



GONZALO VILA

ACFCS



SANCIONES

The word "SANCIONES" is written in a bold, black, hand-drawn font. It is positioned over two overlapping rectangular blocks: a yellow one on the left and a red one on the right. The red block is slightly offset to the right and overlaps the yellow one. The text is centered horizontally across these blocks.

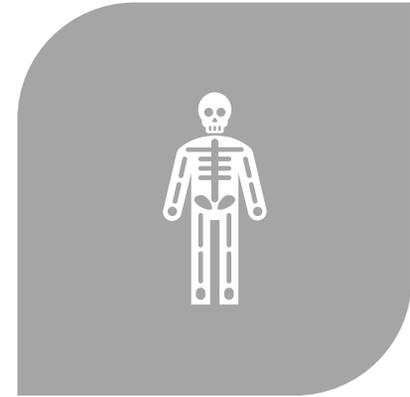
Compliance



AML LAWS AND REGULATIONS IN
THE US (BSA, USA PATRIOT ACT, ET
AL)



FCPA - FOREIGN CORRUPTION
PRACTICE ACT



RÉGIMEN DE SANCIONES **OFAC**,
DEL DEPARTAMENTO DEL TESORO

2019

Standard Chartered Bank US\$640 millones (Reino Unido)

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced a \$639,023,750 settlement with Standard Chartered Bank

From June 2009 until June 2014, SCB processed 9,335 transactions totaling \$437,553,380 that were processed to or through the United States. All of these transactions involved persons or countries subject to comprehensive sanctions programs administered by OFAC.

2005

ABN Amro US\$80 millones

2009

Lloyds US\$350 millones

Credit Suisse US\$540 millones

2010

RBS (ABN Amro) US\$500 millones (Reino Unido)

Barclays \$298 millones (Reino Unido)

2011

JP Morgan US\$88.3 millones (EE.UU.)

2012

HSBC US\$1.900 millones (Reino Unido)

Standard Chartered US\$667 millones (Reino Unido)

ING US\$619 millones (Holanda)

Bank of Tokyo-Mitsubishi US\$8.6 millones (Japón)

2013

RBS US\$100 millones (Reino Unido)

Intesa Sanpaolo US\$3 millones (Italia)

2014

BNP Paribas US\$8.900 millones (Francia)

Clearstream Banking US\$152 millones (Alemania)

Bank of Moscow US\$9.5 millones (Rusia)

Bank of America US\$16.6 millones (EE.UU.)

Bank of Tokyo-Mitsubishi US\$315 millones (Japón)

2015

Commerzbank AG US\$1.450 millones (Alemania)

Crédit Agricole US\$329 millones

PayPal US\$7.6 millones (EE.UU.)

Banco do Brasil, S.A. US\$139,500 (EE.UU.)

2016

Barclays Bank PLC US\$2.48 millones (Reino Unido)

2018

JPMorgan Chase Bank, N.A. US\$5.26 millones (EE.UU.)

Société Générale S.A. US\$54 millones (Francia)

Bancos LatAm

- El Banco Continental S. A., empresa hondureña se convirtió en la primera institución bancaria en entrar al listado OFAC de Estados Unidos de individuos y empresas del andamiaje financiero de “lavado” de ganancias del narcotráfico, fue cerrado por el Gobierno de Honduras, que dispuso una “liquidación forzosa”. **OCTUBRE DE 2015**
- Balboa Bank & Trust, en el que uno de sus directivos fue acusado en **MAYO DE 2016** por presunto blanqueo de capitales y narcotráfico, lo que provocó su inclusión en la denominada Lista Clinton.
- BANCORP Nicaragua, **ABRIL 2019**

[Press Releases](#)[Statements & Remarks](#)[Readouts](#)[Testimonies](#)[Featured Stories](#)[Press Contacts](#)

Treasury Sanctions Argentina-based Goldpharma



May 23, 2019

Goldpharma network of illegal online pharmacies traffics opioids to the United States

Washington – Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) identified the Argentina-based Goldpharma Drug Trafficking and Money Laundering Organization (Goldpharma DTO/MLO) as a significant foreign narcotics trafficker pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act). OFAC also designated eight Argentine nationals for their role in the Goldpharma DTO/MLO, as well as nine entities located

May 23, 2019

[Treasury Sanctions Argentina-based Goldpharma](#)

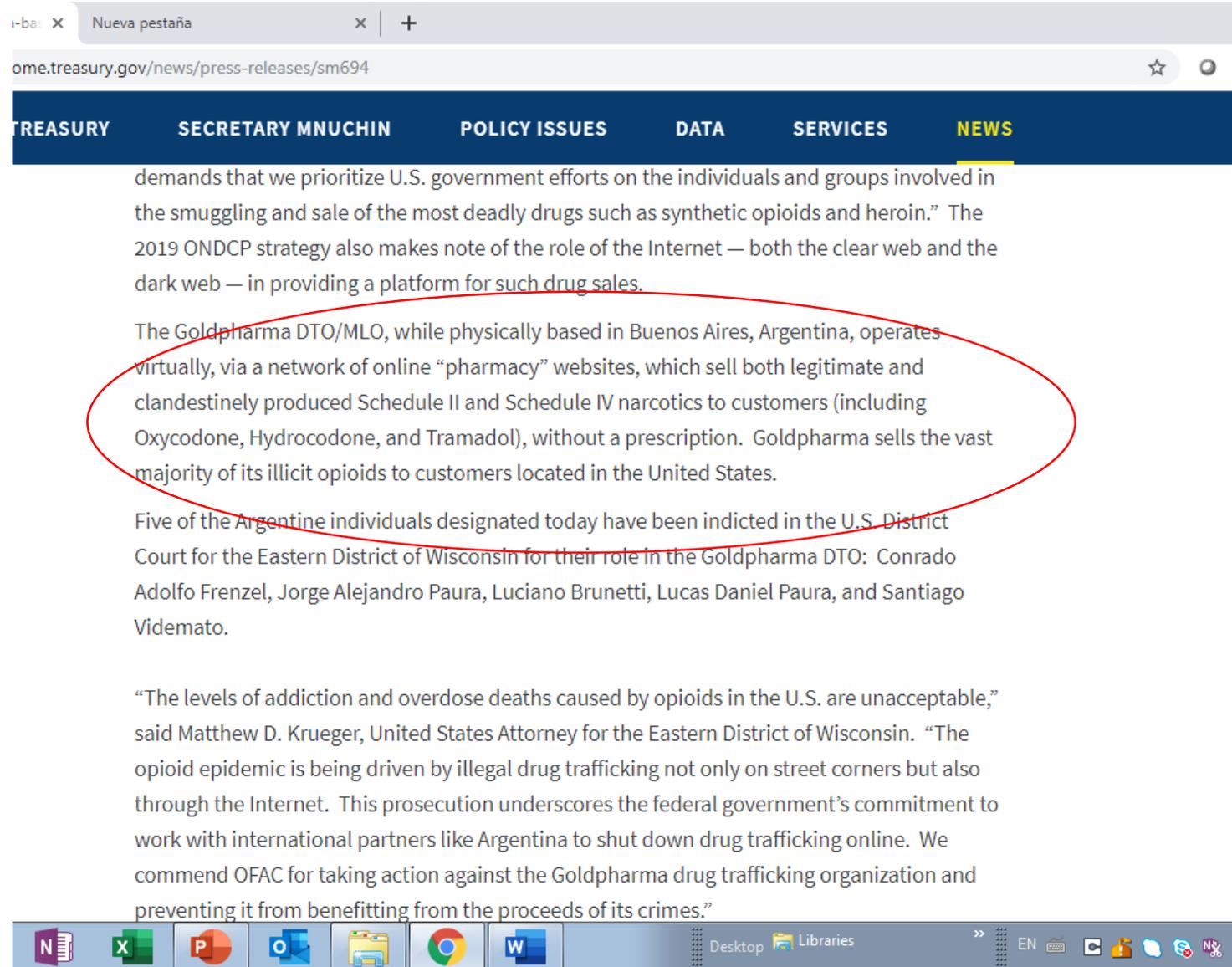
May 17, 2019

[Treasury May 17 Response to Chairman Neal Regarding Tax Return Request](#)[Treasury Works with Government of Mexico Against Perpetrators of Corruption and their Networks](#)

May 16, 2019

[Treasury Targets Additional Individuals Involved in the Sergei Magnitsky Case and Gross Violations of Human Rights in Russia](#)

May 15, 2019



The screenshot shows a web browser window with the URL [ome.treasury.gov/news/press-releases/sm694](https://www.treasury.gov/news/press-releases/sm694). The browser's address bar and tabs are visible at the top. Below the address bar is a dark blue navigation bar with the following menu items: TREASURY, SECRETARY MNUCHIN, POLICY ISSUES, DATA, SERVICES, and NEWS (which is highlighted in yellow). The main content area of the page contains three paragraphs of text. The second paragraph is circled in red. At the bottom of the browser window, the Windows taskbar is visible, showing icons for Microsoft Word, Excel, PowerPoint, Outlook, File Explorer, Google Chrome, and Microsoft Word. The system tray on the right side of the taskbar shows the date and time as 'EN 10/10/2017 10:10' and several system icons.

demands that we prioritize U.S. government efforts on the individuals and groups involved in the smuggling and sale of the most deadly drugs such as synthetic opioids and heroin.” The 2019 ONDCP strategy also makes note of the role of the Internet — both the clear web and the dark web — in providing a platform for such drug sales.

The Goldpharma DTO/MLO, while physically based in Buenos Aires, Argentina, operates virtually, via a network of online “pharmacy” websites, which sell both legitimate and clandestinely produced Schedule II and Schedule IV narcotics to customers (including Oxycodone, Hydrocodone, and Tramadol), without a prescription. Goldpharma sells the vast majority of its illicit opioids to customers located in the United States.

Five of the Argentine individuals designated today have been indicted in the U.S. District Court for the Eastern District of Wisconsin for their role in the Goldpharma DTO: Conrado Adolfo Frenzel, Jorge Alejandro Paura, Luciano Brunetti, Lucas Daniel Paura, and Santiago Videmato.

“The levels of addiction and overdose deaths caused by opioids in the U.S. are unacceptable,” said Matthew D. Krueger, United States Attorney for the Eastern District of Wisconsin. “The opioid epidemic is being driven by illegal drug trafficking not only on street corners but also through the Internet. This prosecution underscores the federal government’s commitment to work with international partners like Argentina to shut down drug trafficking online. We commend OFAC for taking action against the Goldpharma drug trafficking organization and preventing it from benefitting from the proceeds of its crimes.”

In addition, the OFAC action targets Argentine nationals Sergio David Ferrari, Gaston Tomaghelli, and Roberto Javier Perez Santoro for their involvement in Goldpharma's money laundering activities. Ferrari operates a network of entities in multiple countries, known collectively as the "Smile Group," which funnels the proceeds of Goldpharma's narcotics sales back to Argentina. Several of the entities belonging to the "Smile Group" were designated today, including Smile Technologies S.A. (registered in Argentina), SmileWallet S.A.S. (registered in Colombia), Smile Property & Travel Ltd. (registered in the United Kingdom), Smile Technologies Canada Ltd. (registered in Canada), and SmileWallet B.V. (registered in the Netherlands).

Seven U.S. companies owned or controlled by designated members of Goldpharma have also been blocked as part of today's action. These entities include two companies registered in Delaware: SmilePayments LLC and Oyster Investments LLC; three companies registered in Texas: Smilewallet, LLC, Smile Property & Travel Ltd., and Smile Technologies S.A. LLC; and two companies registered in Florida: La Florida Investments Group LLC and Water Hill Corp. As a result of today's action, four condominiums in the Miami, Florida area tied to Oyster Investments LLC have also been blocked.

[Nationals List \(SDN List\)](#)[Consolidated Sanctions List](#)[Search OFAC's Sanctions Lists](#)[Additional Sanctions Lists](#)**OFAC Recent Actions**[Complete List of Sanctions Programs and Country Information](#)[Frequently Asked Questions](#)[OFAC Civil Penalties and Enforcement](#)[Contact OFAC](#)[International](#)[Small Business Programs](#)[Tax Policy](#)[Terrorism and Illicit Finance](#)[Data and Charts Center](#)[FAQ](#)

OFFICE OF FOREIGN ASSETS CONTROL

Specially Designated Nationals List Update

The following individuals have been added to OFAC's SDN List:

BRUNETTI, Luciano (a.k.a. "BIFF TANNEN"; a.k.a. "LUCHO"), Buenos Aires, Argentina; DOB 30 Aug 1988; POB Argentina; nationality Argentina; Gender Male; Passport AAC206993 (Argentina); D.N.I. 34142353 (Argentina) (individual) [SDNTK].

FERRARI, Sergio David (a.k.a. "Yagy"), Chivilcoy 3157 Piso 2 Depto D, Buenos Aires 1417, Argentina; Buenos Aires, Argentina; DOB 10 Feb 1968; POB Buenos Aires, Argentina; nationality Argentina; Gender Male; Passport AAA760416 (Argentina); D.N.I. 20010866 (Argentina); C.U.I.T. 20200108664 (Argentina) (individual) [SDNTK] (Linked To: SMILE TECHNOLOGIES S.A.; Linked To: SMILE PROPERTY & TRAVEL LTD; Linked To: SMILEWALLET S.A.S.; Linked To: SMILE TECHNOLOGIES CANADA LTD).

FRENZEL, Conrado Adolfo (a.k.a. "OTTO"), Buenos Aires, Argentina; DOB 07 Nov 1968; POB Buenos Aires, Argentina; nationality Argentina; Gender Male; Passport AAA435057 (Argentina); D.N.I. 20608046 (Argentina); C.U.I.T. 23206080469 (Argentina) (individual) [SDNTK] (Linked To: HIGH NUTRITION SOCIEDAD DE RESPONSABILIDAD LIMITADA; Linked To: B-WORK S.A.S.).

PAURA, Jorge Alejandro (a.k.a. "LARRY"), Buenos Aires, Argentina; DOB 31 Oct 1967; POB Buenos Aires, Argentina; nationality Argentina; Gender Male; Passport AAB376848 (Argentina); D.N.I. 18580686 (Argentina); C.U.I.T. 20185806864 (Argentina) (individual) [SDNTK] (Linked To: BAJER S.R.L.; Linked To: HIGH NUTRITION SOCIEDAD DE RESPONSABILIDAD LIMITADA).

PAURA, Lucas Daniel, Buenos Aires, Argentina; DOB 04 Jan 1988; POB Buenos Aires, Argentina; nationality Argentina; Gender Male; Passport 33533978N (Argentina); D.N.I. 33533978 (Argentina) (individual) [SDNTK].

<https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190523.aspx>



CRIPTOACTIVOS

ome.treasury.gov/news/press-releases/sm556

of the United States Government

Accessibility Languages

DEPARTMENT OF THE TREASURY

SECRETARY MNUCHIN POLICY ISSUES DATA SERVICES **NEWS**

PRESS RELEASES

Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses

388 242

LATEST NEWS

May 17, 2019
Treasury May 17 Respor
Neal Regarding Tax Reti

Treasury Works with Go
Against Perpetrators of
their Networks

May 16, 2019
Treasury Targets Additi
Involved in the Sergei M
Gross Violations of Hur

May 15, 2019
Statement of Secretary

Desktop Libraries ES

Central to the SamSam ransomware scheme's success were **Khorashadizadeh** and **Ghorbaniyan**, who helped the cyber actors exchange digital currency derived from ransom payments into Iranian rial and also deposited the rial into Iranian banks. To help convert the digital currency ransom payments into rial, **Khorashadizadeh** and **Ghorbaniyan** used the following two digital currency addresses: 149w62rY42aZBox8fGcmqNsXUzSStKeq8C and 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V. Since 2013, **Khorashadizadeh** and **Ghorbaniyan** have used these two digital currency addresses to process over 7,000 transactions, to interact with over 40 exchangers—including some US-based exchangers—and to send approximately 6,000 bitcoin worth millions of USD, some of which involved bitcoin derived from SamSam ransomware.

SECURITY & FRAUD

Five Or More Mexican Banks Suffer Unauthorized Transfers

By PYMNTS
Posted on May 14, 2018



TRENDING RIGHT NOW



APPLE
Apple Close To \$1 Trillion In Mkt Cap, With Amazon Close Behind



SECURITY & FRAUD
Credit Card Data Stolen In Chili's Malware Attack

https://www.pymnts.com/apple/2018/apple-amazon-stock-one-trillion-retail/

Hackers robaron US\$10 millones en ataque al Banco de Chile

El caso sería el mayor ciberataque sufrido por un banco chileno, y se suma a otros contra instituciones financieras en la región y el mundo



Una banda de hackers que atacó el mes pasado al privado Banco de Chile logró robar cerca de US\$10 millones, los que en gran parte terminaron en cuentas en Hong Kong, dijo el gerente general de la firma en una entrevista a un medio local publicada el sábado.

Banco de Chile CHI.SN, la segunda entidad financiera del país, desconectó unas 9.000 estaciones de trabajo en sus sucursales el 24 de mayo en un intento por frenar la propagación de un virus, que habría servido de distracción para sustraer el botín, según dijo Eduardo Ebensperger al diario La Tercera.



Ciberataque al Banco de Chile: Queda en evidencia que SBIF tiene poca capacidad para auditar ataques informáticos

Archivado en: Banca · SBIF · seguridad informática · Banco de Chile · Felipe Harboe · Mario Farren

Estrategia On line | Jueves, 7 de junio de 2018, 19:47

 Compartir 1  

Por indicación del senador Felipe Harboe, este miércoles 6 de junio la Comisión de Economía del Senado citó al superintendente de Bancos e Instituciones Financieras (SBIF), Mario Farren, para que entregara explicaciones respecto al problema informático sufrido por el Banco de Chile hace unas semanas, dejando en evidencia la poca capacidad que tiene la institución para auditar ataques informáticos.



"La Superintendencia se transformó en un vocero del Banco de Chile", señaló el senador Harboe frente a la explicación difundida por el ente regulador, que se limitó a replicar la infor

ver3.bigapis.net/www/delivery/ck.php?oaparams=2__bannerid=2444__zoneid=62

transformó en un vocero del Banco de Chile", señaló el senador Harboe frente a la explicación difundida por el ente regulador, que se limitó a replicar la información entregada por el banco, con lo que a juicio del parlamentario se confirma "que no existe una capacidad real de la Superintendencia para poder entender y saber, a ciencia cierta y con información propia, lo ocurrido con el Banco de Chile". En este sentido, el legislador PPD indicó que resulta evidente que la SBIF requiere mejorar su capacidad técnica. "No es aceptable que el regulador sólo se guíe por la información que le entrega el afectado, el banco en este caso".

Por otro lado, la Comisión de Economía del Senado solicitó a Farren transparentar las inversiones que están llevando a cabo los bancos en materia de seguridad e informática, puesto que resulta evidente que hay una carencia al respecto, acordando una próxima citación en la comisión.

"Lo más importante acá es asegurarnos que en este proceso de bancarización y digitalización de la economía, los bancos han tomado las medidas para resguardar la seguridad informática para evitar lo ocurrido con el Banco de Chile. Este no es un caso puntual, tenemos una serie de faltas de inversión en esta materia", señaló Harboe, quien antes de ser senador se desempeñó como subsecretario del Interior.

5
6
7
8
9
10

OFAC emite una guía detallada con expectativas de compliance, mejores prácticas y deficiencias en fallas pasadas

7 mayo, 2019 / por [Gonzalo Vila](#)

El brazo del Tesoro de EE.UU. encargado de administrar los programas de sanciones del país ha emitido su guía más detallada y prescriptiva hasta el momento sobre lo que considera un programa de cumplimiento sólido para evitar que los bancos y las empresas de todo tipo se enfrenten a los cambiantes requisitos que las obligan [...]

[Leer más](#)

OFAC declara que si bien cada SCP basado en el riesgo variará dependiendo de una variedad de factores, incluidos el tamaño y la sofisticación de la compañía, los productos y servicios, los clientes y las contrapartes y las ubicaciones geográficas, cada programa debe basarse e incorporar al menos cinco componentes esenciales de cumplimiento:

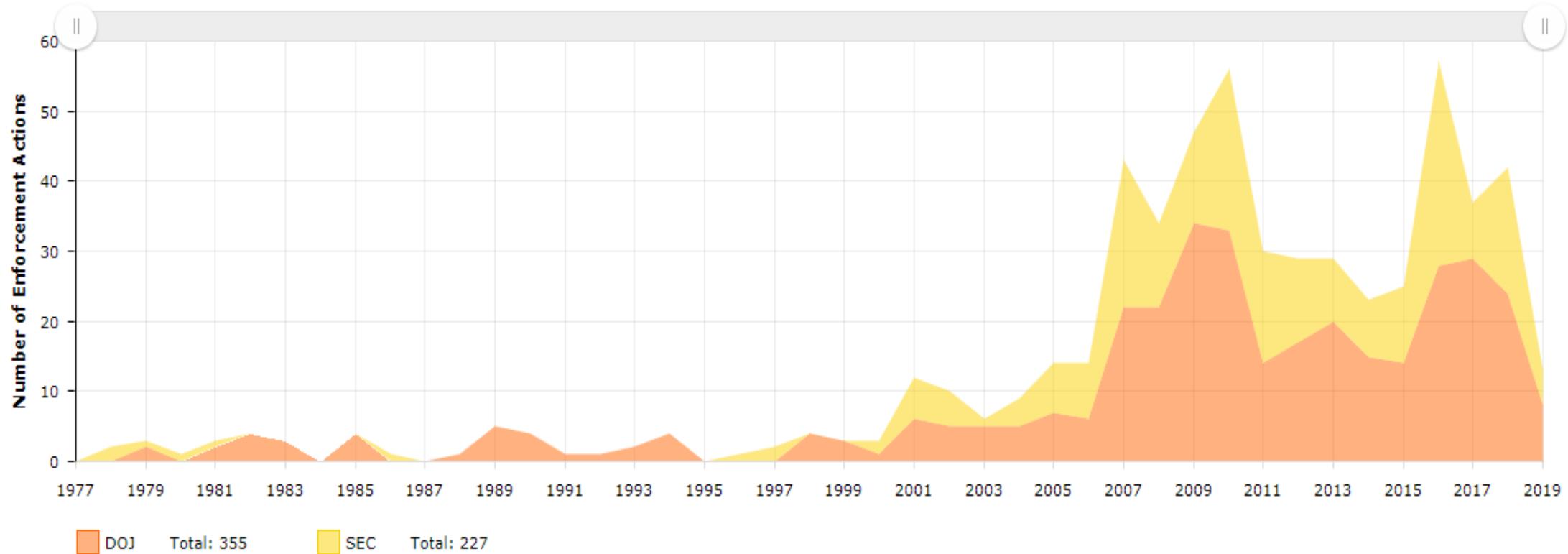
- Compromiso de la gerencia / administración: promueve una cultura de cumplimiento al garantizar que los empleados de SCP tengan la autoridad, la autonomía, los recursos y la capacidad de respuesta ejecutivas adecuadas para las fallas.
- Evaluación de riesgos: similar a la evaluación de riesgos ALD/CFT, pero realizada a través de la lente de las políticas de sanciones de EE.UU., reconociendo la importancia de los regímenes deshonestos, evasores de sanciones.
- Controles internos: como en el caso del sistema de monitoreo de transacciones ALD/CFT, estos pueden incluir los sistemas automatizados de detección de sanciones en vigencia y las políticas sobre las investigaciones y la escalada de posibles impactos.
- Pruebas y auditorías: este suele ser un grupo fuera del ámbito de sanciones—ya sea interno o externo—, que puede revisar tanto las entradas como los resultados de las sanciones y analizar las decisiones del personal para garantizar que los posibles impactos se analicen, se escalen y se eliminen.
- Capacitación: sin capacitación sobre cómo los regímenes evaden las políticas de sanciones, en qué regiones del mundo sucede esto y de qué manera, como a través del comercio y los corresponsales cooptados, no hay manera de que los analistas puedan tomar las decisiones correctas. La capacitación debe ser expansiva, relevante, matizada e infundida con los cambios de poder geopolíticos que impulsan a los evasores de sanciones.

LA CERTIFICACIÓN CFCS
ES LA JUGADA PERFECTA
QUE CAMBIARÁ SU CARRERA



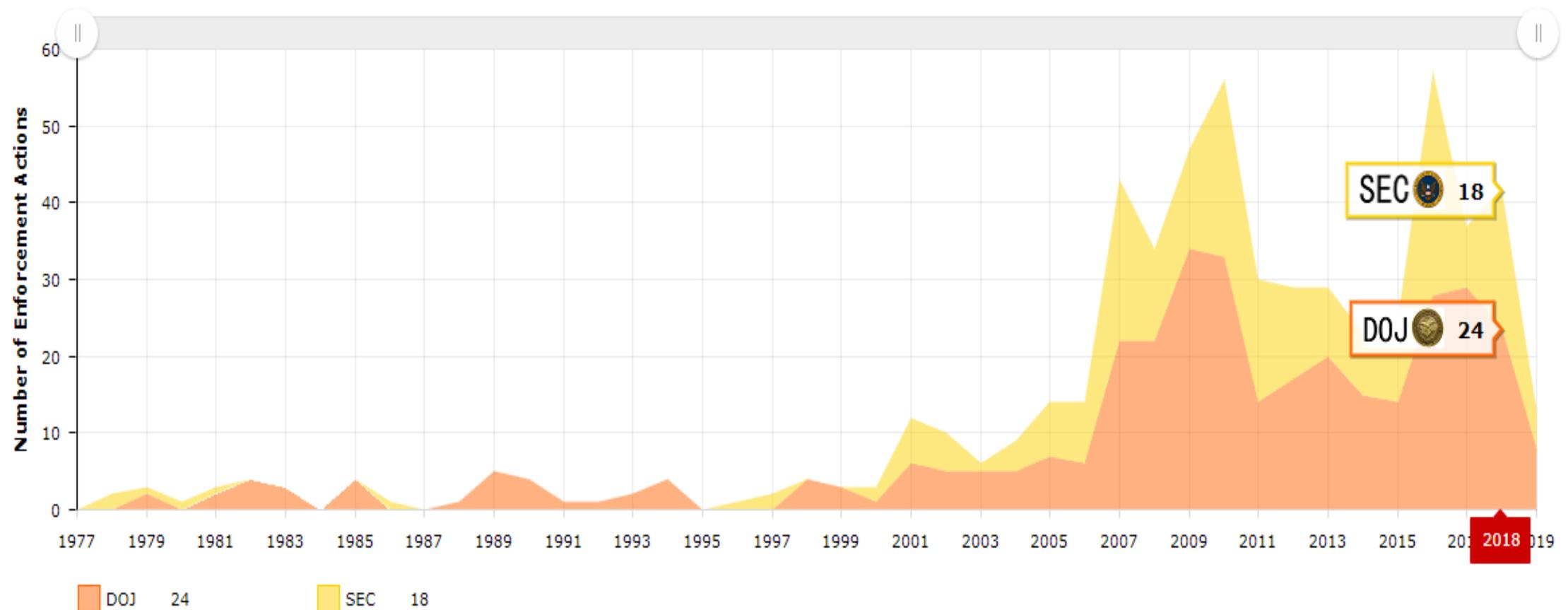
¿Qué es la FCPA?

- **Una ley de EE.UU. promulgada en 1977**
- **Enfocada en dos áreas**
 - Sobornos de funcionarios extranjeros
 - Requiere libros y registros contables precisos y buenos controles internos
- **Aplicada por el Departamento de Justicia de EE.UU. y la Comisión de Valores y Bolsas (SEC)**
 - Departamento de Justicia tiene jurisdicción sobre las compañías estadounidenses y sus subsidiarias
 - SEC tiene jurisdicción civil sobre las compañías que cotizan en bolsa



Description for DOJ and SEC Enforcement Actions per Year

This chart identifies the number of Enforcement Actions the SEC or DOJ initiated per year, for each year since the statute's enactment. By hovering over a year, users can see the number of Enforcement Actions filed by the SEC and the number of Enforcement Actions filed by the DOJ. If the SEC and DOJ jointly file an Enforcement Action, that action is counted once for the SEC and once for the DOJ. See [About Us - Datasets](#) for a definition of "Enforcement Action." There are many ways to define an FCPA enforcement action and to count the number of such actions filed per year. This graphic presents one possibility among several.



Description for DOJ and SEC Enforcement Actions per Year

This chart identifies the number of Enforcement Actions the SEC or DOJ initiated per year, for each year since the statute's enactment. By hovering over a year, users can see the number of Enforcement Actions filed by the SEC and the number of Enforcement Actions filed by the DOJ. If the SEC and DOJ jointly file an Enforcement Action, that action is counted once for the SEC and once for the DOJ. See [About Us - Datasets](#) for a definition of "Enforcement Action." There are many ways to define an FCPA enforcement action and to count the number of such actions filed per year. This graphic presents one possibility among several.

- 1. Petrobras (Brasil): US\$1.780 millones en 2018.**
- 2. Telia Company AB (Suecia): US\$965 millones en 2017.**
- 3. MTS (Rusia): US\$850 millones en 2019.**
- 4. Siemens (Alemania): US\$800 millones en 2008.**
- 5. VimpelCom (Holanda): US\$795 millones en 2016.**
- 6. Alstom (Francia): US\$772 millones en 2014.**
- 7. Société Générale S.A. (Francia): US\$585 millones en 2018.**
- 8. KBR / Halliburton (Estados Unidos): US\$579 millones en 2009.**
- 9. Teva Pharmaceutical (Israel): US\$519 millones en 2016.**
- 10. Keppel Offshore & Marine Ltd.(Singapur): US\$422 millones en 2017.**

1. Petrobras (Brasil): US\$1.780 millones en **2018**.
2. Telia Company AB (Suecia): US\$965 millones en **2017**.
3. MTS (Rusia): US\$850 millones en **2019**.
4. Siemens (Alemania): US\$800 millones en 2008.
5. VimpelCom (Holanda): US\$795 millones en **2016**.
6. Alstom (Francia): US\$772 millones en 2014.
7. Société Générale S.A. (Francia): US\$585 millones en **2018**.
8. KBR / Halliburton (Estados Unidos): US\$579 millones en 2009.
9. Teva Pharmaceutical (Israel): US\$519 millones en **2016**.
10. Keppel Offshore & Marine Ltd.(Singapur): US\$422 millones en **2017**.

1. Petrobras (**Brasil**): US\$1.780 millones en 2018.
2. Telia Company AB (**Suecia**): US\$965 millones en 2017.
3. MTS (**Rusia**): US\$850 millones en 2019.
4. Siemens (**Alemania**): US\$800 millones en 2008.
5. VimpelCom (**Holanda**): US\$795 millones en 2016.
6. Alstom (**Francia**): US\$772 millones en 2014.
7. Société Générale S.A. (**Francia**): US\$585 millones en 2018.
8. KBR / Halliburton (Estados Unidos): US\$579 millones en 2009.
9. Teva Pharmaceutical (**Israel**): US\$519 millones en 2016.
10. Keppel Offshore & Marine Ltd. (**Singapur**): US\$422 millones en 2017.

FCPA sanciones en Latinoamérica

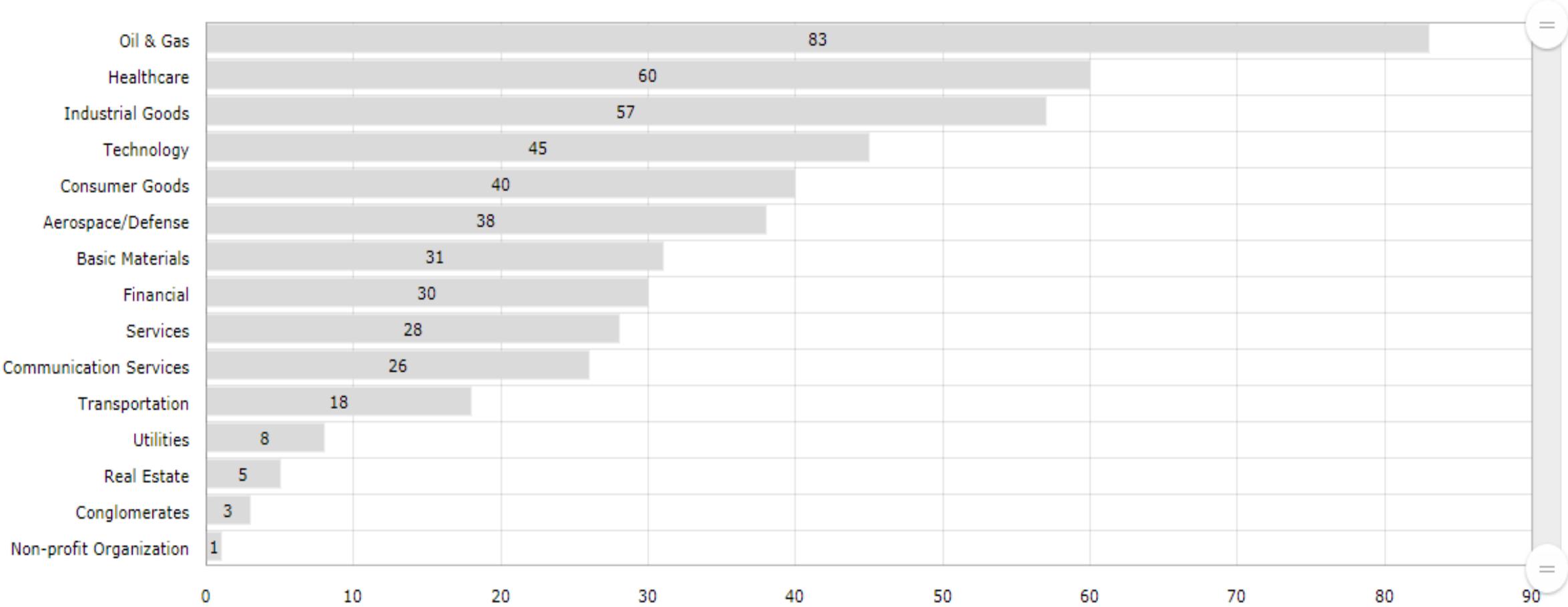
1.	China	56
2.	Nigeria	23
3.	Irak	22
4.	México	21
5.	Indonesia	21
6.	Brasil	20
7.	India	20
8.	Gabón	19
9.	Rusia	15
10.	Argentina	14

- Venezuela 12
- Colombia 6
- Ecuador 5
- Panamá 5
- Republica Dominicana 5
- Costa Rica 4
- Nicaragua 3
- Haití 3
- Honduras 2
- Perú 2
- Chile 2
- España 2
- Guatemala 1
- Bolivia 1

FCPA SEC

- América Latina
- 2010 - Alcatel-Lucent
- Argentina
- 2013- Ralph Lauren Corporation
- 2012 - Biomet
- 2011 - Ball Corporation
- 2011 - Siemens executives
- Brasil
- 2012 - Eli Lilly and Company
- 2012 - Biomet
- México
- 2014 - Hewlett-Packard
- 2012 - Orthofix International
- 2011 - Tyson Foods
- 2010 - ABB Ltd
- Venezuela
- 2010- Joe Summers (Pride International)

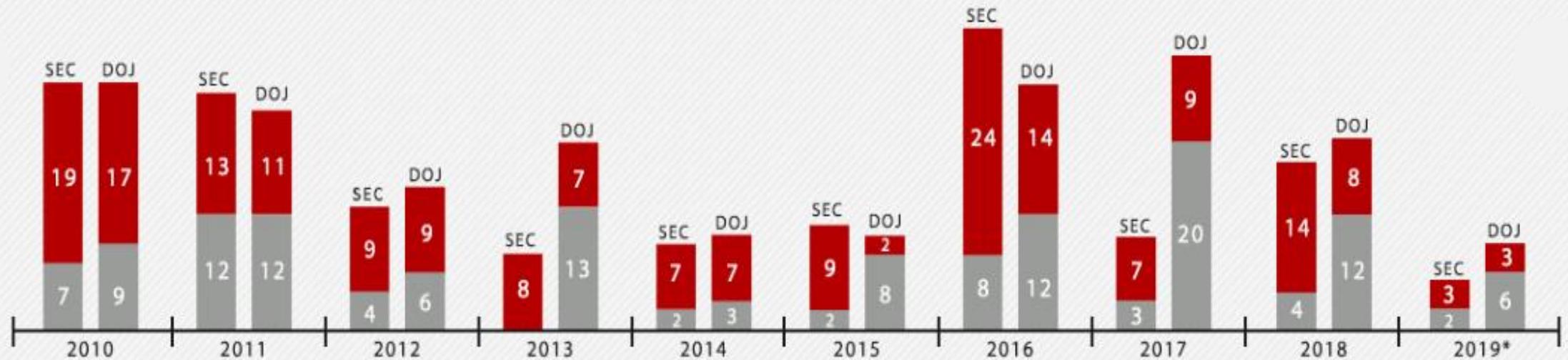
Industry Classifications of FCPA Matters



Description for Industry (FCPA Matters)

This chart identifies the industry classifications of FCPA Matters initiated since the FCPA's enactment. For purposes of this graphic, a single industry is assigned to each Matter based on the industry of the company defendants or other implicated parties at the time of the misconduct. Industry classifications may not comport with NAICS, SIC or classification systems used by other organizations. See [About Us - Datasets](#) for the definition of "FCPA Matter."

ENTITY GROUPS AND INDIVIDUALS CHARGED PER YEAR (FCPA CLAIMS ONLY)



Fuente: StanfordLawSchool - Foreign Corrupt Practices Act Clearinghouse
a collaboration with Sullivan & Cromwell LLP

El lavado de dinero y el delito financiero

- **Whistleblowers** o Denunciantes



The screenshot shows the official website of the SEC Office of the Whistleblower. At the top, there is a navigation bar with the SEC logo and the text "SEC.gov | Search SEC.gov". Below this is a large blue banner with the text "SEC | U. S. SECURITIES AND EXCHANGE COMMISSION Office of the Whistleblower". A horizontal menu below the banner includes links for "Home", "Submit a Tip", "Claim an Award", "Final Orders", "Financial Reporting Fraud", and "Resources".

Latest News

- "The SEC as the Whistleblower's Advocate" by Chair White (04/30/2015) **NEW**
- SEC Announces Award to Whistleblower in First Retaliation Case (04/28/2015)
- SEC Announces Million-Dollar Whistleblower Award to Compliance Officer (04/22/2015)
- SEC: Companies Cannot Stifle Whistleblowers in Confidentiality Agreements (04/01/2015)

Videos

WHAT HAPPENS TO TIPS

Windows Media
Transcript

Welcome to the Office of the Whistleblower

Assistance and information from a whistleblower who knows of possible securities law violations can be among the most powerful weapons in the law enforcement arsenal of the Securities and Exchange Commission. Through their knowledge of the circumstances and individuals involved, whistleblowers can help the Commission identify possible fraud and other violations much earlier than might otherwise have been possible. That allows the Commission to minimize the harm to investors, better preserve the integrity of the United States' capital markets, and more swiftly hold accountable those responsible for unlawful conduct.



Sean McKessy
Chief, Office of the Whistleblower

The Commission is authorized by Congress to provide monetary awards to eligible individuals who come forward with high-quality original information that leads to a Commission enforcement action in which over \$1,000,000 in sanctions is ordered. The range for awards is between 10% and 30% of the money collected.

Estructuras para ocultar al beneficiario real



Lavado de Dinero - Tendencias y Tecnologías

- **Riesgos de lavado de dinero con nuevas tecnologías**
 - **Mundo FinTech /RegTech**
 - **Bancos Digitales y Banca en Línea**
 - **Monedas Virtuales**
- **Facilitado por muchas instituciones e intermediarios, incluidos los agentes de creación de compañías**

FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws

Immediate Release: April 18, 2019

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) has assessed a [civil money penalty](#) against Eric Powers for willfully violating the Bank Secrecy Act's (BSA) registration, program, and reporting requirements. Mr. Powers failed to register as a money services business (MSB), had no written policies or procedures for ensuring compliance with the BSA, and failed to report suspicious transactions and currency transactions.

Mr. Powers operated as a peer-to-peer exchanger of convertible virtual currency. As “money transmitters,” peer-to-peer exchangers are required to comply with the BSA obligations that apply to MSBs, including registering with FinCEN; developing, implementing, and maintaining an effective AML program; filing Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs); and maintaining certain records.

“Obligations under the BSA apply to money transmitters regardless of their size,” said FinCEN Director Kenneth A. Blanco. “It should not come as a surprise that we will take enforcement action based on what we have publicly stated since our March 2013 Guidance—that exchangers of convertible virtual currency, such as Mr. Powers, are money transmitters and must register as MSBs. In fact, there were indications that Mr. Powers specifically was aware of these obligations, but willfully failed to honor them. Such failures put our financial system and national security at risk and jeopardize the safety and well-being of our people, as well as undercut responsible innovation in the financial services space.”

Mr. Powers advertised his intent to purchase and sell bitcoin on the internet. He completed transactions by either physically delivering or receiving currency in person, sending or receiving currency through the mail, or coordinating transactions by wire through a depository institution. Mr. Powers processed numerous suspicious transactions without ever filing a SAR, including doing business related to the illicit darknet marketplace “Silk Road,” as well as servicing customers through The Onion Router (TOR) without taking steps to determine customer identity and whether funds were derived from illegal activity.

Mr. Powers conducted over 200 transactions involving the physical transfer of more than \$10,000 in currency, yet failed to file a single CTR. For instance, Mr. Powers conducted approximately 160 purchases of bitcoin for approximately \$5 million through in-person cash transactions, conducted in public places such as coffee shops, with an individual identified through a bitcoin forum. Of these cash transactions, 150 were in-person and were conducted in separate instances for over \$10,000 during a single business day. Each of these 150 transactions necessitated the filing of a CTR.

Muchas gracias

Gonzalo Vila, CFCS

Director de Latinoamérica
Asociación de Especialistas
Certificados en Delitos
Financieros

Gvila@ACFCS.org

DelitosFinancieros.org

