Abril 2019
Volume 5, Issue 4

Asociación de Oficiales de Cumplimiento de Cooperativas de Puerto Rico

# BSA Newsletter

## Standard Chartered deberá pagar $1,100 millones de multa por violar el régimen de sanciones

10 abril 2019
Gonzalo Vila
Asociación de Especialistas Certificados en Delitos Financieros

**Standard Chartered deberá pagar una multa de $1,100 millones en Estados Unidos y el Reino Unido** por haber provisto servicio a clientes con conexiones iraníes entre 2012 y 2014, violando de ese modo los regímenes de sanciones internacionales que pesan sobre el régimen iraní, según ha destacado el Departamento del Tesoro de los Estados Unidos en un comunicado. Además, también admitieron haber violado sanciones impuestas a Birmania, Cuba, Sudán y Siria, y existe un caso separado que involucra violaciones a sanciones relacionadas con Zimbabue.

StanChart, con sede en Londres, pagará $947 millones al Departamento de Justicia de Estados Unidos, la Oficina del Fiscal del Distrito de Nueva York, el Departamento de Servicios Financieros de Nueva York, la Reserva Federal y la Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro de Estados Unidos. Además, Standard Chartered también fue sancionado con 102 millones de libras por la Autoridad de Conducta Financiera británica (FCA, por sus siglas en inglés).

**Todas las transacciones involucraron personas o países sujetos a programas de sanciones administrados por la OFAC**, dijo el Departamento del Tesoro.

Desde junio de 2009 hasta mayo de 2014, **el banco procesó 9,335 transacciones por un total de unos $440 millones que se canalizaron a través de Estados Unidos. Todas estas transacciones involucraron personas o países sujetos a programas de sanciones integrales administrados por la OFAC** (incluidos Birmania, Cuba, Irán, Sudán y Siria). La mayor parte de las violaciones se refieren a cuentas relacionadas con Irán mantenidas por las sucursales de Emiratos Árabes Unidos en Dubai para varias empresas de comercio general y una empresa petroquímica.

StanChart procesó transacciones en dólares a través de la sucursal de Nueva York u otras instituciones financieras de Estados Unidos a nombre de clientes que enviaron instrucciones de pago

### En esta edición

Procedencia de los fondos .....2

A new wire fraud scam targets your direct deposit info and sends your paycheck to a criminal's account .....3

Hamas está siendo financiado por complejo sistema de tráfico de criptomonedas .....4

Nueva York ve su primera condena por lavado de dinero a través de criptomonedas y de Western Union .....5

Puerto Rico: abrieron un nuevo banco para comerciantes cripto .6

### Puntos de interés

- Los reguladores y las agencias de aplicación de la ley siempre han estado preocupados por el potencial del dinero digital, relativamente anónimo y fácilmente accesible en línea, para financiar el terrorismo.
- Un caso que involucra millones de dólares en pagos a través de Bitcoin y Western Union ha resultado en la primera condena del estado de Nueva York por lavado de dinero en criptomonedas.
- El pagador-receptor es responsable de preguntarle al titular o conductor de la transacción la procedencia de los fondos y el propósito de la transacción monetaria.

# Standard Chartered deberá pagar US$ 1,100 millones de multa por violar el régimen de sanciones cont.

a la sucursal en Dubai pero que **se encontraban físicamente o residían habitualmente en Irán**. El banco también procesó instrucciones bancarias online para residentes de países sancionados.

El pasado 21 de febrero, la firma ya informó de que había previsto $900 millones para hacer frente a las multas.

**Todas las transacciones en Zimbabue involucraron a personas identificadas en la lista SDN de OFAC o partes que eran propiedad del 50% o más, directa o indirectamente, por parte de personas en la Lista SDN en el momento en que ocurrieron las transacciones.**

La entidad británica aceptó "toda la responsabilidad" por las "deficiencias de control" de las que es acusada, aunque atribuyó los hechos a las acciones de dos empleados de corta trayectoria profesional que ya no trabajan en StanChart. La entidad se comprometió además a implementar procedimientos para garantizar el cumplimiento de las sanciones.

El DOJ dijo esta semana que **StanChart acordó devolver (forfeit) $240 millones y pagar una multa de $480 millones** por violar la Ley de Poderes Económicos de Emergencia Internacional. OFAC dijo en el acuerdo global acreditará a StanChart el monto de las sanciones penales pagadas.

El martes, en el Reino Unido, la Autoridad de Conducta Financiera (FCA por sus siglas en inglés) **multó a StanChart con £ 102 millones ($133 millones) por infracciones contra el lavado de dinero** relacionadas con sus sucursales en los Emiratos Árabes Unidos. Entre otras cosas, **la FCA dijo que StanChart abrió una cuenta con $653,000 en efectivo de una maleta "con poca evidencia de que el origen de los fondos haya sido investigado".**

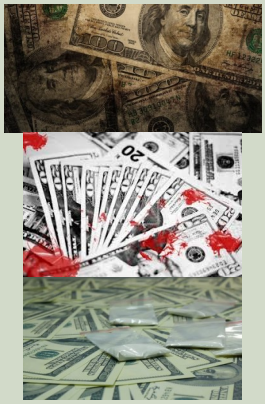
En 2016, Singapur incautó $177 millones de StanChart y otros bancos por fallas ALD relacionadas con 1MDB.

*La FCA dijo que StanChart abrió una cuenta con **$653,000 en efectivo de una maleta** "con poca evidencia de que el origen de los fondos haya sido investigado".*

## Estado de los billetes

Inspeccione el estado de los billetes que recibe.

1. Sucios
2. Polvo extraño
3. Mal olor
4. Manchas, tinta
5. Mutilados



## Procedencia de los fondos

⇒ El pagador-receptor es responsable de preguntarle al titular o conductor de la transacción la procedencia de los fondos y el propósito de la transacción monetaria.

⇒ Si la contestación o negativa del depositante levanta sospecha, la misma deberá ser referida al Departamento de Cumplimiento y Seguridad.

⇒ La pregunta debe ser abarcadora que permita evaluar la contestación y determinar si la misma se ajusta al perfil personal y transaccional del depositante.

| PREGUNTA ABARCADORA | RESPUESTA RELEVANTE |
|---|---|
| ¿De dónde es la procedencia de los fondos? | Los tenía guardados en casa. |
| ¿Producto de qué son los fondos? | Ahorros míos. |
| ¿A qué usted se dedica? | Soy retirado del gobierno. |
| ¿Durante cuánto tiempo los mantuvo guardados? | 5 años |
| ¿Dónde los guardó? | Debajo del "mattress" de la cama |

⇒ Recuerde solicitar evidencia de la procedencia del dinero. En muchas ocasiones el socio trae la evidencia, pero si no se la piden no la entregan.

⇒ El representante de servicios es responsable de preguntar el propósito de apertura de la cuenta y la fuente de depósitos.

# A new wire fraud scam targets your direct deposit info and sends your paycheck to a criminal's account

April 9, 2019
Kate Fazzini@KateFazzini
www.cnbc.com

Around two or three times per month, KVC Health Systems, a midsize nonprofit agency for child welfare based in Kansas City, **receives phishing emails from criminals with the goal of rerouting an employee's paycheck by direct deposit.**

The emails look legitimate at first, as though they come from the CEO, CFO or payroll director.

**The scammer is trying to convince human resources personnel to change the bank account and routing information the employee uses to have paychecks direct-deposited.** Once routed to the criminal's account, the company is on the hook for replacing the stolen funds and the employee faces the inconvenience of a late paycheck.

**It's a new version of wire fraud scams** that have devastated businesses in recent years, and a more focused version of a series of payroll fraud crimes that the IRS warned late last year were on the rise. The fraud is growing, experts said, because it easily bypasses many existing technical controls, and the small sums stolen are inoffensive enough that they can be folded into the cost of doing business.

**The fake emails defy many existing controls for malicious communications**, said Erik Nyberg, director of information technology at KVC. **They are usually well written, cordial and lack the misspellings, grammar mistakes and exclamation points that would trigger many popular email filters that search for spam or phishing attempts.**

"They might just say, 'I need to update my direct deposit information," said Nyberg. "Or they start with, 'Hey, do you have a second?' and if that target person responds, then they go from there." KVC has had a few near misses, Nyberg said, but has not transferred any paychecks to scammers.

**A new scam with a convincing pitch**

The scam has only emerged in the past month, according to Adrien Gendre, chief solutions architect at email security company Vade Secure.

**Many companies "have put processes in place to validate big wire transfers, so now [criminals] want to stay under the radar.** It's a new approach, and every day we have more customers reporting it," he said. Gendre said a dozen Vade companies have reported attempts to change direct deposit information.

The scam does not only bypass some email controls. It also bypasses warnings companies may have already issued to their employees about wire fraud, because scammers aren't asking for money or an invoice transfer — they're simply asking to change a bank account number.

**The fraudsters typically impersonate the company's higher-value employees, like the CFO or CEO**, Nyberg said. **The emails are usually brief, polite and lightly urgent, and often ask HR personnel to change the direct deposit information quickly, "before the next paycheck."**


From: [redacted]
Sent: Thursday, February 28, 2019 9:22 AM
To: [redacted]
Subject: Good morning

[redacted]

Do you have a minute? i need you to help me take care of something important. I need to update my direct deposit for payroll. Can you get it done on your end?

Regards

Others try to discourage the target from calling, by writing "I am going into a meeting now."

An email to employees at KVC Health Systems attempts to start a conversation about direct deposit by convincing the receiver to not call the employee.

**The spoofing doesn't require the criminal to hack into anyone's email account**, as it often does with bigger-ticket wire fraud. **The scammers generate the fake emails with free services like Gmail** -- the scammer simply opens a new Gmail account and fills in the employee's name — which allows them to get around tools meant to detect hacking attempts on employee email, Nyberg explained. Employees may not notice, either because they are working quickly and they don't notice the full email address, or they are working on a mobile device where only the person's name is displayed in the "from" field, he said.

Why would scammers target a nonprofit? Nyberg said he expects that the organization may be attractive in part because of its genial culture: "The nature of our work is helpful, people who are very literally here to help other people. They might also believe that our training isn't as rigorous as a Fortune 500 company," he said.

The emails are meant to be simple and direct, with few misspellings or grammatical errors that would trigger email filters.

Despite the relatively low dollar figure associated with this scam -- thousands of dollars compared with hundreds of thousands in a typical wire scam -- Gendre said it's so cheap to execute that he expects it to become more attractive for criminals.

"They have found a way to automate it, which means you can scale it. You may not make $100,000 in one hit, but you may be able to make 20 hits staying in one company and be able to make your return [on investment]."

**How to combat it**

To fight the threat, Nyberg said the organization has focused on training people on a simple truth: "The CEO is never going to email you out of the blue and ask you for any deposit changes. And **if you have any sliver of a doubt, call the person who is making the request.**"

Gendre said his company has used "natural language processing," which analyzes the language used in incoming emails to test for "urgency," then flagging those emails as potentially suspicious, especially if they come from a new email address.

Nyberg also said they've asked executives to avoid using their personal emails when sending messages to staff, and the company has also tweaked its email filters to pick up on common hallmarks of the request. Companies that see versions of the scam can also report them to the FBI's IC3 tip line.

# Hamas está siendo financiado por complejo sistema de tráfico de criptomonedas

26 abril 2019
israelnoticias.com

Los investigadores dicen que Hamas está utilizando métodos cada vez más complejos para recaudar fondos a través de bitcoin, destacando las dificultades que enfrentan los reguladores para rastrear el financiamiento de la criptomoneda a grupos terroristas.

Las Brigadas Izz el-Deen al-Qassam, con sede en Gaza, proscritas por los Estados Unidos y la Unión Europea, **han pedido a sus partidarios que hagan donaciones utilizando la moneda digital** en una campaña de recaudación de fondos anunciada en línea a fines de enero.

Originalmente, les pedía a los donantes que enviaran bitcoins a una sola dirección digital o billetera.

Sin embargo, según una investigación compartida con Reuters por la firma líder de análisis Elliptic, **en las últimas semanas ha cambiado el mecanismo, y su sitio web genera una nueva billetera digital con cada transacción.**

Esto hace que a las compañías de todo el mundo les resulte más difícil controlar el financiamiento de la criptomoneda del grupo, dijeron los investigadores. Una sola billetera digital se puede marcar en rojo para los intercambios de criptomonedas, en teoría, lo que les permite evitar que los fondos se muevan a través de sus sistemas hacia ese destino.

**Pero una billetera diferente para cada donación hace que este llamado etiquetado sea mucho más complicado**, dijo Elliptic.

Entre el 26 de marzo y el 16 de abril, se envió un bitcoin de 0,6, por un valor aproximado de $3,300, a las carteras creadas en el sitio web, según encontró la investigación de Elliptic. En total, la campaña de recaudación de fondos de cuatro meses ha recaudado alrededor de $7,400, dijo la firma.

Un portavoz de Hamas, que ha gobernado el territorio de Gaza desde 2007, se negó a comentar sobre la investigación de Elliptic.

Tales fondos son una fracción de las decenas de millones de dólares en fondos anuales que Israel y Estados Unidos dicen que Hamas recibe de Irán. Sin embargo, la campaña da una idea de cómo un grupo terrorista se ha ocupado de la recaudación de fondos de bitcoin.

"Todavía están en la fase de experimentación: están probando, viendo cuánto pueden recaudar y si funciona", dijo el cofundador de Elliptic, Tom Robinson.

Irán no ha detallado públicamente su financiamiento de Hamas, aunque no ha negado su apoyo al grupo islamista. Hamas ha dicho que Teherán es el mayor patrocinador de las Brigadas al-Qassam.

Elliptic, con sede en Londres, y el rival estadounidense Chainalysis son las firmas de análisis de cadenas de bloques más prominentes, y han ganado popularidad como guardianes, compañías de criptomoneda y firmas como los fondos de cobertura que buscan herramientas para rastrear monedas digitales.


Respaldados por inversionistas, incluyendo el brazo de capital de riesgo de Banco Santander, los clientes de Elliptic incluyen firmas financieras, reguladores y agencias de cumplimiento de la ley en Europa y los Estados Unidos.

Desde 2016, ha ganado contratos con la Oficina Federal de Investigaciones, el Servicio de Impuestos Internos y la Administración de Control de Drogas, de acuerdo con USAspending.gov, una base de datos de contratos del gobierno de EE. UU.

Los ejemplos de campañas de financiación de criptomonedas por parte de grupos terroristas son raros. Pero la investigación subraya los dolores de cabeza para las empresas en el sector emergente al identificar y eliminar la exposición a monedas digitales potencialmente contaminadas, incluso a medida que las herramientas para rastrear las criptomonedas se vuelven más sofisticadas.

Tratar con el uso ilegal es visto como vital si las criptomonedas van a crecer desde nichos, tokens especulativos a activos abarcados por la corriente principal. **La mayoría de las grandes firmas financieras se han mantenido alejadas de Bitcoin y sus semejantes, con el jefe de lavado de dinero entre las preocupaciones.**

INSTRUCCIONES PASO A PASO

**Hamas es designado como una organización terrorista por los Estados Unidos** y la Unión Europea. Otros, incluido Gran Bretaña, han proscrito solo a las Brigadas al-Qassam.

**Dicha designación significa que**, en los Estados Unidos, por ejemplo, **es ilegal proporcionar dinero o capacitación, y las empresas financieras que controlan los fondos relacionados están obligadas a informarlas a las autoridades.**

Un video de dos minutos en el sitio web de las Brigadas al-Qassam presenta instrucciones paso a paso en árabe sobre cómo los partidarios pueden evitar el sistema financiero tradicional y donar criptomonedas. "¿Cómo apoyar a la resistencia palestina a través de Bitcoin?" se pregunta.

**Con gráficos pulidos y subtítulos en inglés, explica cómo enviar bitcoins** directamente, a través de una oficina de cambio de moneda o mediante un intercambio de criptomonedas. **"Use un dispositivo público para que la billetera no esté vinculada a su dirección IP"**, dice.

Elliptic utiliza una base de datos de información que vincula las direcciones de monedas digitales con los intercambios, los mercados de la darkweb y los grupos prohibidos para rastrear las criptomonedas.

**Se identificaron las carteras creadas por el sitio web mediante el seguimiento de los patrones en sus direcciones únicas.** La firma supervisó estas direcciones e identificó posteriormente múltiples transacciones que enviaban fondos desde las direcciones a un importante intercambio de criptomonedas con sede en Asia.

Trece de las donaciones se hicieron a partir de un intercambio por separado, también

# Hamas está siendo financiado por complejo sistema de tráfico de criptomonedas cont.

de Asia, dijo Elliptic, que se negó a dar más detalles de los intercambios. No estaba claro si el bitcoin se había convertido a las monedas tradicionales, dijo la firma.

REGLAMENTO DE PATCHY

Las finanzas de Hamas están sufriendo. El presidente egipcio Abdel-Fattah Al-Sisi cerró en 2013 cientos de túneles debajo de la frontera entre Gaza y Egipto, impidiendo el contrabando de armas y mercancías que van desde vacas a automóviles, privando a Hamas de los ingresos fiscales.

La financiación de Irán también ha disminuido tras la condena de Hamas por el asesinato de musulmanes sunitas en la guerra civil de Siria, según los analistas.

Bitcoin podría proporcionar un respiro en ese apretón de efectivo.

"Hace que sea difícil para los fondos ser rastreados por las autoridades financieras", dijo Lotem Finkelshtein, jefe de inteligencia de amenazas en Check Point Technologies, una firma de seguridad cibernética en Tel Aviv.

**"No es tan sencillo vincular billeteras a organizaciones".**

La agencia de inteligencia Shin Bet, el ministerio de defensa y el ejército de Israel declinaron hacer comentarios.

El ministro de Finanzas, Moshe Kahlon, quien también es miembro del gabinete de seguridad nacional, dijo a la página web de Ynet TV que este mes no estaba al tanto de la recaudación de fondos.

**Los reguladores y las agencias de aplicación de la ley siempre han estado preocupados por el potencial del dinero digital, relativamente anónimo y fácilmente accesible en línea, para financiar el terrorismo.**

Las normas de criptomoneda varían de un país a otro. El guardián global para el lavado de dinero, consciente de las brechas en las reglas, debe presentar los primeros estándares internacionales sobre la supervisión de la criptomoneda en junio.

Pero con la regulación aún irregular, el riesgo de exposición a monedas contaminadas ha mantenido alejados a la mayoría de los grandes inversores.

Incluso la exposición indirecta a las criptomonedas contaminadas presentaría problemas para las firmas financieras, dijo Kyle Phillips, un abogado de la firma de abogados Fieldfisher.

**"Hay problemas reales con el establecimiento de los beneficiarios reales"**, dijo.

# Nueva York ve su primera condena por lavado de dinero a través de criptomonedas y de Western Union

24 abril 2019
Fuente: Coindesk
Traducción: Mayi Eloísa Martínez
DiarioBitcoin

Un caso que involucra millones de dólares en pagos a través de Bitcoin y Western Union ha resultado en la primera condena del estado de Nueva York por lavado de dinero en criptomonedas.

La Oficina del Fiscal del Distrito de Manhattan anunció que los acusados Callaway Crain y Mark Sánchez, ambos de 35 años de edad, **lavaron $2.8 millones ganados a través de las ventas ilegales de sustancias sometidas a control** (es decir, productos farmacéuticos que no se pueden vender libremente, sin receta médica) realizadas a través de Internet.

**Entre 2013 y 2018, los dos hombres vendieron esteroides y otras drogas, incluida Viagra, en todo Estados Unidos, a través de su sitio web "NextDayGear" y en la Dark Web. Vendieron más de 10,000 paquetes y aceptaron pagos en criptomoneda y moneda fiduciaria a través de Western Union, que les permitió el lavado.**

**Los clientes generalmente pagaban en Bitcoin**, de acuerdo con la Oficina del Fiscal, y los demandados lavaban las ganancias a través de una o más carteras de criptomonedas "intermediarias" para ocultar la fuente de los fondos. Los bitcoins se convirtieron luego a dólares estadounidenses utilizando una plataforma de intercambio de criptomonedas antes de depositar el efectivo en sus cuentas bancarias.

Los pagos de Western Union, por otro lado, se lavaron mediante el uso de identidades falsas o transferencias electrónicas internacionales de receptores fuera de los EE. UU.

La dupla ahora se declaró culpable y se enfrenta a una pena de prisión de 2.5 a 7.5 años, y se espera que la sentencia se lleve a cabo el 12 de julio.

El fiscal de distrito de Manhattan, Cyrus R. Vance, Jr., declaró: "Estos acusados obtuvieron millones de dólares y dinero en efectivo en su sitio web que vendía esteroides falsificados sin receta y otras sustancias controladas a clientes en los 50 estados. Los vendedores de medicamentos en línea que hacen negocios en Nueva York deben tomar nota: ya sea que esté operando a simple vista o en rincones ocultos de la red oscura, mi oficina tiene las habilidades y los recursos para rastrear el dinero. Cierra tu negocio y hazte responsable."

La semana pasada, la misma oficina del fiscal del distrito **también acusó a tres personas por comerciar con drogas y lavar $2.3 millones en criptomoneda usando tarjetas de débito precargadas y retirando efectivo en cajeros automáticos** en Manhattan y Nueva Jersey.

# Puerto Rico: abrieron un nuevo banco para comerciantes cripto

2 abril 2019
Mayi Eloísa Martinez
www.diariobitcoin.com

**El San Juan Mercantile Bank & Trust International (SJMBT, por sus siglas en inglés) es una nueva institución con sede en Puerto Rico que ha abierto sus puertas al negocio cripto y atiende a los comerciantes de criptomoneda.**

El SJMBT aceptó su primer depósito de cliente. Con licencia el mes pasado como entidad financiera internacional (IFE) por la Oficina de la Comisión de Instituciones Financieras (OCIF) de Puerto Rico, el banco es una unidad de Mercantile Global Holdings (MGH), que también es propietaria de San Juan Mercantile Exchange (SJMX), una plataforma de comercio electrónico de grado institucional para activos digitales que pronto será lanzada.

Sobre SJMBT

El banco proporcionará servicios de custodia y liquidación tanto para fiat como para cripto negociados en la bolsa. SJMBT en sí no está asegurado por la Corporación Federal de Seguros de Depósitos (FDIC, por sus siglas en inglés) de los EE UU. Sin embargo, un portavoz comentó que colocará los depósitos de los clientes en los bancos corresponsales que sí lo están.

Del mismo modo, la compañía aclaró que los activos digitales de los clientes se mantendrán en "custodios de activos digitales aprobados".

Mercantile Global Holdings (MGH) comentó que mantener la custodia y el comercio bajo el mismo techo traerá ciertos beneficios. Por ejemplo, el intercambio tendrá en cuenta los saldos de los clientes depositados en el banco al establecer los límites de negociación, lo que le permitirá liquidar las transacciones en tiempo real.

Nick Varelakis, presidente y director de operaciones de SJMB & T, comentó: "A medida que haya más lugares de liquidez a bordo con SJMX para comercializar activos digitales, SJMBT proporcionará servicios críticos, como liquidación en tiempo real y reequilibrio de cuentas, en apoyo de las actividades comerciales de nuestros clientes."

Veteranos de finanzas

El liderazgo de MGH incluye a veteranos de compañías financieras reconocidas.

Varelakis, por ejemplo, es un ex director ejecutivo de JPMorgan Chase para la arquitectura y transformación de negocios, así como un ex director de operaciones del Noble Bank de Puerto Rico, más conocido en el espacio de cifrado por su antigua relación con Tether, la compañía detrás de la stablecoin del mismo nombre.

Además, el banco y la bolsa MGH fueron fundados hace un año por J. Robert Collins Jr., ex presidente de la Bolsa Mercantil de Nueva York (NYMEX, parte del Grupo CME) y fundador de la Bolsa Mercantil de Dubai.

De acuerdo con un comunicado de prensa de MGH, la empresa indicó que la comercialización se iniciará de forma inminente: "Con los nuevos clientes incorporados en el banco, la bolsa puede lanzar operaciones de intercambio, a través de la plataforma SJMX Dark Pool y a través de SJMX Blocks, su lugar de operaciones de venta libre (OTC)."

Finalmente, la banca sigue siendo difícil para los participantes en el mercado de la criptomoneda, ya que **solo unas pocas instituciones están dispuestas a prestar servicios al sector debido a preocupaciones por el lavado de dinero y otros riesgos.**


Asociación de Oficiales de Cumplimiento de Cooperativas de Puerto Rico

**PO Box 95**

**Hatillo, PR 00659**
**Tel. (787) 552-0076**

**(787)898-3260**

**Fax (787) 898-0050**

**Email:**

**info@aoccpr.com**

**Webpage: www.aoccpr.com**