sí misma no era muy complicada.

Sin embargo, siendo las cosas como son en Afganistán, nunca nada es sencillo. Reunimos las pruebas para llevar el caso a juicio. La ANP llevó a cabo la vigilancia y aconsejé sobre los planes de detención. Sería una empresa bastante grande con un montón de piezas de movimiento rápido con un objetivo de bastante alto perfil, pero mis colegas de ATFC y yo pensamos que era alcanzable. Era algo que nosotros mismos haríamos si estuviéramos en casa. Al final, la detención de este sospechoso y la orden de registro de su domicilio y recinto no sucedieron.

En verdad, yo no puedo hablar mal de la ANP en este sentido. A veces es necesario dar un paso atrás y si bien es fácil criticar, también es necesario considerar el contexto. Una tarde, casi al final de esta investigación, estaba sentado en la oficina pequeña, mal ventilada del supervisor de la ANP con mi par de la ANP, un par de otros investigadores de la ANP y de nuestro traductor. Yo estaba realmente presionándolo duro para ejecutar este plan de arresto y detener al tipo ese por algún delito. Me di cuenta de que se estaba enojando conmigo teniendo en cuenta que había estado presionándolo con dureza durante un par de semanas. Finalmente nos pusimos de acuerdo en dejar la investigación hasta un momento más adecuado.

Después, al reunirme con mi colega de la ANP, le pregunté si había exagerado y estaba exigiendo demasiado. Por respuesta, me preguntó: "Ken, ¿sabes cuánto cuesta asesinar a un policía en Afganistán? $250 USD". Bueno, eso es un poco de contexto bastante austero, supongo. Lo entiendo.

De hecho, ser un oficial de policía en el país más corrupto de la tierra puede ser sólo uno de los trabajos civiles más peligrosos que se me ocurren. Considere que el Ejército Nacional Afgano (ANA) se mantiene en la base y por lo general sólo se despliega para llevar a cabo misiones. La ANP, por otro lado, maneja los puestos de control de tráfico y patrulla todo el día y la noche. Mientras estaba en Kabul experimentamos algunos ataques insurgentes bien coordinados en la ciudad y fue siempre la ANP la que ocupaba esos puestos de control, los primeros en responder a los tiros de los insurgentes y la voladura de las calles. Estos policías fueron asesinados y heridos en números altos, mientras yo estaba allí. De hecho, tenga en cuenta sus pérdidas recientes: entre marzo y septiembre de 2013, la ANP sufrió 1.792 muertos en acción (1,14 por ciento de la ANP) y 2.700 heridos en acción (1,72 por ciento de la ANP). Eso fue sólo en seis meses. Desde el año 2003 han tenido más de 10.000 muertos en acción.[3]

Hay un montón de diferentes perspectivas sobre la ANP y Afganistán en general, pero esta es sin duda una de ellas. Esta es la que uso para que me ayude a ganar un poco de contexto sobre qué hice mientras estuve en Afganistán y por qué lo hice. Si alguna vez tiene la intención de aceptar uno de estos nombramientos, asegúrese de llevar un montón de empatía y paciencia. Las necesitará.

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

[2] http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/9706093/Kabul-Bank-diverted-540-million-to-group-of-12-in-massive-fraud.html Accesado el 30 de marzo de 2014

[3] http://www.presstv.ir/detail/2013/09/03/321812/1792-afghan-police-killed-since-march/ y http://news.yahoo.com/another-female-police-officer-shot-afghanistan-062545180.html Accesado el 30 de marzo de 2014.

Muéstrelo, no lo diga

Como líder de un equipo plurijurisdiccional de revisión de informes de actividad sospechosa (SAR, por sus siglas en inglés), leo docenas y a veces cientos de SARs a la vez. Al igual que un programador que lee las líneas de un código, mi cerebro ha aprendido a interpretar grandes franjas de los datos en cuadros o imágenes. Docenas de pequeños cables que llevan a un receptor en América Central se convierten en un caso potencial de trata de personas, y decenas de cables a un destinatario quien luego envía los fondos a una nación conocida por su actividad fraudulenta pintan un retrato familiar.

Al leer estos SAR, a veces me encuentro con uno donde el redactor claramente quiere decirme algo, al igual que una víctima de asfixia agitando una mano mientras se sujeta la garganta con la otra. Por desgracia, no puedo oír lo que el redactor está diciendo porque ya sea a propósito o accidentalmente, ha dejado fuera alguna información importante.

Cuando leo estos SARs recuerdo algunos buenos consejos de redacción que recibí de un profesor mío: "Muéstrelo, no lo diga".

> Incluyendo más información y detalles que menos en su SAR es mucho mejor

He aquí un ejemplo de un SAR que dice, pero no muestra: "Este SAR es para informar que Mary Jones se ha dedicado a una posible actividad estructurante que encaja en el perfil de la trata de personas. Las transacciones se realizaron entre enero 1 hasta el 2 de abril. Los registros están archivados y disponibles a pedido". FIN DE SAR.

Quien redactó está claramente tratando de ser útil. Él o ella ha incluido varias palabras clave y debe estar escribiendo este SAR con un genuino deseo de alertar a las autoridades que aplican la ley (LE). Sin embargo, paradójicamente, este SAR es el tipo más común de SAR que se pasará por alto. Quien redactó, por el contrario, puede creer que tan pronto como las LE lean su informe, el teléfono sonará. Por desgracia, lo contrario es cierto por varias razones importantes.

En primer lugar, las LE cuentan con recursos limitados. Tenemos un pequeño equipo de investigadores que leen y hacen el seguimiento de centenares de SAR cada año. Cada vez que revisamos un SAR nuevo tomamos una decisión acerca de qué casos se considerarán y cuáles se dejarán de lado.

En segundo lugar, lleva tiempo solicitar documentos justificativos. No toma mucho tiempo, por supuesto, pero todo tiempo malgastado en un caso es tiempo no dedicado a otro. El caso debe ser asignado, registrado, seguido por nuestro equipo y luego revisado para su seguimiento.

Por último, (y espero que ningún banquero se ofenda por esto), los redactores de SAR no son abogados y no son LE. Además, a menudo informan de la actividad que ellos creen que podría ser delictiva cuando no lo es. Sin embargo, esta es bueno porque es mejor que se nos informe de más que de menos. Aunque la mayoría de los casos que investigamos resultan actividad inocente y no delictiva, preferimos hacer esa llamada nosotros antes que usted y no podemos tomar esa decisión sin ver los hechos.

En consecuencia, cada vez que leemos uno de estos "SAR misteriosos" nos enfrentamos al mismo dilema: ¿Es esto realmente actividad delictiva? ¿Vale nuestro tiempo?

La mayoría del tiempo, nuestra respuesta es seguir y nunca solicitar documentos de apoyo. Nuestra esperanza, por supuesto, es que si la actividad continúa, tal vez el redactor del SAR escribirá un SAR mejor la próxima vez. De este modo, sabemos que corremos el riesgo de dejar de lado inadvertidamente actividad delictiva real. Es una elección de Hobson y desearía que nunca hubiera sucedido.

La solución, por supuesto, es simple: Mostrar, no decir. Sé a qué se parece la estructuración, así que muéstremelo. Por ejemplo, sea detallado: "Depósito el 1 de enero de $9.900 depósito el 2 de enero de $9.900, etc.) Además, sé lo que son los datos de casos de la trata de personas, fraude, contrabando y pornografía infantil, así que muéstreme los datos por escrito. Déme una razón para dar seguimiento al SAR presentado.

Incluyendo más información y detalles que menos en su SAR es mucho mejor. No se limite a decir que un cliente es sospechoso de estructuración. Detalle las operaciones que causan las sospechas y contrástelas con otras cosas que sabe de su cliente (KYC, por sus siglas en inglés). Por ejemplo, el "Cliente X hizo dos depósitos de $9.000 en dos sucursales diferentes con apenas horas de diferencia. Esto es inusual, porque el cliente es un empleado municipal y no había depositado dinero en efectivo en el último año y antes tenía un saldo de menos de $2.000".

A veces esta lección significa tener que preguntarse "¿Por qué me parece que este comportamiento obviamente sospechoso es sospechoso?" Después de todo, para usted el comportamiento podría ser obviamente problemático en función del perfil del cliente y la actividad sospechosa. Sin embargo, aunque usted conoce todo el perfil del cliente, un oficial de las LE sólo verá su SAR y ninguna otra información. Es más, ese oficial de las LE probablemente leerá su SAR en 90 segundos o menos y determinará si hay que hacer seguimiento o no.

Si "Muestra, no lo dice", logra que el funcionario siga los enlaces a la conclusión a la que usted llegó. Si el investigador se da cuenta de que los hechos realmente merecen su conclusión, es mucho más probable que le dé seguimiento.

De lo contrario, si su SAR intenta alertar a las LE de un delito o actividad delictiva sin suficiente descripción, será como que grita en una habitación vacía. Por supuesto, me doy cuenta de que a veces su trabajo lo hace sentir como que está gritando en una habitación vacía. Sin embargo, lo cierto es que alguien realmente está escuchando; de hecho, estamos leyendo regularmente sus SAR y que son importantes para nuestro trabajo en la aplicación de la ley. Sabemos que los que estamos en la aplicación de la ley siempre podemos mejorar, y tal vez este consejo lo ayudará a usted o a su equipo a hacer un producto mejor también.

Elliot Casey, fiscal asistente, oficina del fiscal de EE.UU., Charlottesville, VA, EE.UU., ecasey@albermale.org

Programa Ciber-respuesta: Las primeras 48 horas...¿está listo?

Durante el último año, las responsabilidades de seguridad cibernética han sido evitadas, desviadas y pasadas a otros departamentos dentro de las organizaciones. Algunos gerentes de empresa, directores y hasta ejecutivos pueden haber negado que se hackeó, tal vez debido a la falta de conciencia. También ha habido disputas sobre que no hay culpabilidad para sus respectivos departamentos para "preocuparse" por la intrusión. Afirman que es problema del sector de tecnología de la información (IT) y que esos individuos en IT deben responsabilizarse de la resolución de los problemas.

Cuando volvemos la mirada a sólo los últimos cinco años, la persona menos analítica se da cuenta de que existen múltiples facetas de un ataque cibernético. Afectan no sólo a la empresa, sino también a los distintos departamentos que pueden haber intentado originalmente evadir la responsabilidad de ayudar con la reparación. Si usted no ha considerado un Programa de Ciber-respuesta (CRP, por sus siglas en inglés), entonces tal vez sea hora de evaluar su riesgo.

Las primeras 48 horas

Cuando se produce una intrusión cibernética, las miradas van inmediatamente a los informáticos de la empresa. Esto es correcto, son la primera línea de defensa y se encargan de la seguridad de sus entornos, pero ¿qué pasa con el segundo día, el séptimo día o el día 20? Las primeras 48 horas son las más críticas para una iniciativa de respuesta de su organización. ¿Se detiene allí con IT? Muchos han dicho "Sí". Pero la reducción del riesgo se extiende por toda la empresa, y el ataque no debe descansar sobre los hombros de sólo el departamento de IT. Es así, gente de informática, respiren aliviados, pero sólo un poco, todavía juegan un papel fundamental.

¿A quién involucramos?

Se ha producido la intrusión. ¿Y ahora qué? ¿Quién toma la iniciativa? Fuera de los grupos de IT, la mayoría de las organizaciones cuentan con áreas para las operaciones de riesgo. Ellas pueden ser responsables de cumplimiento, seguridad física, posiblemente auditoría y muy probablemente el antilavado de dinero (ALD) y las investigaciones de fraude. Evidentemente, esta no es una lista completa y dependiendo de la estructura de su organización, puede que no todas ellas estén incluidas en su departamento de riesgos. Pero con experiencia y acceso a la información, hay recursos claves para ayudar a una empresa a resolver y responder a un ataque cibernético rápidamente.

Una palabra que se ha vuelto más frecuente en estos días es: "colaboración". Los primeros días de romper los silos internos de los departamentos polítizados probablemente se produjeron debido a los programas de cumplimiento de ALD. Estos programas dieron lugar a esfuerzos de colaboración con el fin de reunir la mayor cantidad de información posible en un grupo, para así decidir adecuadamente sobre la identificación y denuncia de una actividad sospechosa. A medida que evolucionaron las organizaciones y se pusieron en marcha requisitos más rigurosos de parte de las agencias reguladoras, los departamentos de ALD y fraude comenzaron a compartir los datos recogidos durante sus investigaciones. Como resultado, más paredes empezaron a derribarse cuando los departamentos de ALD y fraude comenzaron

a compartir los datos recogidos durante las investigaciones. Los esfuerzos de exámenes internos y externos en última instancia aseguraron que ambas áreas de investigación se encontraban cubriendo los vacíos en toda la empresa para mitigar el riesgo de que un grupo pueda estar informando sobre un cliente mientras que el otro simplemente cerraba el caso. Este nivel de colaboración entre los departamentos alineó los equipos y el conocimiento compartido, confirmó que los hallazgos de investigaciones sincronizaban y que una disposición adecuada se lograba para la empresa en general.

Los jefes de riesgo, de IT y de cualquier otro departamento considerados de participación razonable, deben formar un grupo de tareas cooperativo para hacerle frente de inmediato a la amenaza. Tenga en cuenta que hay que formar este grupo de tareas antes de que ocurra un evento; y que debe estar en estado de alerta para enfrentar un ataque. En el centro de este equipo se encuentran sus recursos técnicos. IT confirma que se ha producido la intrusión. Asegura los sistemas para que ninguna otra información quede capturada inmediatamente por el hacker. Identifica el cómo, qué y cuándo. ¿Cómo se comprometieron los entornos? ¿Qué datos quedaron al descubierto? ¿Cuándo entró el hacker por primera vez al sistema hasta el punto donde la información se impidió de salir de la base de datos? Está claro que hay una multitud de funciones, pero para los propósitos de este artículo, vamos a mantenerlo limitado a CRP 101.

Reúna a las unidades de caballería

Deberían reunirse a los caballeros de la mesa redonda con todas las partes, como por ejemplo, y sin duda sin limitarse a, márquetin, seguridad física, la(s) unidad(es) de investigación, informática e incluso auditoría. Los datos desde el primer día deben ser compartidos y comentados. Cada miembro del equipo será responsable de sus áreas de especialidad para asegurar que toda la información se comparte y que van a ser la autoridad que representa a su departamento mientras se trabaja con el grupo de tareas.

Márquetin se encargará de la prensa y la reputación de la organización. Lo peor que puede hacer una empresa es dejar de informar o tratar de ocultar que se ha producido una violación de datos. Como se dijo anteriormente, el propósito principal de la iniciativa CRP es asegurar la transferencia de conocimientos y desarrollar un plan de acción basado en los acontecimientos del ataque. Se puede necesitar desarrollar una campaña para su uso posterior a medida que se examina el caso presente. En el mejor de los casos: no se tomaron datos y usted pudo detener el ataque antes de que hubiera una pérdida. Utilice esto para su beneficio anunciando orgullosamente que hubo un intento significativo y que se detuvo al intruso y salvó a sus clientes de formar parte de las estadísticas. En cualquier caso, debe haber preparación para asegurar que un fuerte mensaje esté listo, de ser necesario.

Las investigaciones internas/de seguridad física deben ser una parte de su proceso también. A medida que continúa el examen, los investigadores de seguridad física/internas deben preguntarse a sí mismos: ¿Hubo alguien de adentro que ayudó con el ataque? ¿Se ha producido una violación del perímetro que puede haber sido captado por la cámara que no se ve ni se alertó? ¿Hay brechas que pueden ser identificadas y llenadas para evitar una mayor intrusión? ¿Hubo empleados nuevos con acceso a los sistemas afectados que pueden haber tenido la oportunidad de colocar el malware?

Involucre a su equipo de investigadores y deje que ellos hagan lo que mejor saben hacer, reunir y correlacionar todas las pruebas recogidas por el grupo de tareas. La(s) unidad(es) de investigación inician la evaluación de los datos y la información que le(s) fue robada. Confeccionan el caso y comienzan la construcción de una investigación en torno a todo el evento. Su sistema de manejo de casos es una herramienta colectiva para su grupo de tareas, por lo cual todo el mundo puede compartir su información y mantenerla almacenada en una ubicación. Si es necesario, ellos trabajan con la policía y retienen la información adecuada y pruebas necesarias para promover la identificación de los sospechosos. ¿Hay algo relevante acerca de los datos robados? ¿Cómo puede el atacante usar los datos obtenidos? Un dossier del ataque será fundamental para obtener una perspectiva limpia y concisa del evento y la actividad documentada por los otros miembros del equipo. Al hacer una presentación a las agencias, debe presentarse un frente unido. Su reputación e ingresos están en juego.

En el caso de un ataque, ¿por qué querría que auditoría interna participe? Porque son su primera línea de defensa cuando se trata de los reguladores y la mayoría de ellos pueden sacar el máximo partido; es su trabajo. Ellos estarán examinando la información y facilitando la información pertinente a los organismos involucrados para asegurar que haya controles en el lugar y que los planes de acción están en vigor. Este será un tema muy delicado y el momento será fundamental. La difusión de la información adecuada en el momento adecuado dará el resultado bueno o malo de un examen externo. Usted necesita su apoyo y necesita aprovechar sus capacidades para demostrar que la organización tiene los conocimientos adecuados para corregir el problema y seguir teniendo una buena reputación en lugar de parecer incompetente.

IT cae de su peso cuando se trata de una ciber-intrusión. Ellos estarán buscando cada abertura y cada punto de entrada para evitar no sólo otra intrusión, sino también estarán construyendo barreras contra futuros intrusos. Los hackers tienen una comunidad—se lo aseguro—una vez que se descubre que existe una vulnerabilidad, van a encontrar varias más de las que aprovecharse. IT tiene que estar un paso o más delante de ellos; deberían identificar los puntos vulnerables antes de que otros lo hagan. Haga un simulacro utilizando a su personal interno de mayor experiencia con los recursos que tiene para defenderse y protegerse. Es un juego de ajedrez para estos atacantes, sólo asegúrese de que usted gane.

Hay muchas otras facetas en función del tamaño, la complejidad y el tipo de industria que afecta a la participación de los departamentos y los miembros del equipo. Los mencionados anteriormente son sólo un ejemplo de quiénes podrían ser sus colaboradores internos. Una evaluación debe llevarse a cabo para identificar los recursos y construir un CRP antes de un incidente. Usted no necesita contratar recursos costosos cuando se tienen departamentos e individuos internamente bien equipados. Es posible que sólo necesite una persona que tome el mando y construya los equipos necesarios para reunirse en caso de ataque.

Conéctese y comunique

Reagrupe, comunique y absorba. ¿Qué han descubierto los otros equipos y cómo se conecta con la información que otro miembro del equipo ha encontrado a través del simulacro? ¿Ha habido alguna exposición a los medios y se preparan declaraciones en caso de que sea necesario un anuncio? ¿Investigaciones internas/seguridad física ha identificado a algún sospechoso? Va a haber muchas preguntas y cada miembro del equipo tiene que tener consciencia de la respuesta.

Un CRP va a ser una nueva iniciativa que permita agilizar y ahorrarle dinero y daños a la reputación a la organización si se gestiona adecuadamente. Claramente, esta es la versión de Cliffs Notes; ya que hay una mayor cantidad de detalles detrás de cada paso que debe tomarse. No se puede escapar de una ciber-intrusión y dejárselo todo a IT. Se necesita una aldea para defenderse contra un ataque. Si usted no ha considerado un CRP, entonces es hora de empezar a mitigar el riesgo para su organización al ver la infraestructura de su empresa y la identificación de la calidad de los recursos internos que están listos para responder.

Cameron T. Jones, CAMS, director, Inteligencia de Seguridad de SAS, Chicago, IL, EE.UU., cameron.jones@sas.com

La convergencia basada en la colaboración en la prevención de delitos financieros: **Soluciones para intercambiar datos de referencia**

La implementación de una nueva aplicación de antilavado de dinero (ALD) expone las necesidades y los problemas que requieren soluciones prácticas complejas. El panorama de ALD se encuentra en constante cambio. Mientras que la gran estrategia de ALD y convergencia del fraude (convergencia de delitos financieros) sigue progresando, la colaboración y línea de visión fehaciente es un buen comienzo. La convergencia finalmente juntará a los grupos de fraude y ALD, pero hoy en día, muchas organizaciones aún tratan el fraude y el ALD como procesos completamente separados. Sería difícil forzar los procesos y datos de forma rápida por lo que un modelo de colaboración es un buen primer paso. Aunque la convergencia basada en la colaboración se refiere a los procesos y datos dentro de una organización, también hay partes externas que pueden jugar un papel. Por ejemplo, las autoridades que aplican la ley podrían desempeñar un papel similar al de un Centro de Servicios de Medicare (CMS) definiendo o mejorando el significado de los datos de referencia para mejorar la coherencia y la comparabilidad de las comunicaciones de las instituciones supervisadas.

Como parte de cualquier aplicación nueva o transformacional de ALD, es necesario revisar el panorama actual de los procesos comerciales, modelos de organización, información y tecnologías. Una de las tareas más comunes en una nueva implementación consiste en asegurar que todas sus transacciones son adecuadamente tenidas en cuenta en la nueva aplicación. Muchos de los bancos y cooperativas de crédito pequeños y medianos tercerizan su plataforma de banca o tienen niveles significativos de contratistas/contratos con terceros que hacen el mantenimiento de sus aplicaciones internas, por lo que el conocimiento de las peculiaridades de las transacciones puede ser escaso. Estas instituciones se enfrentan a algunos de los mismos niveles de regulación, control y riesgo que las instituciones más grandes, sobre todo al traspasar el umbral de $10 mil millones de activos. Reducir el riesgo de las grandes instituciones es aumentar los riesgos para las instituciones más pequeñas ya que los comportamientos y los clientes más riesgosos migrarán a instituciones menos protegidas.

A modo de ejemplo, una empresa de gestión de inversiones con operaciones bancarias comenzó una nueva implementación de aplicaciones de ALD. Entre muchas de las tareas estuvo la de la integración de los datos de la transacción y su mejora con conceptos adicionales. A cada transacción se le asigna un tipo de transacción por la aplicación que la procesa. El tipo de transacción se denomina "datos de referencia" y es sólo un ejemplo entre cientos que se necesitan para implementar un sistema de ALD. Pero hay cuestiones y preguntas que rodean el tipo de transacción:

- Siempre es conveniente identificar el dinero en efectivo con mayor claridad en los datos de las transacciones, aunque algunos sistemas de código hacen más difícil lograrlo de manera coherente. Dependiendo de cómo funciona su sistema de transacción, puede ser difícil identificar dinero en efectivo en los datos de referencia de la transacción.
- Múltiples líneas de negocio (LOB) cada uno de los cuales utiliza diferentes sistemas y procesos, la identificación de los tipos de transacciones y la comprensión de las diferencias y los matices pueden ser muy difíciles.
- A menudo hay varias hojas de cálculo, varias versiones de las hojas de cálculo muy similares, documentación del proveedor, configuración del proveedor e información de configuración del sistema de ALD actual que tienen que configurarse conjuntamente.
- A menudo hay miles de códigos de transacción para revisar con el fin de conocer, identificar las limitaciones, administrar y conciliar.

La mayoría de los sistemas de ALD asumen que usted está proporcionando datos de entrada limpios y no pueden normalizar y garantízar la integridad de los tipos de transacciones y otros datos de referencia críticos. Por lo tanto, típicamente le toca a la institución resolver estos problemas a través de algún otro mecanismo.

Los tipos de problemas mencionados anteriormente sugieren que un ejercicio simple de tecnología de la información (IT) podría resolverlos. Sin embargo, la empresa tiene que ser dueña de este trabajo ya que este tipo de análisis lleva a la visión que permite priorizar mejor las actividades del proyecto utilizando un enfoque basado en el riesgo. Por ejemplo, es necesario que se comprenda y analice sus transacciones para entender la materialidad de las operaciones de cable de su negocio. Pero las transacciones de cable pueden ser de una prioridad más baja para la nueva aplicación en comparación con la comprensión de los procesos de pago de jubilación en una suma global porque los pagos de sumas globales pueden tener un patrón de pagos más grande y de una ambigüedad mucho más difícil de eliminar. El cumplimiento, la gestión de riesgos, la auditoría interna y los examinadores de fraude internos también juegan un papel importante contribuyendo a un conjunto estándar de tipos bien definidos, códigos y otros datos de referencia, junto con las definiciones y reglas para su uso.

Hay algunas preguntas que usted puede utilizar para medir la complejidad de su aplicación y entender cuál es el nivel de solución que tiene sentido en torno a los datos de referencia:

- ¿Es necesario escanear rápidamente un negocio de múltiples proveedores o de múltiples LOB para comprender el estado de los datos de las transacciones y todos sus datos y procesos críticos de ALD, manteniendo una línea de visión continua en las operaciones y los cambios?

- ¿Normalmente siente que necesita hablar con un conjunto amplio de personas a través de la organización, la consolidación de los resúmenes de las "instantáneas actuales" y siempre están tratando de mantenerse a la vanguardia de las preguntas en torno a "¿Qué ha cambiado?" O "¿Cuál es la estado actual?" o "¿Cómo va todo?" ¿Usted también siente que debe haber una manera más fácil de responder a estas preguntas?
- ¿A menudo asiste a varias reuniones dirigidas por diferentes grupos donde todos parecen estar haciendo preguntas muy similares acerca de datos y usted no está muy seguro de quién está a cargo, o cuál es el proceso que están siguiendo o si alguno de estos grupos están coordinados entre sí?

Si las respuestas a estas preguntas son más "sí" que "no", entonces usted necesita pensar cómo resolver este problema de gestión de la información. Mientras que una sola aplicación de ALD y fraude es una visión agradable, es muy difícil y costosa y, desde el punto de vista organizacional, es difícil lograr una visión de una única aplicación hecha de manera oportuna. Durante la implementación de la nueva aplicación de ALD, es necesario encontrar una manera de abordar los problemas de forma incremental. La gestión intencional de estos temas lo ayuda a usted a evitar planes de acción interinos, costosos, que distraen de sus auditorías internas o revisiones del regulador.

Experiencia de método de solución: Colaborando temprano y con frecuencia

Considere una organización con las siguientes características (algunas de estas pueden resonar con sus experiencias):

- Varias LOB principales centradas en un segmento de clientes y canal de ventas específico.
- Una nueva visión desarrollada por una firma de estrategia que se centra en la convergencia mediante una estrategia de una sola aplicación, tanto para ALD y fraude.
- Personal muy fuerte y apasionado en la LOB, pero menos precedencia histórica en torno a "una" visión de la empresa.
- Tercerización significativa a proveedores de aplicaciones con focos aislados de aplicaciones de cosecha propia dedicados a un solo producto o una tarea.
- Superposición y madurez muy variable en la disponibilidad de datos, la comprensión y la experiencia. Existen múltiples aplicaciones para casi todas las necesidades, pero muchas personas de la organización reconocen que los pensamientos expresados en el apartado anterior se aplican a su organización.
- El primer arco de la implementación del ALD enfoca un subconjunto de productos y servicios de una línea de negocio, hay tres aplicaciones a las que se enfrentan los principales clientes, aproximadamente 30 aplicaciones de oficina media y ningún único conjunto de documentación de cualquier grupo o sistema coherentes entre sí en su totalidad.
- El intercambio de datos de conozca a su cliente (KYC) para fines de regulación y de riesgo se lleva a cabo de manera incoherente.

Mientras que la visión a largo plazo pedía una sola aplicación en toda la empresa, se puede pronosticar con facilidad que podría haber una cantidad significativa de tiempo antes que el nuevo sistema pudiera cubrir todas las operaciones de la delincuencia financiera.

Sobre la base de este escenario, se debe considerar la creación de un repositorio de datos de cumplimiento (CDS). Un CDS es una solución de gestión de datos y control de versiones que une los ambientes de ALD y fraude, así como la gobernanza, regulación y suite de cumplimiento (GRC). A partir de la descripción de la solución de más abajo, es posible reconocer que muchos aspectos de esta solución tienden a ser implementados de forma manual a través de la organización y, a menudo usando procesos ad hoc, a destiempo y mal documentados o varias aplicaciones complejas.

¿Cuáles son los ingredientes clave de una solución?

La idea básica es crear un nexo en la organización que no es tan grande pensando como una sola aplicación de "el mundo", y reconoce la necesidad de tener un poco de centralización de los activos que generalmente son difíciles de encontrar y para los cuales hay varias versiones—muy similar a la descripción en torno a las transacciones mencionadas arriba. Equilibrar la sencillez con coste asegura que la solución sería tener una rápida comercialización, así como un nivel razonable de financiación y apoyo de la ejecución.

El concepto de CDS reuniría la información y proporcionaría capacidades en un solo lugar. Estas capacidades incluyen:

- Normas históricas y datos relacionados (como datos de referencia), incluyendo una pista de auditoría de cambios.
  - —Si bien las reglas están mejor documentadas en los sistemas existentes que las utilizan, algunas aplicaciones pueden ya haber sido retiradas y no pueden ser inspeccionadas por las normas o las reglas se mantienen en hojas de cálculo.
  - —A pesar de que las reglas cambian en el nuevo sistema, deben almacenarse y auditarse en los CDS.
- Historial detallado de la actividad, cambio de cuenta de línea y cliente para tener en cuenta la relación de línea.
  - —Su conocimiento de las relaciones cambia con el tiempo. Muchos sistemas actuales puestos específicamente para capturar esta información—el grupo de IT denomina estos sistemas sistemas de gestión de datos maestros—puede dejar de apoyar una amplia variedad de requisitos de ALD y fraude. La captura de un conjunto minimalista de "relaciones" mejora la captura de lógica y la capacidad de retro-examinar.
- La clasificación del riesgo
  - —Migración de los datos de riesgo que se relaciona con el modelo de las instituciones financieras de calificación de riesgo para todos los delitos financieros (fraude/ALD) y los requisitos de cumplimiento.
  - —Datos históricos, incluyendo pero no limitados a la información anterior de riesgo definido en relación con los productos y servicios prestados por la institución financiera tienen que ser recogidos de fuentes dispares. Esto incluiría reunir esta información de varios sistemas bancarios centrales después de una fusión o adquisición. Los datos históricos primarios (front end en inglés) y secundarios (back end en inglés) deben estar integrados a través de líneas de negocio en la nueva organización.
  - —Los cálculos de los riesgos deben basarse matemáticamente, llegando a una cifra que combina los datos de una amplia muestra de posibles tipos de riesgo que se relacionan con el fraude universal y conductas de lavado de dinero, no sólo de los silos segmentados anteriores.
- Pista de auditoría de la diligencia debida
  - —Actualizaciones y análisis de noticias negativas, así como lista de sanciones/vigilancia y revisiones relacionadas (piense 314s) deben registrarse como evidencia de las medidas del programa de ALD de diligencia debida.
- Métricas de procesos de negocios, tales como el número de casos, número de comentarios, registro de actividad, etc.

— La granularidad específica de las métricas tendrá que ser diseñada. Por ejemplo, a veces las estadísticas resumidas por días, semanas o meses son suficientes.

— Si las métricas de procesos de negocio ofrecen alta precisión, a continuación, los CDS también podrían desempeñar un papel de proporcionar datos para cuadros de mando e informes ejecutivos.

- Historial de controles de datos y alertas de datos

  — Controles de datos monitorean sus datos a medida que fluyen a través de su empresa. Las alertas pueden ser generadas, similares en concepto a una alerta de ALD, si se detecta algo sospechoso en los datos. Un control de datos no está tratando de reproducir normas de ALD o cálculos de calificación de riesgo, sino que se centra en la información relacionada con los datos correspondientes a las operaciones basadas en datos de ALD. Por ejemplo, cuestiones como que los números de identificación fiscal no coinciden en todo o cuentas mal formateadas. Las alertas de datos se crean sobre la base de los umbrales establecidos en la normativa.

  —La captura de versiones de los controles de datos y su lógica o reglas permite el análisis de los impactos, así como el retro-examen antes de su adopción.

- Historial de caso modificado/de gestión de legado de sistemas de ALD

  — Por lo general, una razón empresaria para una nueva aplicación de ALD o fraude es la reducción de costos de las licencias y del sistema. La eliminación de un sistema de ALD existente puede significar que usted necesita almacenar los datos de legado de ALD por separado, pero aún tenerlos disponibles para consulta. La posibilidad de consultar datos de un sistema retirado destaca el concepto de ciclo de vida de los datos.

  — La conversión a un formulario normalizado de datos también permite el retro-examen y el retro-aprovisionamiento de datos para casi cualquier auditoría concebible o requisito de revisión regulatoria sin contratar a un ejército de consultores o proveedores.

- Soporte de migración para el sistema de ALD legado

  — Proporcionar soporte para la migración es típicamente parte de explicar cómo la nueva aplicación de ALD es diferente de la anterior, pero la comparación de resultados y la explicación de las diferencias. Una línea de base se debe establecer y actualizar en el contexto de la migración.

  — Fechas de vencimiento y de desmantelamiento fijas (sí, realmente apagar algo y eliminarlo junto con la eliminación de los servidores antiguos y de almacenamiento) es un compromiso fundamental de costo/beneficio realizado por los programas de migración. Al darse cuenta de estos beneficios es crítico, así como lo es evitar conjuntos de datos "huérfanos" y códigos de aplicación.

Este conjunto de capacidades son impulsados por las dificultades específicas que muchas organizaciones enfrentan a medida que actualizan sus entornos. Crear una solución para implementar estas capacidades supone que una colección de datos tabulares y otros tipos de datos no tabulares se debe mantener en el CDS. Un CDS no es un sistema de gestión de documentos y no es una base de datos de operaciones o aplicación de gran complejidad. Tampoco debe ser una colección de sistemas de gestión de datos muy dispares, por ejemplo, un sistema de IT orientado por mayor capacidad. Un CDS debe proporcionar juegos de historia con estado de datos relacionados, la mayoría sólo para lectura para preservar pistas de auditoría y retrovisión, así como "las cadenas de evidencia" para los cambios efectuados en las normas y los umbrales. A medida que se producen cambios, usted captura su lógica y puede "retro-examinar" resultados más fácilmente.

La idea central de un CDS es automatizar un entorno integrado y controlado en el que se reúne una cantidad de información tallada para ayudar a responder preguntas y estar al tanto de los cambios. Para un profesional de IT, el nombre puede implicar una "muy estructurada base de datos orientada a transacciones", pero para los profesionales de ALD o los de fraude de negocios en toda la compañía, el nombre debería implicar un lugar fehaciente para "almacenar datos de cumplimiento" que constantemente necesita organización y revisión. Los miembros de las fuerzas del orden y de la comunidad de inteligencia deberían ver estos almacenes de datos como una forma más fiable de las instituciones reguladas y supervisadas para proporcionar una pista de auditoría profunda de datos estandarizados. Deben esperar que las instituciones supervisadas para desarrollar algo como un CDS y demostrar la madurez en sus prácticas de gestión de datos. Las agencias federales necesitan más coherencia, calidad e historia de sus esfuerzos para integrar datos institucionales con sus propias fuentes de datos. El CDS proporciona un conjunto estable de valores estandarizados junto con conjuntos de datos históricos precisos y detallados para apoyar las presentaciones regulatorias, así como respuestas para el descubrimiento y análisis más complejo.

Las fuerzas del orden pueden ayudar proporcionando ejemplos de formatos y especificaciones de los datos, al igual que sus pares en otras áreas del gobierno, como hace el CMS con los formatos y códigos de datos sanitarios. Hay ejemplos similares de la SEC y del Tesoro para la información financiera. Las respuestas a las consultas de hacer cumplir la ley a las PYMES en constante evolución de sus capacidades de cumplimiento podrían utilizarlas para simplificar sus esfuerzos y proporcionar respuestas fáciles de entender. Las fuerzas del orden también pueden proporcionar información sobre la eficacia de las respuestas de datos actuales a sus consultas para ayudar a las instituciones a mejorar sus respuestas. En concreto, la retroalimentación sobre la coherencia y comparabilidad de los valores de referencia (por ejemplo, los códigos y los indicadores de condición) ayudará a las instituciones a sintonizar sus datos de referencia en los almacenes de datos de cumplimiento. En tercer lugar, las fuerzas del orden pueden participar de manera más directa con las asociaciones de la industria, incluyendo ACAMS, para poner de relieve las mejores prácticas y los resultados actuales en la industria, en particular para los desafíos legales emergentes tales como la moneda virtual.

La gestión de los datos de referencia, tales como los tipos de transacción, es sólo un ejemplo donde un CDS proporcionaría una pista de auditoría directa que es históricamente precisa. Un CDS representa una forma de un enfoque de colaboración más simple en el camino hacia un estado final de "convergencia". También es una manera reflexiva para promover la colaboración sobre delitos financieros al tiempo que reconoce la naturaleza pragmática de su estado actual. Usted ya realiza algunas de, si no todas, estas funciones de forma manual y, probablemente, de manera incoherente. Reglamentos, auditorías y otros cambios serán constantes en el área de prevención de delitos financieros. Dé un paso práctico para que sea un proceso repetible, operativo.

Gregory Lampshire, socio, K2 Solutions, Reston, VA, EE.UU., glampshire@k2-solutions.com

Dan Meers, presidente, K2 Solutions, Reston, VA, EE.UU., dmeers@k2-solutions.com

Robert A. Goldfinger, CAMS, presidente, NominoData LLC, Incline Village, NV, EE.UU., rgoldfinger@nominodata.com

ALD AL INVERSO

Puede ser que poner su planificación investigativa de antilavado de dinero (ALD) en la inversa podría en realidad actualizarla?

Por su mayor parte, el ALD se enseña e investiga desde una perspectiva de arriba hacia abajo. Los casos son diseñados comúnmente siguiendo los fondos sospechosos hasta llegar a un culpable. Esto puede estar bien para destacarlo en titulares o cuando se trata de violaciones en mega-dólares; sin embargo, si usted se encuentra más a menudo involucrado en las tramas más habituales y comunes usted podría encontrar que iniciar a la inversa puede ser el mejor enfoque de investigación. Trabajando a la inversa desde el culpable hasta llegar al dinero puede descubrir algunos enlaces sorprendentes y valiosos.

Aunque resulta agradable resaltar las grandes sumas y los casos teatrales grandes para conferencias, seminarios y presentaciones de capacitación, hay muchas más tramas de lavado de dinero de rutina bien dignos de consideración de aplicación seria. Por desgracia, ese enfoque común de investigación de arriba hacia abajo puede hacer que se quede corto en las pruebas necesarias para demostrar estos casos. Empezando por el culpable y trabajando hasta el dinero, usted puede encontrar algunos lugares sorprendentes donde se desembolsan fondos ilícitos. Las banderas rojas de alerta que usted está buscando pueden estar en los detalles aparentemente menores de la vida diaria que usted puede haber pasado por alto y donde el que es el objetivo de su investigación nunca se dio cuenta de que era vulnerable.

Las tramas de lavado de dinero normalmente se desarrollan en torno a una negación plausible en cuenta a la planificación. Las personas implicadas (y al final todos los casos se reducirán a un individuo) tendrán una historia cubridora bien practicada que servirá para las dudas sobre el sistema de dinero a sabiendas ilícito. Las dudas irreprochables son algo muy poco atractivo para los fiscales. Los culpables se preparan normalmente para desviar las actividades sospechosas fácilmente identificables. En los peores casos, cuando los investigadores no han cavado más profundo en estas desviaciones, los culpables han sido capaces de dar vuelta la mesa y describirse como víctimas inocentes de investigadores que se extralimitan o tienen celo en exceso. Estas falsas representaciones podrían haberse expuesto si los investigadores no hubieran limitado su enfoque a las actividades a menudo más grandes y que acaparan la atención y que probablemente sirvieron de base para el lanzamiento de la investigación inicial.

El enfoque de abajo hacia arriba

Hay algunas premisas necesarias para un enfoque investigativo desde la base para arriba. En primer lugar, los canallas gastarán o buscarán la manera de disfrutar de los frutos de sus labores ilícitas. Siempre habrá problemas inherentes al tratar de dispersar grandes cantidades de dinero en efectivo o un ingreso continuo de dinero basado en negocios ilícitos. Es un error creer que el dinero malo se limitará a tipos muy grandes o específicos de transacciones. Los elementos de las tramas de lavado de dinero manchan casi todos los aspectos de sus vidas. Usted nunca debe limitar su ámbito de investigación o subestimar cómo y dónde se hará.

En realidad, el enfoque de la base hacia arriba debe empezar por conocer cómo un culpable mantiene una casa. Aparte de la comida, la vivienda es la mayor consideración de nuestra supervivencia financiera e incluso global. Por lo tanto, nunca debe tomarse a la ligera como parte de cualquier investigación financiera, ya que no será menos importante en la vida de un canalla de lo que es en la suya. Tradicionalmente consume un gran porcentaje de nuestros ingresos; por lo tanto, es un lugar muy popular para dispersar las ganancias mal habidas. Usted se sentiría apremiado por encontrar una investigación exitosa de lavado de dinero donde la vivienda no era un factor. Puede que no haya sido siempre parte del caso principal, pero cualquier análisis de detrás de escenas probablemente revelará su papel.

Si el culpable tiene una hipoteca, usted tiene un tesoro de pistas potenciales. Las solicitudes de hipotecas a menudo contienen información financiera o de las conexiones que no se encuentran en otros lugares. En el enfoque de base hacia arriba es necesario identificar exactamente cómo se paga esa hipoteca. Si no es de una cuenta de retiro directo o un cheque periódico de una cuenta, usted tiene ahí una pista. Si usted encuentra otras formas de pago, necesita examinarlas.

Si el culpable no paga una hipoteca regular o alquila una vivienda, es importante saber quién lo hace o por qué no. Proporcionar vivienda a otra persona no es una decisión hecha a la ligera. Incluso si es parte de una dinámica familiar, rara vez se lleva a cabo de forma gratuita. Un no miembro de la familia abre la posibilidad de un candidato nominal o comprador testaferro que también requerirá enfoque investigativo. Con la familia o los amigos, a sabiendas o no, un culpable probablemente filtrará algunos de los fondos lavados para este propósito. En el enfoque de base hacia arriba o a la inversa, a diferencia del análisis patrimonial más conocido, no sólo es importante saber que se paga una hipoteca o alquiler, sino, con precisión, cuál es la forma de pago que se utilizó. Además, a diferencia del tradicional análisis patrimonial, no va a ser la totalidad de los pagos lo importante sino que podría ser una sola anomalía en la forma de pago la que lo hace una pieza de evidencia viable.

Después de la vivienda, el enfoque de la base hacia arriba requiere un escrutinio similar del resto de los gastos de subsistencia tradicionales. Los servicios públicos deben encontrarse en lugar prominente en esta lista. Quien pague la electricidad, el agua corriente y la calefacción deben ser examinados cuidadosamente. En un caso real, un traficante de drogas hacía que muchos de sus clientes habituales le pagaran con cheques por cantidades disímiles. Más tarde rellenaba el beneficiario con sus diversas facturas de servicios públicos. Si los investigadores hubieran aceptado sólo el hecho de que los servicios públicos estaban a nombre del culpable, miles de fondos provenientes del lavado se habrían perdido. Y esto es sin mencionar el valor de este tipo de pruebas coloridas para los fiscales.

Una de las mayores banderas rojas de alerta para el lavado de dinero es cuando los giros postales se utilizan para pagar cuentas regulares mientras se mantiene una cuenta bancaria regular. Este es un claro indicador de que hay que dispersar cantidades de dinero. Este es uno de los problemas más comunes de los lavadores de dinero y de actividades delictivas en efectivo. Los investigadores deben tener en cuenta todos los elementos posibles de la vida del culpable en la que incluso pequeños gastos regulares se pueden hacer con el dinero contaminado. Compras regulares de alimentos y comestibles por sí solas pueden dar cuenta de miles. Una mirada detallada de los estados de cuenta bancarios regulares que carecen de cualquier indicador de comestibles y artículos diversos que se compran debe ser una bandera roja para los investigadores.

Las empresas de servicios públicos no son una parte normal de la Ley de Secreto Bancario y antilavado de dinero (BSA/ALD) y no suelen notificar a las autoridades cuando los giros se utilizan sospechosamente como forma de pago. Sin embargo, con las compañías de tarjetas de crédito hay numerosos informes de actividades sospechosas (SAR, por sus siglas en inglés) presentados a los clientes que utilizan las compras múltiples, a menudo estructuradas, de órdenes de pago para pagar sus cuentas. Una vez más, esto requiere que se investiguen los detalles de los métodos de pago actuales. Con el tiempo, los gastos diarios regulares pueden dar cuenta de importantes cantidades de dinero que es lavado.

En la práctica, muchos investigadores han utilizado a menudo una técnica similar a esta con compras nominales o fantasmas de automóviles. Hay numerosos casos en los que los traficantes de drogas pierden sus automóviles de lujo comprados de manera espuria cuando los investigadores utilizan los recibos procedentes de los pagos de rutina de gas, reparaciones, pagos de peaje, e incluso los boletos de estacionamiento para vincular el beneficiario efectivo con el vehículo. Hay evidencia similar en muchos otros aspectos de la vida de un lavador de dinero si se toma el tiempo para explorarlas. Algo tan simple como un proyecto de ley de televisión por cable puede ser justo la ayuda que necesita para desmantelar una conspiración criminal multimillonaria.

Cuando un enfoque de arriba hacia abajo ha dejado su investigación sin las pistas y pruebas necesarias, pruebe con poner su investigación en reversa y desarrollar velocidad. La gran oportunidad en su caso puede estar en las pequeñas cosas.

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

Trata de personas: **Si ve algo, diga algo**

A *CAMS Today* habló con Tonja Marshall, agente especial de supervisión del Departamento de Seguridad Interna, Investigaciones de Seguridad Nacional; Barbara Martinez, Fiscal Federal Adjunta, Jefa de la Sección de Investigaciones Especiales de la Fiscalía de Miami de los EE.UU.; y con el Sr. Carmen Pino, agente especial adjunto a cargo del Grupo de la trata de personas y la Trata de Personas del Departamento de Seguridad Interna del sur de Florida, Grupo de Tareas de Investigaciones de Seguridad Nacional para discutir el importante tema de la prevención de la Trata de Personas.

Tonja Marshall es agente especial de supervisión del Departamento de Seguridad Interna, Investigaciones de Seguridad Nacional, con sede en Miami, Florida. La agente Marshall comenzó su carrera en el gobierno en 1983 como una estudiante/practicante del ex Servicio de Aduanas de los EE.UU., mientras estudiaba en la universidad. Después de graduarse, se la nombró agente especial de aduanas destacada en Dallas, Texas. Durante sus 13 años en Dallas, llevó a cabo investigaciones relacionadas con estupefacientes, delitos financieros y pornografía infantil y fue elegida *Agente Especial del Año en 1997* por la sección regional de la organización de Mujeres en la Ejecución de la Ley Federal. De 1997 a 2001, la Agente Marshall sirvió en la sede de Aduanas de los EE.UU. en Washington, DC, donde fue asignada a la División de Investigaciones de contrabando. En 2001, fue seleccionada para supervisar el grupo de Investigación del Cambio del Peso de Mercado Negro en Miami, Florida. En 2004, fue promovida a agente especial a cargo, Houston, Texas, donde supervisó la División de Investigaciones Financieras. En 2008, la Agente Marshall regresó a Miami cuando fue seleccionada para supervisar el Grupo de Tareas de Tráfico Humano de South Florida, un esfuerzo de colaboración entre la policía, los fiscales, las organizaciones no gubernamentales, comunidades religiosas, y ciudadanos interesados dedicados a interrumpir y desmantelar las organizaciones de tráfico de personas a la vez que prestaban servicios a las víctimas de trata. En 2012, los Niños de la Florida y del Gabinete de la Juventud seleccionaron a la Agente Marshall como su *Oficial de Aplicación de la Ley del Año* por su trabajo en la lucha contra la trata de personas. La agente Marshall actualmente supervisa un grupo de delitos financieros que se encarga de la protección de la integridad de la infraestructura financiera de los EE.UU. al observar las formas en que las entidades delictivas ganan, mueven y almacenan las ganancias de sus delitos.

En la foto: Tonja Marshall

La fiscal federal adjunta (AUSA) Barbara A. Martinez es actualmente jefa de la Sección de Investigaciones Especiales de la Fiscalía de Miami en los EE.UU. En esta capacidad, AUSA Martinez supervisa a los fiscales federales a cargo de los casos de trata con fines sexuales, la explotación infantil, y los casos de delitos violentos que resultan en muerte o lesiones corporales graves, que incluyen robos en serie, toma de rehenes, secuestros y actividades relacionadas con pandillas. AUSA Martinez es también la Coordinadora de la trata de personas y la Coordinadora del Proyecto Niñez Segura (PSC) para el Distrito Sur de Florida. Como Coordinadora del Distrito para estos programas, AUSA Martinez es responsable de la coordinación entre las entidades no gubernamentales, federales, estatales y agentes de la ley locales y los fiscales en el Distrito Sur de la Florida que colaboran en los esfuerzos para combatir la trata de personas y la explotación infantil. Ella lleva a cabo cursos de capacitación para funcionarios encargados de hacer cumplir la ley y los fiscales a nivel local y en el extranjero. Además, participa habitualmente en eventos de alcance comunitario y se dirige al público para aumentar la conciencia de la comunidad. Ha sido conferencista invitada a foros públicos para trabajadores migrantes, estudiantes de escuela primaria, padres, estudiantes universitarios, la organización y miembros de clubes sociales, profesionales de la salud, miembros de asociaciones de abogados y empleados de la Embajada EE.UU. Martinez también enseña trata de personas en la Universidad de Miami, Escuela de Derecho, como profesora adjunta.

El Sr. Carmen J. Pino es actualmente el agente asistente especial a cargo (ASAC) de Investigaciones de Seguridad Nacional en Miami, Florida. En su cargo actual es el responsable de todas las investigaciones relacionadas con violaciones de

la Ley de Inmigración y Nacionalidad, así como jefe del Grupo de Tareas para la Trata Humana de Florida del Sur.

El ASAC Pino comenzó su carrera policial en 1995 en Filadelfia con la DEA antes de transferirse al ex Servicio de Aduanas de los EE.UU. en 1997. El ASAC Pino había aceptado diferentes tareas con Aduanas en Arizona, Nueva York y en la sede en Washington D.C. antes de ser nombrado agente especial asistente a cargo en Miami.

ACAMS Today: ¿Cuál es el nivel de importancia que tiene el problema de la trata de personas en el sur de la Florida?

Carmen Pino: Tiene una importancia enorme. Si tenemos en cuenta la geografía del sur de la Florida, la población y la economía, es un ambiente propicio para la trata de personas . En cuanto a la trata sexual, tenemos una industria turística alta, y cuando se tienen muchas personas que vienen para grandes eventos, como el Super Bowl o las finales de la NBA o Ultra, va a haber demanda. Con demanda va a haber oferta. Así que hemos visto acompañantes de alta gama traficadas por la delincuencia organizada.

También hemos visto extranjeros ricos explotando criadas o amas de casa, manteniéndolas en una habitación y obligándolas a trabajar 17 horas al día con poco o ningún sueldo. Esa es la esclavitud moderna. Somos también un gran productor agrícola para la mayoría del país. A medida que las estaciones van cambiando, producimos tomates, lechugas y frutas y otras verduras. Hay gran potencial para el tráfico de mano de obra ya que tenemos una gran cantidad de trabajadores inmigrantes que van llegando durante el año. Por desgracia, podríamos tener las mismas organizaciones dedicadas a trabajos forzados, forzando también a niñas y mujeres a participar en actos sexuales para los trabajadores migrantes. Se les puede cobrar a los trabajadores migrantes entre $20 a $30 por tener relaciones sexuales con estas mujeres. Hemos visto a menores y adultas violadas 20 veces por noche y a la víctima mudada de lugar semana por medio.

Esas son algunas de las razones por las que realmente hacemos hincapié en nuestro programa de divulgación. Estos casos de trata se están produciendo y la mayoría de las personas no los reconocen. Gran número de personas han visto las banderas rojas de alerta de la trata, pero no pudieron identificarlas como tráfico de personas. Digamos, por ejemplo, que usted entra en un salón de manicura y cada vez que va ve a la misma persona. Puede ir en la mañana, tarde en la noche o el fin de semana, y esa persona siempre está allí. Usted trata de tener una relación normal de cliente interactuando de manera típica, pero esa persona no habla con usted. Si

En la foto: Barbara Martinez

intenta entablar una conversación mira a otra persona para ver si tiene permiso para responder. Tal vez usted puede encontrarse con alguien que parece preocupado. Pero cuando se acerca y le pregunta si todo está bien, otro habla por ese alguien y le dice: "No habla inglés. Si tiene algún problema, hable conmigo".

Los indicadores de la trata incluyen a alguien que está siendo controlado, alguien que no se involucra en una relación de cliente normal, a quien se le ve trabajando desde la mañana hasta el mediodía y luego a la noche. Esto ocurre y una gran cantidad de personas no se dan cuenta. Cuando llegué por primera vez al sur de la Florida se me dijo "Sabes, aquí no hay mucho tráfico". Ahora, cuando se ve la cantidad de clientes potenciales que se acercan y la cantidad de casos que estamos trabajando, es evidente que hay mayor conciencia. El hecho es que si nos fijamos en las estadísticas, somos una de las tres principales áreas de trata de personas. Así que es aquí, está sucediendo y sólo necesitamos que la gente se dé cuenta de ello. Si ve algo, diga algo.

AT: ¿Cuántos casos de trata de personas ha procesado su oficina?

Barbara Martinez: Desde 2007, la Oficina del Fiscal de los EE.UU. para el Distrito Sur de la Florida ha iniciado aproximadamente 55 casos de trata de personas y hecho 90 imputaciones. Estos casos federales de trata de personas incluyen tanto la trata laboral como el tráfico sexual. Creo que es importante tener en cuenta que estas cifras sólo reflejan los casos en que los estatutos de trata de personas fueron realmente imputados. El número de casos federales de trata de personas empezados aquí en el sur de la Florida durante este período se considera alto en comparación con otros distritos. Aún así, estas cifras ciertamente no reflejan la totalidad del problema en el sur de Florida. Creo que todos estamos convencidos de que hay situaciones de trata de personas que no están siendo identificadas o denunciadas; por lo tanto, hay mucho más trabajo que hacer en tanto comunidad, lo que ayudará a combatir e identificar la trata de personas.

CP: Sí, ese número puede parecer un poco bajo; sin embargo, también hay momentos en los que podemos no tener todos los requisitos legales para hacer las imputaciones de la ley federal de tráfico. Así, hay tanto socios estatales como locales que aportan un poco de herramientas a nuestra caja de herramientas. Por ejemplo, si no podemos imputar por la trata, podemos imputar a los delincuentes por otra cosa, como el tráfico de indocumentados, fraudes de visa o delincuencia relacionada con la droga. Si nosotros no imputamos a un traficante, eso no quiere decir que tal vez no haya situaciones que tienen indicadores de la trata.

AT: ¿A qué sanciones se enfrentan los traficantes de seres humanos en el sistema federal?

BM: En el sistema federal, la Ley de Protección de Víctimas de la Trata (TVPA), que fue promulgada en 2000, tipifica como delito la trata de personas. La TVPA prevé una pena máxima de prisión de 20 años por obligar a realizar trabajos forzados. Las violaciones de tráfico sexual llevan ya sea de un mínimo obligatorio de 10 o 15 años y un plazo máximo de cadena perpetua. Un mínimo

obligatorio de 15 años se aplica si se utilizó fuerza, fraude o coerción o si la víctima es menor de 14. Si la víctima tiene entre 14 y 17 años, se aplica un mínimo obligatorio de 10 años. La sentencia final depende realmente de la gravedad de la coacción o la fuerza, el número de víctimas, y una serie de otros factores. Me gustaría decir que hemos tenido numerosos acusados en el sur de Florida que han sido condenados a cadena perpetua por tráfico de personas.

AT: ¿Qué enfoque toma cuando trabaja con las víctimas de un caso de trata de personas?

BM: Sin duda, un enfoque centrado en las víctimas. La TVPA establece un enfoque centrado en las víctimas que comienza en el momento en que nos encontramos con una víctima potencial, así como al inicio de cualquier investigación de trata de personas. La protección de las víctimas y proveer para sus necesidades es una prioridad durante cualquier investigación criminal, procesamiento e incluso después de que el caso termina. En tanto fiscal federal, el enfoque centrado en las víctimas significa que puede haber momentos en que las necesidades de la víctima pueden ser incompatibles con los esfuerzos de la fiscalía. De hecho, podemos decidir no enjuiciar un caso si se encuentra en el mejor interés de la víctima. Cuando usted está utilizando un enfoque centrado en la víctima primero debe considerar si la víctima quiere proceder con el enjuiciamiento y si proceder se encuentra en su mejor interés. Un fiscal que trabaja en un caso de tráfico humano también debe determinar cómo proveer por las necesidades de la víctima durante todo el proceso penal. No se nos permite llevar a las víctimas a casa con nosotros, proporcionarles alimento, ropa o servicios médicos, darles el estatuto de inmigrantes o conseguirles un puesto de trabajo. Por lo tanto, tenemos que trabajar muy de cerca con y depender de nuestros socios de aplicación de la ley, socios comunitarios, organizaciones no gubernamentales, entidades privadas y organismos de base local para prever por las víctimas. Tenemos que coordinar con nuestros socios. Esto puede ser muy difícil; sin embargo, los fiscales que trabajan en casos de trata de personas aprenden rápidamente que estas alianzas son fundamentales para ayudar a las víctimas.

CP: Cuando decimos que tenemos un enfoque centrado en las víctimas, algo de lo que el público tiene que darse cuenta es que no es como, digamos, un caso de droga o de lavado de dinero donde permitimos que las cosas sigan su curso para lograr pruebas adicionales o dejar que las cosas funcionen por sí mismas. Si sabemos que una víctima está sufriendo físicamente o que se la maltrata brutalmente de cualquier forma, hacemos un rescate en ese momento. No hay un momento de "espera" ni se dice "Bueno, no tenemos todas las pruebas". Dejamos lo que estamos haciendo, y hacemos el rescate y luego tratamos de averiguar qué elementos tenemos. Así que, sólo quería que el público supiera que no vamos a permitir que alguien continuara siendo víctima por el simple motivo de tratar de probar un caso.

BM: No hay duda de que la utilización de un enfoque centrado en las víctimas impacta cómo los que aplican la ley investigan estos casos y la forma en que procesamos los casos de trata de personas. Las decisiones que tomamos a lo largo del proceso penal federal pueden ser diferentes, simplemente porque son lo mejor para la víctima. Muchos otros tipos de casos delictivos no requieren que los que aplican las leyes y los fiscales utilicen este enfoque. Además, debo añadir que en el sistema federal hay una gran cantidad de protecciones legales de la intimidad de las víctimas, sobre todo si son menores de edad. Hay cierta información que simplemente no puede ser lanzada al público. Hacemos grandes esfuerzos por sellar los documentos y por restringir realmente el número de personas que obtiene información sobre el caso. En el sistema federal, a diferencia del sistema judicial del estado de Florida, nuestras víctimas no rinden testimonio para la defensa antes del juicio. Obviamente, esto es un gran beneficio para la víctima.

AT: Cuando se trabaja con la comunidad, los que ejecutan la ley y las ONG, todos están trabajando como defensores de las víctimas. ¿Su oficina tiene que pasar por los defensores con el fin de obtener información de las víctimas?

BM: Sí, por lo general. El abogado de la víctima juega un papel importante en ayudarnos a construir una buena relación con la víctima y hacer frente a los temores y preocupaciones de la víctima. Le diré que a menudo construimos muy buenas relaciones con las víctimas. Si hay una buena relación con la víctima, los defensores a menudo confían más en los que aplican la ley y los fiscales, lo que permite una mejor coordinación. Sin duda, hace que sea mucho más fácil para todas las partes, cuando todo el mundo tiene el mejor interés de la víctima en mente.

AT: ¿Cuáles son algunos de los otros tipos de delitos que surgen, además de la trata de personas?

BM: Algunos son

a. Las leyes de inmigración

b. Fraudes de visados

c. Leyes laborales

d. El fraude en la contratación de mano de obra extranjera

e. La Ley Mann, acusaciones de prostitución federal

f. Chantaje Civil, Influencia y Organizaciones Corruptas (RICO, por sus siglas en inglés)

g. El contrabando de extranjeros

h. El lavado de dinero

Si no podemos acusarlos de trata de personas, todos tenemos la opinión de que deberían ser procesados por otros delitos conexos, si es posible.

CP: Otra cosa por mencionar es que el componente de lavado de dinero de nuestra investigación es fundamental, ya que en algunos de nuestros casos de tráfico laboral y sexual, si podemos identificar los activos, podemos usar ese dinero para restituirlo a las víctimas.

AT: ¿Cómo investigan los casos de trata de personas?

CP: Muchas veces los casos se ponen en nuestro conocimiento por parte de varias fuentes diferentes. Número uno, podemos obtener una referencia de uno de nuestros socios, ya sea de aplicación de la ley o de una operación encubierta o algo a nivel local. También recibimos referencias del proveedor de servicios sociales o las organizaciones no gubernamentales, que han entrado en contacto con la víctima y que nos traerán esa información. Como nuestro alcance ha aumentado con el tiempo, el número de información que estamos recibiendo por parte del público ha aumentado considerablemente. Llegan de una variedad de maneras. Básicamente, miramos todo desde un lugar doble, pues, como explicamos anteriormente, tomamos un enfoque centrado en las víctimas. Tenemos que tomar una decisión: ¿Hay una oportunidad para hacer un rescate, y si es así es nuestro enfoque principal en el momento. Si no sabemos dónde puede estar la víctima o si no sabemos si alguien es víctima, llevamos a cabo el método de investigación estándar, ya sea la vigilancia, entrevistas de testigos, cosas por el estilo. La mayoría de ellos vienen del público, lo que demuestra que nuestro programa de extensión está ganando impulso y que el público se está concientizando del problema que sucede en su patio trasero.

BM: Las investigaciones actuales se manejan a través del Grupo de Tareas de Menores federal y el Grupo de Tareas de la Trata de Personas de Florida del Sur. Estos grupos de tareas incluyen, el estado y los funcionarios federales locales encargados de hacer cumplir la ley y los fiscales, así como las organizaciones no gubernamentales, organizaciones religiosas y miembros de la comunidad local.

CP: Como jefe del Grupo de Tareas de la Trata de Personas de Florida del Sur, por lo general tenemos una multitud de representantes de aplicación de la ley y sobre todo su HSI, la oficina del Fiscal de los EE.UU., el FBI, los miembros

del Departamento de Estado, la salud y los servicios humanos, y el Departamento de Trabajo. Del lado del estado tenemos al sheriff del condado de Broward, el departamento de policía de Miami-Dade, hasta departamentos de policía individuales más chicos,—pero lo que es único es la estrecha relación que tenemos con nuestras organizaciones no gubernamentales y los proveedores de servicios sociales. Interactuamos con ellos semanalmente y a veces diariamente. Así que saben lo que vamos a estar haciendo (aunque, obviamente, tenemos que proteger cierta información de las autoridades de control legal), pero vamos a decirles "Oigan, estén preparados, que es posible que tengamos uno o dos víctimas para ustedes esta noche". Hay un montón de planificación logística que se dedica a una situación de rescate. Tenemos que estar preparados para todo, desde encontrar una cama para que duerman hasta conseguir ropa o artículos médicos para las víctimas. Además de los proveedores de servicios sociales, tenemos una comunidad muy grande basada en la fe o iglesia que es una muy buen defensora nuestra. Salen a todas las diferentes iglesias y aumentan la conciencia. Así que puede imaginar la cantidad de gente que va a la iglesia cada domingo y que oye de los indicadores de la trata—lo que es una gran cosa. También tenemos buena cooperación con el mundo académico. Tenemos la Universidad de St. Thomas con la que tenemos mucha interacción. Así que cuando usted reúne todos estos diferentes factores y las diferentes áreas, tenemos un gran grupo de personas y ahora si podemos hacer que la comunidad financiera se nos una también eso será otro socio increíble para agregar a un grupo de tareas ya muy grande y muy robusto.

AT: ¿Cuáles son algunos de los retos más importantes en la investigación de la trata de personas?

CP: El desafío más grande que tuvimos es que la prueba las más de las veces es nuestra víctima. Cuando tiene a alguien que usted ha rescatado y ha conseguido alejarla de esa horrible condición en la que estaba, puede que tenga que hacerla revivir lo sufrido a través de entrevistas y potencialmente estar en el banquillo frente a su agresor. Por lo tanto, durante mucho eso es muy difícil porque no queremos volver a lesionar a la persona mentalmente y hacer que reviva esa experiencia horrible. Si no tenemos una víctima, a veces no tenemos un caso. Por eso he dicho... sí, tenemos una gran cantidad de enjuiciamientos exitosos con la ley de trata actual, pero en muchas oportunidades optamos por una acusación distinta sólo porque puede ser que no queremos poner a esa víctima en el banquillo y hacer que pase por los horrores nuevamente. Así que podríamos enjuiciarlos por lavado de dinero o lo que sea, y eso es algo que tanto los fiscales como la ONG nos acompaña en cualquier decisión que se tome.

BM: En primer lugar, la identificación de la trata de personas es un reto porque la mayoría de las víctimas de la trata de personas no sabe qué es la trata. De hecho, la mayoría de las víctimas no se consideran víctimas en absoluto. Esto significa que debemos confiar en mucho más que auto-reportes para rescatar a las víctimas de la trata de personas. En segundo lugar, es extremadamente difícil asegurarse de que las víctimas se sientan seguras y que estén dispuestas a confiar en uno lo suficiente como para explicar lo que realmente sucedió. Cuando se las encuentra por primera vez, la mayoría de las víctimas inicialmente les tienen mucho temor a los traficantes y no les quieren causar ningún problema. Trabajamos duro para asegurarnos de que las víctimas se sientan seguras y para ganar su confianza. En tercer lugar, una vez que nos enteramos del abuso y trauma que sufrieron, tenemos que garantizar que se satisfagan sus necesidades. La víctima suele tener muchas necesidades físicas, emocionales y personales. Asegurarse de que las personas adecuadas se ponen en contacto y que los recursos estén disponibles es un reto. En cuarto lugar, la obtención de la corroboración de las declaraciones de la víctima es a veces un reto, porque hay una falta de testigos o registros. Esta es una razón por la que investigar el tema del dinero resulta tan útil. La evidencia de lavado de dinero o de grandes ganancias de los traficantes viene a corroborar las denuncias de trata de personas y a revelar la imagen completa a un jurado. Por último, en coordinación con todos nuestros socios y asegurando que la víctima es atendida durante todo el proceso es siempre un reto.

AT: ¿En qué industrias ha encontrado víctimas de la trata de personas?

CP: Hemos visto trata de personas en

a. La industria del sexo (los servicios de acompañamiento, striptease, burdeles, salones de masajes)

b. Salones

c. Agricultura, silvicultura, industria pesquera

d. Servicios gastronómicos (restaurantes, hoteles)

e. Trabajos de construcción

f. Trabajos de paisajismo

g. Pequeñas empresas

h. Fábricas

i. Servidumbre doméstica

De hecho, tuvimos un caso de amplias zonas ajardinadas en Boca Ratón, donde 20 trabajadores filipinos se vieron obligados a trabajar en condiciones horribles y tenían que trabajar muchas horas en condiciones de esclavitud. Si existe la necesidad de mano de obra, va a haber traficantes por ahí que van a poner a esas personas en esas posiciones.

AT: ¿Con qué frecuencia utilizan los traficantes de personas el sector financiero?

Tonja Marshall: En cuanto a la utilización del sector financiero, yo diría que alrededor del 99 por ciento de los casos que vemos utiliza el sector financiero, ya sea a través de los MSB o a través de la institución financiera típica donde tenemos cuentas bancarias. Las víctimas están enviando dinero a través de los MSB a los miembros de la familia y de vuelta a los traficantes, que, a veces hemos encontrado, son una y la misma cosa: los traficantes son miembros de la familia. Hemos visto ejemplos de las víctimas que están trabajando en lo que llamamos el "circuito". Estas víctimas se trasladan de ciudad a ciudad y utilizan los MSB para enviar dinero a los traficantes de aquí en los EE.UU. como a nivel internacional, haciendo depósitos en las cuentas bancarias de los traficantes utilizando cajeros automáticos.

AT: ¿Cuáles son los beneficios de investigar los aspectos financieros de la trata de personas?

TM: Para mí, consiste en seguir la pista del dinero cuando se trata de tráfico o cualquier tipo de caso. Cuantos más registros tengamos, más fácil podremos identificar una organización en su conjunto. Al seguir los documentos que se están produciendo a medida que mueven su dinero, podemos identificar la organización. También se puede encontrar información sobre otros jugadores involucrados, lo que podría dar lugar a detenciones y procesamientos potenciales. Esto nos ayudará a obtener más información acerca de los líderes delincuentes y sus organizaciones. Este es uno de los mayores beneficios de tomar en cuenta el dinero. En cuanto a la trata de personas, creo que la restitución para las víctimas es importante, como mencionó Carmen. Y a pesar de que está escrito en la TVPA federal, no siempre vemos que personas o investigadores utilizan esa herramienta. Afortunadamente, hemos tenido mucho éxito en el sur de la Florida con la herramienta de restitución y de poder demostrar que se les deben salarios a las víctimas de la labor y el tráfico sexual. En el caso mexicano de tráfico sexual había 8 o 10 víctimas de tráfico sexual a las que se les adjudicaron más de 1,2 millones de dólares en restitución.

AT: Usted dijo "los investigadores no siempre usan la herramienta de la restitución" a pesar de que la estamos usando aquí en el sur de Florida, ¿por qué los investigadores no están utilizando la herramienta de la restitución? ¿Es por falta de recursos? ¿Dónde va el dinero si no se está utilizando para las víctimas?

TM: La restitución se concede a las víctimas, ahora más que nunca. Al principio no estábamos tan enfocados en la restitución, sino más en asegurar

que la víctima recibiera los servicios que necesitaba y que a los traficantes se les procesara—es mucho trabajo hacer todo esto cuando se trata de víctimas. Tratar con el caso de un ser humano es muy diferente a tratar con ganancias, pero creo que lo estamos haciendo más ahora. Además, un montón de veces, lograr conseguir los activos es sumamente difícil. Tenemos mucha cooperación de países extranjeros para identificar los activos y para compartir algunos activos con las víctimas. Pero en cuanto a la restitución, muchas veces es muy difícil saber a dónde va el dinero. Es mucho más fácil hacer un seguimiento de las organizaciones más grandes de crimen organizado, ya que podemos ver dónde utilizan y ponen las ganancias en la organización. En cuanto a los grupos de traficantes o grupos con menos organización, a veces no somos capaces de ver los activos que provienen del dinero que están obteniendo.

> Mientras más sofisticada es la organización, más fácil es para nosotros seguir el rastro del dinero

AT: ¿Así que, en otras palabras, nos gusta capturar a los bien organizados? Estoy bromeando, preferimos capturar a todos.

TM: [Risas] Bueno, diría que he hecho las dos cosas, pero con la cooperación de las fuerzas del orden y los fiscales extranjeros, muchas veces vemos que la familia es en realidad la organización y volvemos al país extranjero en el que vive la familia y lo que vemos es que están construyendo otra planta en su casa. Allí es donde van los ingresos del cliente, porque ninguno de los miembros de la familia trabaja. Han estado viviendo de los salarios de la víctima de la trata. No están manejando los coches de lujo que usted podría pensar; sin embargo, vemos cómo viven una vida más lucrativa que otros basados en el hecho de que la víctima de la trata es un cónyuge o una novia de uno de los miembros de la familia y ella está aquí en los EE.UU. como una víctima de la trata.

CP: Para complementar lo que está diciendo Tonja: Mientras más sofisticada es la organización, más fácil es para nosotros seguir el rastro del dinero. Por ejemplo, si usted está trabajando en un caso de trata laboral y los traficantes o el negocio hace una declaración de impuestos, tienen una nómina—en esencia hay algo que usted puede seguir. Si se trata de un servicio de acompañantes de alto nivel en el que se está ejecutando una red de prostitución a través de una página web usted está viendo todo tipo de intercambios por medio del correo electrónico. Así que hay documentos o cualquier otra cosa donde se puede seguir el rastro del dinero. Especialmente para nuestras víctimas de México, América Central o América del Sur donde las víctimas son desplazadas de burdel en burdel, se trata de una empresa muy pequeña que usa efectivo. Son veinte o treinta dólares por viaje. Además, un montón de veces el dinero se lleva a un MSB o a veces se hacen envíos a granel. Cuanto más sofisticada es la organización –sobre todo si se trata de tráfico de mano de obra y se comercia con negocios legítimos, más fácil será para nosotros encontrar los fondos ilícitos.

AT: ¿Hay algo que pueden hacer las instituciones financieras para ayudar con sus investigaciones?

BM: Ahora estamos viendo que el sector financiero se está convirtiendo en una gran fuente de información al inicio de una investigación cuyo objetivo es la trata de personas. Por lo tanto, los informes de actividades sospechosas (SAR) nos pueden conducir a estas organizaciones de trata de personas.

TM: Las instituciones financieras deberían seguir haciendo lo mismo que ya están haciendo, la búsqueda de anomalías en las actividades de las cuentas que no siguen lo que declararon como razón de ser de la cuenta o del negocio. Por lo general, grandes depósitos en efectivo en una cuenta personal, especialmente si se están haciendo por un tercero. Esto lo vemos mucho y es por lo general cuando la víctima deposita en la cuenta de los traficantes. Muchos de estos casos tienen características similares en cuanto a las banderas rojas que usted busca en las cuentas bancarias reales en las instituciones financieras. Por ejemplo, para nuestros casos de trata sexual, cuando se trata de hacer depósitos en efectivo, será típicamente por menos de $10.000. Dependiendo de si se trata de una acompañante de alta gama en comparación con el burdel de México o de América del Sur, las cantidades variarán, pero siempre son menos de $10.000. A veces nos ponemos en contacto con los MSB porque los MSB por lo general desarrollan una relación personal con sus clientes y hay otras cosas que pueden buscar en cuanto a si la persona que hace el depósito está siendo controlada por otra persona.

AT: ¿Qué ha hecho su agencia para aumentar las alianzas mundiales para combatir la trata de personas?

TM: Cuando se trata de tráfico de personas y el sector financiero, ¡la idea de que estamos hablando de trata de personas en conferencias como las de ACAMS es increíble! Porque, no creo que todo el mundo piense en el aspecto de los activos o en el financiero de la trata, pero continuar extendiendo este tipo de alianzas tanto en los EE.UU. como a nivel internacional es importante. Siempre he sido una defensora de hablar, hablar y hablar más. Cuanto más se habla de ello, más aprendemos. Cuando empecé a hacer esto veíamos muy pequeños depósitos en efectivo para los MSB, y a medida que ha avanzado hemos aprendido más y más acerca de cómo las organizaciones de traficantes, ya sean grandes o pequeñas, cambian y se adaptan a lo que están haciendo las fuerzas del orden y lo que estamos viendo. Seguir hablando en los sectores público y privado—lo digo de nuevo, tanto a nivel nacional como internacional—es muy importante.

Hace un par de años, me encontré en un grupo de tareas que mi agencia patrocinaba en Washington D.C., donde nos sentamos con los jefes del ALD y cumplimiento de las principales instituciones financieras aquí en los EE.UU. y hablamos de trata de personas y de contrabando. Hablamos de las investigaciones finalizadas con ellos y compartimos lo que vimos y fue una experiencia increíble y que nos abrió los ojos a ambas partes sobre cómo asociarnos y continuar nuestras conversaciones.

AT: ¿Dónde pueden ir los miembros para reportar la trata de personas o para obtener más información?

CP: Nuestro enfoque principal ha sido en la investigación y promoción de la trata de personas y la conciencia del contrabando de personas, pero estamos armando un sitio web. Mientras tanto, la gente puede ir al Blue Campaign del Departamento de Seguridad Nacional, la oficina del Fiscal de los EE.UU. tiene enlaces e indicadores de bandera roja y nuestra agencia, www.ice.gov también tiene una gran cantidad de información e indicadores de bandera roja.

TM: Estoy segura de que usted está familiarizada con el proyecto STAMP y la Operación Cornerstone y sé que muchas de las instituciones financieras contactan nuestra oficina de operaciones en relación con las presentaciones de Cornerstone. Alguien nos ha llamado para pedir cosas específicas, tales como "¿Puede decirnos algo acerca de la trata de personas y de los indicadores que podemos buscar?" Así que eso se puede incorporar en una presentación de Cornerstone para cualquier institución financiera que esté interesada.

Las sospechas de trata de personas del sur de Florida pueden reportarse a la Línea Nacional de Tráfico Humano: 1-888-373-7888.

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

acamsglobal.org

ACAMS 13th Annual

AML & Financial Crime CONFERENCE

Main Conference: September 29 - October 1 | Pre-Conference Training: September 28 | ARIA, Las Vegas

FEATURED SPEAKER

Federal Bureau of Investigation
Angela Byers
Section Chief
Financial Crimes Section
Criminal Investigative Division

Top regulators and law enforcement officials address the hottest topics including 2014 examination trends, banking marijuana-based businesses and virtual currencies.

"Good mix of law enforcement, regulators and BSA professionals on plenary panels."

Wood Forest National Bank
David Brown, AML Manager

Mix-and-match sessions to fit your training needs — choose from 9 tracks now including Digital Trends, Investigations, Casinos, and a Compliance Summit.

"Excellent conference, loved the variety of breakout sessions that allowed me to customize to my needs. Great job!"

MetroBank
Sharon Psencik, Assistant Vice President, BSA High Risk Analyst

Expand your network to peers from across the globe for information, ideas and new perspectives — providing you year-round professional support.

"I meet new people and develop networking opportunities around the world."

Wells Fargo Bank
Bret A. Cropley, Compliance Consultant

SAVE $350 through June 20 with VIP code VGF-350*

acamsglobal.org | +1 305.373.0020 | info@acams.org

* Register and pay using VIP code VGF-350 by June 20, 2014, and save $350 off the standard, non-government main conference price. Virtual conference option does not qualify for this discount. Pre-conference workshops and the CAMS Examination Preparation Seminar are not included in main conference pricing. Discounts cannot be combined.

FinCEN APOYA LOS NEGOCIOS DE marihuana medicinal

Durante años, la piedra angular de un programa fuerte de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) era su capacidad para detectar y prevenir la venta de sustancias ilícitas mediante la identificación de los ingresos derivados de la actividad delictiva. Con la legalización de la marihuana al por menor en Colorado y Washington, un experimento cauto está actualmente en marcha, con fuertes implicaciones para la aplicación de la ley y el sector financiero. Sobre la base de la aparición de la marihuana medicinal, disponible en diferentes grados en otros 18 estados[1] más el Distrito de Columbia, la evolución del paisaje de delitos financieros ha creado un período de transición con potencial para el riesgo y la recompensa.

Más vale malo conocido que bueno por conocer

La publicación por parte del Departamento de Justicia (DOJ) de una guía orientativa[2] respecto de la aplicación de leyes sobre la marihuana el 29 de agosto del 2013 marcó un cambio en el enfoque de aplicación de la ley federal. Comúnmente conocido como el Memorando Cole, la guía afirma que en los estados donde existe un sistema de regulación fuerte y eficaz, el DOJ no enjuiciará a menos que exista la sospecha de que una de las ocho prioridades federales de aplicación ha sido violada. Efectivamente, el DOJ ha respetado el derecho de los estados en sus asuntos internos, siempre y cuando sus regímenes normativos no interfieran con los mandatos federales, que incluyen:

1) Impedir la distribución de marihuana a menores de edad;
2) Impedir que los ingresos de la venta de marihuana vayan a empresas criminales, pandillas y cárteles;
3) Impedir que se desvíe la marihuana de los estados donde resulta legal de algún modo a otros estados;
4) Impedir que la actividad de la marihuana autorizada por el estado se utilice para cubrir o sirva de pretexto para el tráfico de otras drogas ilegales u otros ilícitos;
5) Impedir la violencia y el uso de armas de fuego en el cultivo y distribución de marihuana;
6) Impedir el uso del manejo drogado y la exacerbación de otras consecuencias adversas para la salud pública asociados con el consumo de marihuana;
7) Impedir la siembra de marihuana en terrenos públicos y los peligros de seguridad pública y ambientales concomitantes planteados por la producción de marihuana en terrenos públicos; e
8) Impedir la tenencia de marihuana o su uso en propiedades federales.

Siguiendo el ejemplo del DOJ, la Red de Contra los Delitos Financieros (FinCEN) publicó una guía, (FIN- 2014- G001)[3], el 14 de febrero del 2014, que lleva un paso más allá esta presunción de independencia estatal convocando explícitamente a mejorar la disponibilidad de servicios financieros para, así como la transparencia financiera de, los negocios relacionados con la marihuana. Sin dejar de respetar los límites de las prioridades federales de aplicación, FinCEN apoya los negocios bancarios de empresas de marihuana que trabajan en efectivo y aclara las expectativas respecto de la diligencia debida y reporte de actividades sospechosas para esta industria.

Las instituciones financieras seguirán teniendo que presentar informes de actividades sospechosas (SAR, por sus siglas en inglés) para todas las empresas de marihuana, pero ahora se les pide que distingan entre empresas "Marihuana Limitadas" y "Marihuana Sospechosas". Esta distinción se basa en una diligencia debida llevada a cabo por la institución financiera para determinar si el negocio se dedica a cualquiera de las ocho prioridades federales de aplicación. Si la respuesta es sí, entonces la presentación del SAR se considerará sospechosa. Si la respuesta es no, entonces la presentación del SAR se considera limitado. Presentaciones de SAR de "Marihuana Limitada" sólo en teoría serán menos onerosas, ya que sólo requieren los nombres y direcciones de los sujetos y afines, así como una afirmación de que no se ha encontrado actividad sospechosa adicional asociada a un negocio autorizado de marihuana. Sin embargo, los bancos seguirán obligados a presentaciones continuas de SAR siempre que el cliente siga llevando a cabo negocios relacionados con la marihuana.

Por muy enrevesada que pueda parecer la guía orientativa, hay una clara intención de avanzar en incorporar las empresas legales de marihuana al sistema financiero. Esto se basa en una evaluación pragmática por parte del gobierno federal según la cual la legalización de los estados se encuentra fuera de su control y los negocios en efectivo no bancarizados presentan mayor riesgo para la estabilidad financiera que las empresas riesgosas respaldadas por proveedores de servicios financieros de confianza. Esta es la misma lógica que permite la continuación de otras industrias con alto riesgo de lavado de dinero, tales como casinos, negocios de servicios monetarios (MSB, por sus siglas en inglés), y la banca privada. Un beneficio adicional de la incorporación de las empresas relacionadas con la marihuana en el sistema financiero es que le proporciona a FinCEN datos procesables de una industria en la que siempre ha faltado la transparencia. Entender sus fuentes de ingresos permite al gobierno federal rastrear las tendencias del sector y combatir la venta de drogas ilícitas en otras jurisdicciones. Esta información es muy valiosa para la prevención de amenazas a la seguridad pública, la salud y otras cuestiones de orden público. En otras palabras, más vale malo conocido que bueno por conocer.

Los escépticos señalan que los cargos de diligencia debida y requisitos de presentación de SAR más matizados no son zanahorias eficaces para hacer que los bancos saquen las empresas marihuaneras de las sombras financieras, en particular teniendo en cuenta los riesgos asociados con esta industria naciente. Colorado y Washington pueden estar estableciendo cuidadosamente las bases de regulación de un sistema eficaz de controles durante el próximo año, pero aún está por verse en qué medida y con cuánta velocidad se extenderá el apoyo para la marihuana al por menor. Los bancos nacionales de mayor tamaño muy improbablemente explorarán la posibilidad de bancarizar una industria que actualmente está limitada por fronteras estatales y plagada de peligros legales. La realidad es que las industrias al por menor y médicas serán consideradas una inversión de alto riesgo, siempre y cuando la marihuana permanezca bajo la Ley de Sustancias Controladas (CSA).[4]

[1] Alaska, Arizona, California, Connecticut, Delaware, Hawaii, Illinois, Maine, Massachusetts, Michigan, Montana, Nevada, Nuevo Hampshire, Nueva Jersey, Nuevo Mexico, Oregon, Rhode Island, y Vermont.
[2] http://www.justice.gov/opa/pr/2013/August/13-opa-974.html
[3] http://www.fincen.gov/news_room/nr/html/20140214.html

Los bancos ágiles con programas de cumplimiento fuertes pueden obtener ganancias por la prestación de servicios a esta industria

Aunque muchas instituciones financieras puedan ver las empresas relacionadas con la marihuana como una tarea arriesgada, más allá de su apetito, otros las ven como una oportunidad para lograr ventaja del primer movimiento en una industria de amplio crecimiento.[5] Con más de $14 millones en ingresos generados en enero de 2014 por apenas 59 dispensarios con licencia reciente en el estado de Colorado, los bancos ágiles con programas de cumplimiento fuertes pueden obtener ganancias por la prestación de servicios a esta industria. A pesar de que las ventas disminuyan después de la emoción inicial, más dispensarios están entrando en línea para satisfacer la demanda. A partir de marzo de 2014, casi 150 dispensarios por menor fueron autorizados en Colorado.[6] Es poco probable que FinCEN espere que todos los bancos participen, pero la hoja de ruta que han proporcionado tiene el detalle suficiente para satisfacer a las instituciones que tienen menos aversión al riesgo. La diligencia debida recomendada se centra en la verificación de la validez de la solicitud de licencia o estatal; estableciendo y manteniendo un perfil de cliente basado en la información disponible para las partes comerciales y relacionadas; y el seguimiento permanente y la diligencia debida. Muchos de estos requisitos no son más gravosos que los requeridos de los MSB o transmisores de dinero. El enorme escrutinio dirigido al proceso de regulación innovadora asegura que una cantidad significativa de la diligencia debida ya ha sido llevada a cabo por el estado previo a la emisión de una licencia.

El componente más problemático de las directrices necesarias no es el aumento de la carga administrativa de los documentos presentados o la aplicación de la norma de diligencia debida mejorada de búsqueda y salvamento, sino más bien la necesidad de desarrollar una comprensión de la actividad normal y esperada para el negocio, incluyendo los tipos de productos que se venden y el tipo de clientes que se sirve. El Departamento de Ingresos de Colorado no espera que surjan patrones claros antes de mediados de año, momento en el que los funcionarios gubernamentales tendrán una idea del volumen, si no de la composición transaccional, de la industria.[7] Aquí es donde surge lo kafkiano de la guía orientativa de FinCEN—las instituciones financieras no serán penalizadas por ofrecer servicios bancarios a las empresas "Marijuana Limitadas", pero sin antes bancarizarse este tipo de empresas no tendrá los datos de referencia necesarios para establecer si la actividad es sospechosa de acuerdo con los criterios establecidos en el Memorando Cole.

En última instancia, el éxito o fracaso de este experimento audaz se basará en una combinación de finura de regulación, seguridad jurídica, así como el intercambio colaborativo de información. Las instituciones financieras con programas robustos de cumplimiento y apetito por el riesgo apropiados se beneficiarán de abordar con cauto optimismo, sin dejar de presionar para que haya protecciones legales claras para la banca sobre empresas relacionadas con la marihuana. Del mismo modo, los defensores del consumidor y asociaciones de comercio de cannabis se beneficiarán con el establecimiento de directrices para los miembros del ALD, y por promover la transparencia en los patrones de transacciones habituales. La coordinación de esfuerzos y el compromiso de la banca responsable alentarán a los que ejecutan la ley a concentrar sus recursos en las cuestiones que plantean una mayor amenaza a la estabilidad del sistema financiero.

Michael Florence, CAMS, director senior, Treliant Risk Advisors, Washington, D.C., EE.UU., mflorence@treliant.com

Mikela Trigilio, CAMS, analista, Treliant Risk Advisors, Washington, D.C., EE.UU., mtrigilio@treliant.com

[4] http://www.americanbanker.com/bankthink/banks-stay-wary-of-marijuana-related-businesses-1066321-1.html
[5] http://www.nbcnews.com/business/business-news/banks-balk-marijuana-money-despite-u-s-guidelines-n35416
[6] http://www.huffingtonpost.com/2014/03/10/colorado-marijuana-tax-revenue_n_4936223.html
[7] http://www.huffingtonpost.com/2014/03/10/colorado-marijuana-tax-revenue_n_4936223.html

ACAMS Recognition Awards

2014

ACAMS
AML Professional of the Year Award

ACAMS TODAY
Article of the Year

ACAMS Al Gillum
Volunteer
OF THE YEAR


2013


2012


2011


2010

Submit your nominations today: acamsglobal.org/awards.asp

Last day for entries is July 31

El Grupo Wolfsberg actualiza las directrices del banco corresponsal

El 18 de febrero del 2014, el Grupo Wolfsberg de instituciones financieras internacionales, consorcio industrial que establece normas para la industria internacional de antilavado de dinero (ALD), emitió actualizaciones a sus Principios de ALD para el Banco Corresponsal.[1] Los cambios constituyen respuesta al creciente enfoque regulador sobre el ALD y las sanciones económicas y los riesgos asociados relacionados con el banco corresponsal extranjera que han surgido desde que el grupo publicó su guía original en 2002.

La guía se centra en el banco corresponsal tradicional, tales como el establecimiento de relaciones de nostro y vostro, compensación monetaria, gestión de liquidez y préstamos a corto plazo o necesidades de inversión. Puede ser aplicable a SWIFT Aplicación de gestión de relaciones (RMA) relaciones. Sin embargo, el Grupo de Wolfsberg reconoce que algunas jurisdicciones tienen definiciones más amplias del banco corresponsal y que la orientación puede ser aplicable a clientes no bancarios de las instituciones financieras que plantean riesgos similares. La guía se centra en gran medida en la incorporación de varios temas clave en el programa de ALD de la institución.

Responsabilidad y supervisión

Las instituciones deberían establecer políticas y procedimientos que requieren personal específico responsable de garantizar el cumplimiento de estos principios. Esto puede incluir un órgano de gobernanza formal con la vigilancia específica del banco corresponsal extranjera, incluidos el inicio de nuevas relaciones y la escalada de los clientes de mayor riesgo. La aprobación de nuevas relaciones del banco corresponsal se debe obtener de un superior o independiente del patrocinador de la relación. Por otra parte, una revisión independiente se debe emprender para garantizar el cumplimiento de estos requisitos.

Directrices/consideraciones de diligencia debida

Todos los clientes del banco corresponsal deben ser objeto de la diligencia en función del riesgo adecuado, en función del perfil de riesgo del cliente y de la naturaleza de la empresa del cliente. Una serie de factores deben considerarse, en su caso, en la determinación del riesgo de la relación con el cliente. Cada institución debe desarrollar su propia metodología para obtener los niveles de riesgo del cliente, que pueden incluir algunos de o todos estos factores, ponderados o combinados de cualquier manera que la institución elija.

El riesgo geográfico es uno de estos factores de riesgo. Las instituciones deberían considerar la información de organizaciones como el Grupo de Acción Financiera Internacional (GAFI) para evaluar el riesgo del cliente, así como su casa principal y los clientes del cliente.

Las instituciones deben tener en cuenta las sucursales, subsidiarias y afiliadas de los clientes del banco corresponsal. La relación entre un cliente y su empresa matriz, si la hay, debe considerarse. Cuando se trata de estos clientes, el programa de ALD de la casa matriz debe considerarse, sobre todo si el programa de la casa matriz se extiende o no al cliente o si el cliente actúa con bastante autonomía de la casa matriz. Cuando se trata de un afiliado que no está sustancialmente o efectivamente controlado por la casa matriz, la casa matriz y el cliente deben revisarse. Ciertos hechos específicos de una sucursal, subsidiaria o filial pueden dictar que una diligencia debida mejorada (EDD) se aplique (por ejemplo, colegiado en una jurisdicción señalada por el GAFI o de otras autoridades regulatorias locales que exigen EDD).

La guía establece específicamente que sucursales, subsidiarias y afiliadas de la institución, si bien se encuentran dentro de la estructura corporativa, deben ser consideradas clientes y estar sujetas a la diligencia debida en función del riesgo. De nuevo, como con otros clientes, ciertos hechos específicos de una sucursal, subsidiaria o filial pueden exigir que se aplique la EDD. Si bien no se declara explícitamente en las orientaciones, el tratamiento de otros miembros de la institución mayor como clientes pueden servir como un

[1] http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Correspondent-Banking-Principles-2014.pdf

medio útil para el monitoreo del cumplimiento y la comprobación, donde el monitoreo de transacciones puede utilizarse para ayudar a identificar los patrones de la cartera, tal como si proporciona instrucciones completas de envío por cable o si los filtros de sanciones económicas para la filial se realizan adecuadamente.

Las estructuras de propiedad y de gestión del cliente del banco corresponsal son otro componente de riesgo. Los factores que influyen en el riesgo incluyen el país de domicilio y la reputación de los propietarios; la forma jurídica de la empresa del cliente; si es de propiedad estatal, cotiza en bolsa (incluyendo o no si el intercambio en el que aparece tiene una regulación adecuada y si la propiedad significativa de las acciones preocupa) o si es de propiedad privada y cuál es la transparencia de la propiedad. Puede ser apropiado considerar a los ejecutivos de más alto rango a cargo de los negocios del día a día (por ejemplo, el consejo de administración, el consejo de vigilancia, el comité ejecutivo) y si hay noticias negativas asociadas a ellos y si parecen tener suficiente experiencia en la gestión de un banco del tamaño del cliente.

Cualquier persona expuesta políticamente (PEP) en la estructura de gestión o propiedad ejecutiva es una consideración importante, ya que esto aumenta las posibilidades de corrupción política. Para todas las personas con control importante, los beneficiarios finales, las fuentes de riqueza y antecedentes, incluyendo su reputación en el mercado (en particular en relación con las noticias negativas), así como los recientes cambios de propiedad material deben ser determinados en la medida posible a través de la investigación o fuentes públicas. Una comprensión más detallada de la reputación de la dirección ejecutiva del cliente (incluidos cambios significativos recientes) y la identidad de los propietarios controladores importantes deben considerarse cuando existan indicios de noticias negativas.

Obtener un entendimiento del negocio del cliente del banco corresponsal puede influir en el riesgo. Como la parte de sus ingresos implica mayores riesgos de clientes, productos y servicios, el riesgo debe aumentar también. Un banco que ofrece sobre todo la gestión de inversión para grandes

corporaciones multinacionales de todo el mundo tendrá un perfil de riesgo significativamente diferente de uno que ofrece servicios de gestión de tesorería a un gran número de corresponsales menores en una zona de riesgo alto o uno que se centra en ofrecer servicios de banca privada a personas físicas ricas no residentes.

Los productos y servicios que ofrece la institución al cliente alterará de manera significativa el riesgo de la relación. Las instituciones deben documentar el objeto de negocios de la relación con el cliente y la actividad empresarial esperable, para reflejar razonablemente la comprensión de lo que es normal y esperado. Aquellos con los productos de mayor riesgo y de los que se espera mayor uso generalmente presentarían riesgos más altos que los que utilizan los productos de menor riesgo.

La situación regulatoria y la historia del cliente es otro aspecto importante del riesgo general. Se deben tomar medidas razonables para verificar que la entidad está regulada y si el cliente ha sido objeto de alguna medida regulatoria material pertinente, y si es así, para evaluar la medida en que sea relevante para el negocio con el cliente. Si es necesario, nuevas conversaciones con el cliente pueden estar justificadas. A menudo, una vez que la institución ha sido citada públicamente por una violación, está trabajando activamente para hacer frente a esa deficiencia. Esto es cada vez más un requisito en los títulos ejecutivos; los reguladores bancarios de los EE.UU. a menudo ponen fechas límites estrictas en la selección de un consultor independiente para ayudar, redactando un plan para hacer frente a las deficiencias y presentación de informes periódicos sobre los progresos realizados para remediarlos.

Por último, los controles de ALD del cliente deben considerarse. Un enfoque basado en el riesgo debe tomarse para evaluar los controles de ALD del cliente. Esto puede incluir la obtención de respuestas a los cuestionarios de ALD (por ejemplo, el Cuestionario Wolfsberg de ALD, actualizado según las directrices), hablando con los representantes del cliente, la revisión de los controles de ALD (por ejemplo, políticas y procedimientos, una sinopsis de ellos, o incluso una revisión independiente de ellos). Estas oportunidades, sobre todo hablando con el personal de ALD del cliente, pueden ayudar a corroborar otros hallazgos y, a menudo pueden dar lugar a un diálogo mutuamente beneficioso entre los departamentos de ALD de la institución.

Visita al cliente

A menos que otras medidas sean suficientes, una visita del cliente, antes de o dentro de un período razonable de tiempo después del inicio, debería llevarse a cabo. Esto puede o no puede incluir expertos en la materia de ALD, dependiendo del riesgo del cliente. Una reunión en persona es una excelente oportunidad para revisar de primera mano las operaciones de la institución, en lugar de sólo la lectura de la información de tercera mano sobre el cliente, como por ejemplo a través de revisiones de noticias negativas. Sin embargo, como se ha señalado, puede haber otras medidas suficientes, ya que las visitas a los clientes pueden ser difíciles de conseguir en algunos casos (por ejemplo, la logística de los viajes, la disponibilidad de personal, gastos de visitas al sitio). Medios alternativos pueden incluir charlas telefónicas con el cliente y su personal de ALD.

EDD

La guía establece que EDD debe llevarse a cabo cuando ciertos elementos están presentes, para establecer una comprensión suficiente de los riesgos.

Cuando una PEP participa en la relación (por ejemplo, un propietario o un miembro de la alta dirección), la institución debe adoptar medidas para entender a la persona, su papel, la conveniencia del papel, su nivel de influencia con el cliente y el riesgo que presentan a la relación.

> Un enfoque basado en el riesgo debe tomarse para evaluar los controles de ALD del cliente

Cuando el cliente se dedica al banco corresponsal descendente, lo que aumenta el riesgo exponiéndolo a los clientes de sus clientes, se deberían hacer esfuerzos por comprender la naturaleza de las relaciones con los clientes indirectos, incluidos (según el caso) los tipos, número, escala de servicios y la distribución geográfica de los clientes; problemas identificados con el corresponsal descendente; el grado en que el cliente examina los controles de ALD de sus clientes descendentes y si esta actividad presenta un riesgo elevado. Ya que está procesando las transacciones para sus clientes y está confiando en última instancia en sus programas de ALD para ofrecerle a usted comodidad suficiente, su institución debe desarrollar una comprensión suficiente de y saber convivir con estos controles.

Las relaciones de mayor riesgo, tanto en el momento de inicio y revisión periódica, deben estar sujetos a un mayor nivel de aprobación que las relaciones de menor riesgo. Las revisiones periódicas de los clientes de alto riesgo deben realizarse, como mínimo, anualmente.

Seguimiento y notificación de actividades sospechosas

Políticas y procedimientos en todo el banco deben ser implementados para detectar e investigar actividades inusuales o sospechosas y reportar tal como es requerido por la ley aplicable. Estas políticas y procedimientos deberían incluir la orientación sobre lo que se considera inusual o potencialmente sospechoso, incluyendo ejemplos. La institución debe desarrollar una visión integral del cliente, incorporando el monitoreo continuo de la actividad de los clientes con la diligencia debida (incluyendo la calificación de riesgo y otros factores pertinentes) en la evaluación de los riesgos de las transacciones. La institución también debe incorporar los resultados de la vigilancia en la revisión periódica de los archivos del cliente, sobre todo cuando los resultados indican que los niveles de riesgo son elevados. La diligencia debida recogida y el monitoreo realizado deben ser gratuitos; ambos deben informarse mutuamente, en términos de proporcionar información para ayudar a evaluar si la actividad es normal y esperada para el cliente, así como aumentar el riesgo del cliente cuando se observa que el cliente participa en una mayor actividad de riesgo. Esto no quiere decir que los reportes de actividades sospechosas deben incluirse en los archivos del cliente, sino más bien, se deben incorporar, en su caso, en el riesgo global del cliente.

Resumen

La guía ha sido actualizada para reflejar los cambios significativos en las expectativas de los reguladores dentro del banco corresponsal desde la publicación anterior de la guía. Sería útil para una institución evaluar sus prácticas actuales en contra de las Directrices de Wolfsberg, ya que este es un grupo industrial que publica las mejores prácticas para este sector en particular. Las autoridades reguladoras estarán observando esto y considerándolo una mejor práctica de la industria; sería mejor para las instituciones adoptar un enfoque proactivo para la revisión de este documento y hacer cambios antes de que los reguladores vengan y utilicen este nuevo criterio para medir el programa de la institución.

Janice Cassidy Meegan, CAMS, directora, Bank of America, Boston, MA, EE.UU., janice.cassidy.meegan@baml.com

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

Sospecha de que Wang, et al, de la Compañía A, violaron la Ley del Comercio

En marzo de 2012, el Banco A presentó un informe al departamento de antilavado de dinero (ALD), de la Oficina de Investigación (el centro de inteligencia financiera de Taiwan) del Ministerio de Justicia respecto de operaciones sospechosas. Según el informe, el cliente Zhong XX, tenía una cuenta en el banco desde enero de 2012. Sin embargo, Zhong depositaba y retiraba regularmente grandes cantidades de efectivo. Al parecer, la mayoría de las transacciones en cuestión se referían a liquidaciones de compra y venta de acciones. Zhong fue evasivo en sus respuestas a las preguntas formuladas por el personal del banco sobre el origen y el propósito de esos fondos; ella también rechazó las sugerencias de cambiar a remesas. Por lo tanto, sus transacciones despertaron sospechas.

Investigación

A) Tras la aceptación del informe sobre transacciones sospechosas, el departamento de ALD de inmediato comenzó a investigar la identidad de Zhong y su vida profesional. También examinó las transacciones pertinentes y encontró que la mayoría de las transacciones involucraban las acciones de la empresa A, con un volumen significativo de operaciones concentradas de forma repetida en dicha empresa. Dado que Zhong era la cuñada de un conocido especulador de bolsa llamado Zhang XX, el departamento decidió que el caso bien podría incluir el comercio ilegal de acciones. Por lo tanto, lo remitió a la oficina de investigación de Taipei.

B) En ulteriores investigaciones se encontró que:

1. En diciembre de 2011, la compañía A emitió 3.000 bonos convertibles corporativos. El presidente de la empresa Wang XX, el director financiero Huang XX y el especulador de mercado Zhang XX, y Zhang YY, en connivencia con Chen XX de la Compañía de Seguros B distribuyó 2.280 de dichos bonos a Wang, Huang, Zhang XX y Zhang YY por medio de cuentas de mandatario y ejercicios de prospección de demanda (book-building en inglés). Chen recibiría 300 obligaciones convertibles por sus esfuerzos. Además de hacer la diferencia en el precio de los bonos convertibles—como resultado de que llegara a su límite de fluctuación después de haber sido puestos a disposición para el comercio de venta libre (OTC)—las partes arreglaron cuentas de mandatario para la opción de compra de las obligaciones convertibles. Como resultado, se llevaron a cabo aproximadamente cuatro décimas de las acciones de la empresa A mediante el pago de una cantidad nominal.
2. Desde diciembre de 2011, con el fin de inducir a los inversionistas extranjeros a comprar acciones de la empresa A para de ese modo hacer subir el precio de las acciones, Zhang XX y Zhang YY arreglaron para que la Compañía A llevara a cabo transacciones de compra y distribución falsas con proveedores de todo tipo. También inventaron la exportación de mercancías a clientes en el extranjero y llevaron a cabo triangulaciones falsas con varias empresas extranjeras. Zhang XX y Zhang YY incluso trabajaron con empleados de la empresa A para producir documentos de transacción, comprobantes de cuentas de las transacciones falsas mencionadas, y el despliegue de capital de la compañía. Wang y Huang, a su vez, instruyeron al personal de contabilidad de la empresa para que manejaran los procesos de compra y venta y crearan comprobantes de cuentas y pago de mercancías falsos. Por lo tanto, la utilidad de operación de la Compañía A aumentó significativamente entre febrero y octubre de 2012. Así, a los inversores se les hizo creer que la empresa A disfrutaba de buen desempeño empresarial y por lo tanto compraron sus acciones u obligaciones convertibles.
3. Para impulsar el precio de las acciones de la Compañía A, Wang y el resto utilizaron—durante el período de transacciones falsas—las cuentas de valores de la cuñada Zhong de Zhang XX y otros para comerciar exclusivamente las acciones de la empresa A en repetidas ocasiones. Aun cuando las acciones alcanzaron su límite de fluctuación había órdenes de compra, lo cual incitaba a los inversores no iniciados a comprar acciones de la empresa A al día siguiente de la negociación. Con la venta de las acciones de la empresa A a precios altos o ejerciendo sus opciones de compra, que se compraron a precios bajos, Wang y los otros hicieron se beneficiaron en un total de más de 110 millones de dólares taiwaneses.
4. Con el fin de seguir impulsando el alza de los precios de las acciones de la empresa A, a fin de poder vender a precios altos, Zhang XX y Zhang YY buscaron gestores de fondos y los atrajeron por el uso de una proporción fija del importe total obtenido por la venta de las acciones de la empresa A, para comprar acciones de la empresa en el mercado; las transacciones en acciones de la empresa A por fondos mutuos tuvieron el efecto continuado de mantener o incluso hacer subir las acciones de la empresa A. Así Zhang XX y su banda fueron capaces de vender sus acciones al mismo tiempo que fueron adquiridos por los fondos de inversión. Entonces pagaron comisiones a los administradores de fondos en efectivo. Dichos fondos compraron las acciones cuando estaban en alza y las vendieron cuando cayeron. Como resultado, los inversores de los fondos sufrieron pérdidas.
5. A los efectos de la falsa compra de bienes antes mencionada, la empresa A fue obligada a pagar más de 990 millones de dólares taiwaneses a los proveedores amistosos. Una vez deducidos los impuestos de negocios y una tasa de tramitación de

aproximadamente 8 a 10 por ciento, los proveedores necesitarían depositar el saldo en forma de dinero en efectivo en las cuentas de la empresa A ostensiblemente como compras. Alternativamente, se utilizaban los saldos para pagarles a los distribuidores que le habían pagado a la empresa A con cheques. Sin embargo, Zhang XX y Zhang YY eligieron apropiarse indebidamente de los fondos mediante la transferencia a Huang o remitiendo a Wang importes por el 2 por ciento de descuento de los proveedores, o pagando sus gastos de representación. Para acelerar su apropiación indebida de fondos de la empresa A, Huang y el resto hicieron pagos anticipados de bienes a terceros amistosos. Junto con los fondos malversados mencionados, los terceros hicieron que la empresa A incurriera en tener hasta 450 millones de dólares taiwaneses en cuentas por cobrar, los cuales no fueron recuperados.

Litigio

Wang era el presidente de la empresa A, una compañía que cotiza en bolsa, y Huang era su oficial de finanzas principal y portavoz. Como tales, tenían que ser conscientes de su obligación de cuidado y diligencia. En vez, no se aplicaron a las operaciones de la compañía. Desde diciembre de 2011, se pusieron de acuerdo con el gerente general asistente Chen de la Compañía de Seguros B, los especuladores Zhang XX y Zhang YY y se aprovecharon de la emisión de bonos convertibles con garantía de la Compañía A y las posiciones establecidas en acciones de la compañía mediante la compra selectiva a bajo costo, antes de arreglar para comercios falsos con el fin de crear rendimientos de negocios y estados financieros falsos. Tan pronto como la cotización de la compañía alcanzó un máximo, Zhang XX y Zhang YY descargaron sus acciones y ejercieron sus opciones de compra para obtener ganancias ilegales. Entonces sobornaron a los gestores de fondos de inversión de valores para que tomaran acciones de la compañía en niveles altos, lo que provocaba que los inversores de fondos incurrieran en pérdidas. Como tales, fueron acusados de haber violado la Ley del Mercado de Valores, la Ley de Contabilidad Comercial y la Ley de Consultoría y Sociedades de Inversión, etc. En mayo de 2013, un fiscal de la Corte del Distrito de Taipei acusó a Wang y al resto de violaciones de la Ley del Mercado de Valores y la Ley Comercial de Contabilidad de Negocios.

Las lecciones aprendidas en este caso

A) Los indicadores de transacciones irregulares en este caso: el mismo cliente que hace, en diferentes ventanillas, depósitos y retiros de dinero en efectivo que no superan (o superan) el umbral para la presentación de las transacciones sospechosas de lavado de dinero, de manera que la cantidad total alcanzaba cierto nivel. Además, dichas operaciones son claramente incompatibles con la condición y el ingreso del cliente, o no tienen relación con los negocios del cliente.

B) Para los clientes que a menudo llevan a cabo depósitos y retiros por ventanilla de grandes cantidades de dinero en efectivo, el banco informante hizo la investigación adecuada a través de su mecanismo de seguimiento de las transacciones irregulares de la fuente y el uso de los fondos del cliente. El banco también recomendó que el cliente efectuara tales operaciones por medio de remesas para su protección personal. Sus empleados aseguraron que la debida diligencia del cliente (CDD) se llevó a cabo, y se mostraban cautelosos frente a la explicación evasiva del cliente sobre el uso de los fondos y de la negativa de utilizar las remesas, por lo que informaron al Centro de Inteligencia Financiera, permitiendo así que en última instancia el caso fuera descubierto.

C) El Centro de Inteligencia Financiera de Taiwán es una agencia de ejecución de la ley. Todos sus empleados tienen una vasta experiencia en la investigación delictiva, así como en investigación financiera. El centro ha establecido una base de datos para los informes sobre transacciones de divisas (CTR), informes de transacciones sospechosas (SAR) y viajeros que transportan grandes cantidades de moneda extranjera, etc. También está completamente integrado con la base de datos de delitos y la base de datos administrativa, por lo que puede ser altamente efectivo en el análisis de operaciones sospechosas a fin de descubrir las pistas, así como también pudo ayudar a las autoridades policiales para cerrar este caso.

Redactora: Leslie Hsu, agente especial, División de Antilavado de Dinero (FIU, Taiwán), Oficina de Investigación, Ministerio de Justicia, República Popular China

Evaluador: Mike C. J. Lan, jefe de sección, División de antilavado de Dinero (FIU, Taiwán), Oficina de Investigación, Ministerio de Justicia, República Popular China

Su capítulo de ACAMS
—Lo que hay que hacer para tener éxito

Un capítulo exitoso generalmente equivale a tener las personas adecuadas con las intenciones correctas, por medio de las cuales proporcionar educación contra el lavado de dinero (ALD) y oportunidades de establecer contactos con los pares dentro de sus propias comunidades. El artículo de Ed Beemer, *¿Así que quiere empezar un capítulo de ACAMS? Lo que realmente se necesita saber para tener éxito*, publicado en la entrega de diciembre 2013–febrero 2014 de *ACAMS Today* se centra en lo que se necesita para comenzar un capítulo con éxito. Este artículo pone de relieve las responsabilidades de ser un miembro de la junta, las responsabilidades actuales y retos tras el lanzamiento del capítulo e incluye comentarios sobre lo siguiente:

- Hacerse miembro de la junta directiva o presentarse como voluntario;
- Manejo de la conducta de los miembros de la junta directiva;
- Cumplir con la misión del capítulo para proporcionar desarrollo profesional de ALD;
- Planeamiento de eventos; y
- Ampliación de la membresía del capítulo.

Responsabilidad primera

Si usted está contemplando, o ha aceptado un cargo como miembro de la junta directiva de su capítulo local, usted ha reflexionado sobre la oportunidad y ha considerado el compromiso de tiempo que se necesita para apoyar un capítulo exitoso. Asegúrese de que entiende las expectativas y sea justo no sólo consigo mismo, sino también con los demás miembros de la junta directiva.

Cada capítulo puede tener cargos y expectativas adaptados a las personalidades, destrezas, pasiones y los recursos de los socios, así como tomar en cuenta atributos específicos de la comunidad de ALD local. Para ayudarlo a tomar esta decisión, visite las páginas de Capítulos de ACAMS para ver cómo estas oportunidades pueden variar. Esta revisión puede darle ideas sobre cómo complementar mejor los talentos de los miembros de la junta locales con una variada competencia o experiencia que puede ser valiosa.

Si realmente no tiene el tiempo para dedicarse, pero quiere ser parte del capítulo, hágales saber a los miembros de la junta directiva que le gustaría ayudar cuando sí tiene la disponibilidad. Tal vez usted tiene acceso a una lista de oradores interesantes y apropiados o una conexión a un espacio para reuniones y patrocinadores. Cualquiera de estos es útil para la planificación de un calendario de capítulo exitoso. La junta le agradecerá su evaluación honesta de disponibilidad y respetará sus prioridades de tiempo, y apreciará las habilidades, tiempo y recursos que puede contribuir de forma periódica.

La igualdad en la junta directiva

Como Ed Beemer nos recordó a todos en su artículo, los miembros de la junta son voluntarios. Si bien los títulos de los cargos están asociados a cada rol, este está diseñado para ayudar a determinar responsabilidades y no para establecer jerarquías. Cuando surge la política o se muestran comportamientos dictatoriales, los miembros de la junta se verán pronto privados de sus derechos y, finalmente, se alejarán o dejarán de contribuir. Cualquier división o conflicto dentro de la junta puede tener un efecto dominó entre los otros miembros, las actividades de aprendizaje y el establecimiento de contactos.

Desconfíe si el orgullo se convierte en una prioridad sobre la productividad del equipo. Una junta exitosa anima la participación de todos por igual. Esto incluye intervenir y ayudar cuando otro miembro no está o se encuentra abrumado debido a otros compromisos o incluso intervenir para ayudar, independientemente de su papel designado durante un evento. El objetivo de los eventos del capítulo es beneficiar a los asistentes y crear un entorno al que se va a querer volver, que a su vez hará que la afiliación a un capítulo sea constante y creciente, cultivando la asistencia de los no socios y generará ingresos diferentes de los de la cuota de inscripción en los eventos más exitosos del capítulo.

Clave para eventos exitosos

La aceptación de un cargo en la junta directiva significa responsabilizarse de ayudar en el diseño de eventos educativos, de capacitación y de creación de redes para su comunidad local y no debe ser sólo una oportunidad para agregar una viñeta a una hoja de vida. Independientemente de la posición de cualquier persona en su empleo diario, aportar ideas sobre temas, lugares, oradores, motivos, etc., debe ser la meta y la responsabilidad de todos los miembros de la junta. Si el capítulo se ha estructurado con socios de diversos orígenes y de diferentes industrias, la importancia de las contribuciones de todos es crítica cuando hay una sesión de lluvia de ideas sobre un evento próximo. Ser capaz de tomar una buena idea de alguien y ampliarla por lo general conduce a un mejor evento. Recuerde, sin la participación de otros miembros del equipo, el evento podría ser simplemente bueno y no excelente.

Los que no están involucrados en la preparación de eventos no siempre comprenden el esfuerzo realizado por sus colegas. El compromiso de tiempo para "hacer las cosas bien" tiene que ser compartido por todos en la junta directiva. Algunas ideas que vale la pena tomar en cuenta incluyen:

- Organización de eventos
  - — Crear listas de verificación con una línea de tiempo preestablecida
  - — Ponerse de acuerdo con el tema y la duración del programa
  - — Desarrollar la descripción del evento para captar la atención de los asistentes
  - — Asegurarse de que la descripción de un evento de capacitación tiene palabras clave que proporcionan beneficios a los participantes (es decir, ideas para actualizar las políticas/procedimientos o tendencias que conviene buscar)
  - — Conseguir oradores y confirmar biografías para presentar a los oradores y redactar las invitaciones
  - — Confirmar créditos disponibles de ACAMS
  - — Determinar si el evento califica para créditos de CLE
  - — Conseguir patrocinadores, comunicar requisitos de ACAMS, y confirmar el uso de logotipos para las invitaciones, señalización de eventos, etc.
  - — Confirmar lugar/costo/accesibilidad
  - — Crear plantillas para sus comunicaciones
  - — Reunirse con su(s) orador(es) para asegurar que el tema que aborda y se prepara y para delinear un cronograma y un formato. Estas reuniones sirven mucho para construir una buena relación con sus oradores

— Confirmar cualquier equipo necesario para eventos: proyectores (con bombillas que funcionan), computadoras portátiles, micrófonos, podios, etc.

- Gestión de un evento

— Asignar tareas a todos (montaje y desmontaje de puestos de inscripción, alimentos y bebidas, recibir a los invitados, palabras de bienvenida y de clausura, etc.)

— Revisar la lista de actividades después de cada evento para descubrir lo que faltaba o lo que se podría haber mejorado

— Hacer un seguimiento de implicaciones de los miembros de la junta directiva y elevarlas para cumplir con el siguiente evento (aburre que sea la misma gente que hace y deshace). Dividir su junta directiva en grupos básicos que varían las responsabilidades a cada evento garantiza que todos participan por igual. Los eventos mayores/más largos pueden necesitar la participación de todos para tener éxito.

— Considerar el uso de una encuesta de eventos, ya sea en forma impresa el día del evento o en línea después. Recuerde:

➤ No se sienta ofendido cuando se proporcionan comentarios negativos. Considere la posibilidad de que sea un desafío para mejorar el próximo evento.

➤ Pídales a los encuestadores temas de interés, ya que algunos pueden sorprenderlo y pueden ser útiles para su próximo evento.

➤ Nunca asuma que usted conoce por completo a su público.

Nota: Que sea obligado en todos los eventos saludar y pasar momentos con los invitados. Recuerde que los eventos son oportunidades de establecer contactos y aumentar la membresía. Las primeras impresiones de los asistentes nuevos son importantes y muchas veces determinan la participación futura.

Cómo conseguir patrocinadores

Los patrocinadores son muy importantes para el éxito de un evento. Hay dos maneras de asegurarse patrocinios o esponsoreos. En primer lugar, el director del evento puede tener relaciones existentes con los proveedores y estar dispuesto a contactarlos. En segundo lugar, los miembros de la junta directiva pueden preguntarles a los proveedores con quienes trabajan en sus instituciones. Muchos de los vendedores están dispuestos a proporcionar fondos para causas que valen la pena si tienen presupuesto. Ellos van a querer entender los detalles del evento, el orden del día previsto, y los beneficios para el patrocinador. El Manual de Capítulos proporciona algunas buenas directrices sobre lo que los beneficios deberían ser. Utilice estas guías como una ayuda para asegurar que el capítulo y el patrocinador están a la par. Por ejemplo, asegúrese de incluir su logo en la invitación, mantenerlos informados de los detalles y transmítales la información prometida y asegúrese de que los patrocinadores reciben un trato justo.

Recuerde que cuando se destaca el nombre como patrocinador, la percepción de los asistentes del evento se refleja sobre el patrocinador. Si hay comida, ¿qué se ofrece? La gente no entiende que el capítulo es el que está seleccionando la comida y la bebida. Tenga en cuenta que cuanto mayor sea el evento, más altas son las expectativas de los asistentes. Por ejemplo, si se trata de un evento de cuatro horas con almuerzo, la oferta debe incluir una variedad de bebidas y agua. Piense en lo que usted busca antes o después de estar sentado durante un largo período de tiempo en una conferencia, normalmente café o un refresco y tal vez algo salado o dulce.

Concluyendo

Por último, recuerde que debe agradecer a sus patrocinadores, ponentes e invitados. Esto debe ser tanto en persona como en los medios. Este paso adicional refuerza su contribución y reconoce la apreciación del capítulo.

Recuerde que un capítulo exitoso quiere decir tener la gente adecuada dispuesta a proveer educación y oportunidades de contacto de ALD a sus pares dentro de sus propias comunidades. Significa ser respetuoso y reflexivo con el talento y las ideas traídas por otros miembros de la junta directiva del capítulo, así como de sus miembros. No hay jerarquía y esto es un trabajo voluntario. Usted está representando a ACAMS en su comunidad.

Por otra parte, un evento de capítulo exitoso requiere que todos pongan manos a la obra y la participación activa de todos. Asegúrese de dar las gracias a los que hacen un esfuerzo adicional para mantener buena voluntad para los acontecimientos futuros. Nunca asuma que los que llevan un cierto título también llevan toda la responsabilidad relacionada con ese papel. Por ejemplo, todos son responsables de captar nuevos socios y todos son responsables de montar y desmontar un evento. Sea sensible a que los eventos son un esfuerzo grupal y, sobre todo, ¡diviértase!

Nota final: ¡Felicidades a todos los que toman los pasos próximos para apoyar a las juntas directivas de sus capítulos locales combinando sus pasiones en la lucha contra los delitos internacionales de lavado de dinero, con la capacidad de organización, la creación de redes profesionales de éxito y participando en un equipo con liderazgo!

Sande Bayer, CAMS, miembro de la junta directiva del capítulo de GTC, vicepresidente de cumplimiento de ALD, U.S. Bank, Minneapolis, MN, EE.UU., sandra.bayer@usbank.com

Shannon Bennett, CRCM, CAMS, miembro de la junta directiva del capítulo de GTC, directora de Estrategia de la Lucha contra la Delincuencia Financiera, Wolters Kluwer Financial Services, Minneapolis, MN, EE.UU., Shannon.bennett@wolterskluwer.com

ACAMS CANADA Chapter

ACAMS SOUTHERN NEVADA CHAPTER

Association of Certified Anti-Money Laundering Specialists® ACAMS®

Australasian Chapter

ACAMS | Risk Assessment®

MEASURING, UNDERSTANDING & EXPLAINING AML RISK

Help your institution:

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

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

Cesar Marcelo:
Departamento de Contabilidad

Cesar Marcelo se unió a la Asociación de Especialistas Certificados en la Lucha contra el Lavado de Dinero (ACAMS) como contador senior en septiembre de 2009 y actualmente se desempeña como interventor. Sus responsabilidades como interventor incluyen asegurar el exacto y completo cierre contable mensual y la preparación de los estados financieros. Marcelo también es responsable de los resultados informados de las operaciones de integridad financiera de ACAMS.

Antes de emplearse en ACAMS, Marcelo se desempeñó como contador senior de Cushman & Wakefield de la Florida, donde se responsabilizaba de la preparación de presupuestos, la previsión de ingresos y de los estados financieros para el mercado del sur de la Florida. Durante los cuatro años y medio que Marcelo ha estado con ACAMS, el ha trabajado cerca con el director financiero en muchos proyectos diferentes, como también en la supervisión de la producción de estados financieros auditados nacionales e internacionales de ACAMS.

ACAMS Today: ¿Cómo se enteró usted de ACAMS?

Cesar Marcelo: Me enteré de ACAMS a través de mi esposa, que trabajó 11 años en la industria de la banca internacional y muchos de los oficiales de cumplimiento con los que ella trabajó tenían certificación de CAMS.

AT: ¿Cuál diría que es la parte mejor y más desafiante de su trabajo?

CM: Lo mejor y lo más difícil de mi trabajo aquí en ACAMS ha sido mantenerme al tanto de la expansión nacional e internacional. Desde que comencé en ACAMS hemos añadido oficinas en Japón, Beijing, la India y el Reino Unido. En el plano interno, también hemos añadido una cantidad significativa de personal para nuestras operaciones de actualizarse con el crecimiento.

AT: ACAMS ofrece muchos productos y servicios a sus socios, ¿cuál es el producto o servicio que considera más interesante?

CM: El Programa de Desarrollo de Capítulos de ACAMS está prosperando. Actualmente contamos con 40 capítulos (y seguimos contando) en todo el mundo. Los capítulos ofrecen foros locales donde ofrecen educación regional específica y, además, fomentan la creación de redes profesionales entre los socios de ACAMS. He tenido el placer de interactuar con varios socios en eventos en el sur de Florida y es gratificante ver la camaradería de la comunidad local de ALD como consecuencia del capítulo.

AT: ¿Qué te gusta hacer cuando no estás en la oficina?

CM: Cuando no estoy en la oficina me gusta pasar tiempo con mi familia. También me gusta el ciclismo de montaña y la pesca en alta mar en los cayos.

AT: ¿Cuál es el mejor consejo que has recibido?

CM: El mejor consejo que he recibido fue "rodéate de buena gente". A

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

Con la contribución de: Alexa Serrano, asistente editorial, ACAMS, Miami, FL, EE.UU., aserrano@acams.org

A NEW INVESTIGATIVE PLATFORM: CLEAR® FOR ENHANCED DUE DILIGENCE

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

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

THOMSON REUTERS™

CHANGE YOUR DATA PROVIDER

NEGATIVE NEWS – SANCTIONS – PEPS

NEGATIVENEWSPLUS

COST EFFECTIVE NEGATIVE NEWS SERVICE

- A search engine providing compliance professionals the latest in historical negative news for screening individual and corporate accounts
- Continuously indexes thousands of news pages daily from national and international sources
- Built in audit trail and automatic monitoring function that processes your historical searches and checks them against the latest negative news every 24 hours
- Automatic monitoring feature eliminates the need to re-submit searches

OFACPLUS

EFFICIENT SANCTIONS, PEP AND RISK DATA SERVICE

- Aggregates risk sources, sanctions and watch lists into an easy to use data file or web service
- Database automatically updates changes to subscribed lists
- Supports optional name variants
- Integrates seamlessly and can be used with all transaction monitoring, case management and core banking systems

NominoData

Contact: sales@nominodata.com or call +1 775 384 8554