GAFI

INFORME DEL GAFI

Activos virtuales

Indicadores de bandera roja

de Blanqueo de Capitales y

Financiamiento del Terrorismo

Septiembre de 2020

El Grupo de Acción Financiera Internacional (GAFI) es un organismo intergubernamental independiente que desarrolla y promueve políticas para proteger el sistema financiero mundial contra el lavado de dinero, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Las Recomendaciones del GAFI son reconocidas como el estándar global contra el lavado de dinero (ALD) y el financiamiento del terrorismo (CFT).

Para obtener más información sobre el GAFI, visite www.fatf-gafi.org

Este documento y / o cualquier mapa incluido en el mismo se entiende sin perjuicio del estado o soberanía sobre cualquier territorio, de la delimitación de fronteras y límites internacionales y del nombre de cualquier territorio, ciudad o área.

Citando referencia:

GAFI (2020), Indicadores de bandera roja de lavado de dinero y financiamiento del terrorismo asociados con activos virtuales,
GAFI, París, Francia,
www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

Tabla de contenido

Siglas

AEC	Criptomoneda mejorada para el anonimato
CDD	Debida diligencia del cliente
APNFD	Profesiones y negocios no financieros designados
DNS	Registradores de nombres de dominio
GAFI	Grupo de acción financiera
IF	Instituciones financieras
UIF	Unidades de inteligencia financiera
ICO	Oferta inicial de monedas
KYC	Conozca a su cliente
LEA	Las autoridades policiales
ML	Lavado de dinero
STR	Informes de transacciones sospechosas
TF	Financiamiento Térmico
VA / VA	Activos virtuales
VASP	Proveedores de servicios de activos virtuales

Introducción

1. Los activos virtuales [VA] y los servicios relacionados tienen el potencial de estimular innovación y eficiencia, pero sus características distintivas también crean nuevas oportunidades para que los lavadores de dinero, los financistas del terrorismo y otros criminales laven sus ganancias o financien sus actividades ilícitas. La capacidad de realizar transacciones transfronterizas rápidamente no solo permite a los criminales adquirir, mover y almacenar activos digitalmente, a menudo fuera del sistema financiero regulado, sino también ocultar el origen o destino de los fondos y dificultar que las entidades informantes identifiquen actividades sospechosas en de manera oportuna. Estos factores añaden obstáculos a la detección e investigación de actividades delictivas por parte de las autoridades nacionales.

2. En octubre de 2018, el Grupo de Acción Financiera Internacional (GAFI) actualizó sus Estándares para aclarar la aplicación de los Estándares del GAFI a las actividades de VA y a los Proveedores de Servicios de Activos Virtuales (VASP) para, entre otras cosas, ayudar a las jurisdicciones a mitigar el lavado de dinero (LD) y los riesgos de financiamiento del terrorismo (FT) asociados con las actividades de VA y en la protección de la integridad del sistema financiero global. En junio
2019, el GAFI adoptó una Nota Interpretativa a la Recomendación 15 para aclarar aún más la aplicación de los requisitos del GAFI a las actividades u operaciones de VA y VASP, incluso con respecto a la notificación de transacciones sospechosas.

3. El GAFI ha preparado este breve informe sobre indicadores de alerta roja LA / FT asociados con los AV para ayudar a las entidades informantes, incluidas las instituciones financieras (IF), las actividades y profesiones no financieras designadas (APNFD) y los VASP; sin embargo, están categorizados para identificar y reportar actividades potenciales de LD y FT que involucren a AV. Este informe también debería facilitar a las entidades informantes "la aplicación de un enfoque basado en el riesgo a sus requisitos de diligencia debida del cliente (DDC), que requieren saber quiénes son sus clientes y los beneficiarios finales, comprender la naturaleza y el propósito de la relación comercial, y comprender la fuente de fondos.

4. Agencias operativas, incluidas Unidades de Inteligencia Financiera (UIF), ley las autoridades de ejecución (LEA) y los fiscales pueden encontrar este informe como una referencia útil para analizar los informes de transacciones sospechosas (STR) o mejorar la detección, investigación y confiscación de los VA involucrados en el uso indebido.

5. Los reguladores financieros, APNFD y VASP, por otro lado, pueden encontrar estos indicadores útiles al preparar RTS y monitorear el cumplimiento de las entidades con los controles ALD / CFT. Cuando una entidad informante tiene información que indica la existencia de uno o más indicadores sin una lógica de negocio. explicación, pero no presenta un RTS a pesar de la explicación inconsistente del cliente o no busca una aclaración sobre la transacción, las autoridades competentes pueden considerar hacer un seguimiento con la entidad informante teniendo en cuenta el perfil comercial de esta última.

Metodología y fuentes utilizadas en la elaboración de la lista de indicadores de bandera roja

6. Los indicadores de bandera roja incluidos en este informe se basan en más de una cien estudios de caso aportados por jurisdicciones de 2017-2020, los hallazgos de la ¡Informe confidencial del GAFI sobre Financia! Investigaciones que involucran activos virtuales (Junio de 2019] y publicado Definiciones clave de monedas virtuales del informe GAFI y posibles riesgos ALD / CFTR (Junio de 2014], así como información sobre el uso indebido de AV disponible en el dominio público.

Tendencias en el uso de AV para propósitos de LD / FT

La mayoría de los delitos relacionados con VA se centraron en delitos determinantes o de LD. No obstante, los criminales hicieron uso de los AV para evadir sanciones financieras y recaudar fondos para apoyar el terrorismo.

Los tipos de delitos denunciados por las jurisdicciones incluyen LD, venta de sustancias controladas y otros artículos ilegales (incluidas armas de fuego), fraude, evasión fiscal, delitos informáticos (por ejemplo, ataques cibernéticos que resultan en robos), explotación infantil, trata de personas, evasión de sanciones y FT. . Entre estos, el tipo más común de uso indebido es el tráfico ilícito de sustancias controladas, ya sea con ventas realizadas directamente en AV o el uso de AV como técnica de capas de AA. La segunda categoría más común de uso indebido está relacionada con fraudes, estafas y ransomware. Más recientemente, las redes profesionales de ML han comenzado a explotar los AV como uno de sus medios para transferir, recolectar o acumular ganancias.

Fuente: Estudios de caso aportados por jurisdicciones de 2017-2020.

Problemas a tener en cuenta al leer este informe

7. Estos indicadores son específicos de la naturaleza de los AV y sus asociados financieros. actividades, y de ninguna manera son exhaustivas. Las actividades sospechosas que involucran el uso de AV también pueden compartir rasgos similares con las actividades de LD / FT que involucran el uso de moneda fíat u otros tipos de activos. Por lo tanto, las entidades informantes deben considerar los riesgos que plantean sus clientes, productos y operaciones, así como la presencia de indicadores de riesgo convencionales. Los indicadores de bandera roja siempre deben considerarse en contexto.

8. Se pueden desarrollar o desarrollar banderas rojas independientes como las que se enumeran a continuación. combinada con información de agencias operativas, que a su vez puede desarrollarse más a través de una asociación público-privada, en un proceso evolutivo eyelieal que toma en cuenta el riesgo único y el contexto de una jurisdicción, tipo de cliente o la propia entidad informante. La mera presencia de un indicador de bandera roja no es necesariamente una base para una sospecha de LD o FT, pero podría impulsar un mayor monitoreo y examen. En última instancia, un cliente puede proporcionar una explicación para justificar el indicador de bandera roja, los fines comerciales o económicos de una transacción.

9. Al evaluar una actividad sospechosa potencial, las autoridades competentes, las IF, Las APNFD y los VASP deben tener en cuenta que algunos indicadores de alerta pueden ser más fácilmente observables durante el monitoreo transaccional general, mientras que otros pueden ser más fácilmente observables durante las revisiones específicas de la transacción. La observación de uno o más de los indicadores depende de las líneas de negocio, productos o servicios que ofrece una institución o VASP y cómo interactúa con sus clientes. Cuando uno o más indicadores de alerta están presentes y con poca o ninguna indicación de un propósito económico o comercial legítimo, es más probable que la entidad informante desarrolle una sospecha de que está ocurriendo LD o FT.[1] Estos indicadores no deben ser el único determinante de si se debe presentar o no un RTS. Las entidades informantes deben considerar la presentación de un RTS si saben, sospechan o tienen motivos razonables de que se ha cometido LA / FT.

Indicadores de bandera roja

10. Las siguientes secciones contienen una colección de indicadores de bandera roja de sospecha Actividades de VA o posibles intentos de evadir la detección de las fuerzas del orden, identificadas a través de más de cien estudios de casos recopilados desde 2017 en toda la Red Global del GAFI, revisiones de literatura e investigación de código abierto. Como se mencionó anteriormente, la existencia de un solo indicador no necesariamente indica actividad delictiva. A menudo, es la presencia de múltiples indicadores en una transacción sin una explicación comercial lógica lo que genera sospechas de una posible actividad delictiva. La presencia de indicadores debe fomentar un mayor seguimiento, examen y presentación de informes cuando sea apropiado.

Indicadores de bandera roja relacionados con las transacciones

11. Si bien los AV todavía no son ampliamente utilizados por el público, su uso se ha popularizado entre criminái s. El uso de AV para propósitos de LD surgió por primera vez hace más de una década, pero los AV se están volviendo cada vez más comunes para la actividad delictiva de manera más amplia. Este conjunto de indicadores demuestra cómo las señales de alerta tradicionalmente asociadas con transacciones que involucran medios de pago más convencionales siguen siendo relevantes para detectar posibles actividades ilícitas relacionadas con los AV.

Tamaño y frecuencia de las transacciones

- Estructurar transacciones VA (por ejemplo, intercambio o transferencia) en pequeñas cantidades, o en cantidades por debajo de los umbrales de mantenimiento de registros o informes, similar a la estructuración de transacciones en efectivo.
- Realización de múltiples transacciones de alto valor -

  o en una sucesión corta, por ejemplo, dentro de un período de 24 horas;

  o en un patrón escalonado y regular, sin más transacciones registradas durante un largo período posterior, lo que es particularmente común en casos relacionados con ransomware; o

[1] Si bien una serie de indicadores de alerta podrían aplicarse tanto a casos de LD como de FT, por ejemplo, actividades de recaudación de fondos, financiamiento de combatientes terroristas (FTF) y compra de armas (por ejemplo, en la red oscura) utilizando VA, se alienta a los lectores a leer en relación con el Informe confidencial del GAFI sobre la detección del financiamiento del terrorismo: indicadores de riesgo relevantes (junio de 2016) (acceso restringido a los miembros del GAFI) .

o a una cuenta recién creada o previamente inactiva.

- *Transferir VA inmediatamente a múltiples VASP, especialmente a VASP registrados u operados en otra jurisdicción donde:*

  o no hay relación con el lugar donde vive el cliente o realiza sus negocios; o

  o hay una regulación ALD / CFT inexistente o débil.

- *Depositar VA en un intercambio y luego, a menudo, de inmediato:*

  o retirar los VA sin actividad de intercambio adicional a otros VA, que es un paso innecesario e incurre en tarifas de transacción;

  o convertir los AV en múltiples tipos de AV, incurriendo nuevamente en tarifas de transacción, pero sin una explicación comercial lógica (por ejemplo, diversificación de la cartera); o

  o retirar los VA de un VASP inmediatamente a una billetera privada. Esto convierte efectivamente el intercambio / VASP en un mezclador ML.

- *Aceptar fondos sospechosos de ser robados o fraudulentos -*

  o depositar fondos de direcciones de VA que han sido identificadas como tenedoras fondos robados o direcciones de VA vinculadas a los titulares de fondos robados.

Estudio de caso 1. Múltiples transferencias inmediatas de gran cantidad de VA a VASP en el extranjero

Un VASP local presentó RTS luego de sospechas sobre la compra de grandes cantidades de VA por parte de varios individuos y sus subsiguientes transferencias inmediatas a VASP en una jurisdicción extranjera. En varios casos, los individuos compartían la misma dirección residencial; y se accedió a la mayoría de las direcciones de VA desde la misma dirección IP, lo que indica el posible uso de mulas de dinero por parte de los lavadores de dinero profesionales para lavar las ganancias ilícitas.

Además, se organizaron múltiples estratos de los fondos fiduciarios antes de la compra de VA por mulas. Para disfrazar el origen de los fondos, primero se depositó efectivo en varias cuentas en diferentes IF de la jurisdicción. Posteriormente, esos fondos se transfirieron a varias cuentas mantenidas en el nombre de entidades registradas en la jurisdicción. Los pagos electrónicos se realizaron en las cuentas en cantidades más pequeñas. Después de eso, los fondos se transfirieron a otro grupo de cuentas antes de llegar a las cuentas de las mulas en los VASP locales. Los VA se compraron de inmediato y se transfirieron a VASP extranjeros. Más de 150 individuos estuvieron involucrados en este caso, responsables de transferir un total de aproximadamente USD 108 352 900 (o BTC 11,960) a múltiples cuentas de VA mantenidas por dos VASP en el extranjero.

Fuente: Sudáfrica

Estudio de caso 2. Múltiples VA y transferencias múltiples a VASP extranjeros

Un intercambio de VA local informó que aproximadamente KRW 400 millones (EUR301 170) fueron robados a víctimas de phishing y finalmente se intercambiaron por VA como una técnica de estratificación. Lo que desencadenó la denuncia fueron las múltiples transacciones de alto valor transferidas a un VASP extranjero en una sola billetera . Los fondos robados en moneda fíat se cambiaron primero a tres tipos diferentes de VA y luego se depositaron en la billetera de VA del sospechoso en un VASP local. Luego, el sospechoso intentó ocultar la fuente de los fondos transfiriendo fondos 55 veces más a través de 48 cuentas mantenidas en diferentes VASP locales, y luego en una billetera VA diferente ubicada en el extranjero.

Fuente: Corea del Sur

Indicadores de bandera roja relacionados con los patrones de transacción

12. *Similar a la sección anterior, las banderas rojas a continuación ilustran cómo el mal uso de Los AV para propósitos de LD / FT podrían identificarse a través de patrones de transacciones irregulares, inusuales o poco comunes.*

Transacciones relativas a nuevos usuarios

- *Realizar un gran depósito inicial para abrir una nueva relación con un VASP, mientras que el monto financiado es inconsistente con el perfil del cliente.*
- *Realizar un gran depósito inicial para abrir una nueva relación con un VASP y financiar la totalidad del depósito el primer día que se abre, y que el cliente comience a negociar el monto total o una gran parte del monto ese mismo día o al día siguiente. , o si el cliente retira la totalidad del importe al día siguiente. Dado que la mayoría de los VA tienen un límite transaccional para los depósitos, el lavado de grandes cantidades también se puede realizar a través del comercio extrabursátil.* [2]
- *Un nuevo usuario intenta intercambiar todo el saldo de los VA, o retira los VA e intenta enviar el saldo completo fuera de la plataforma.*

Estudio de caso 3. Depósito inicial incompatible con el perfil del cliente

La presencia de los siguientes indicadores sospechosos llevó a una IF (banco) a presentar un RTS a las autoridades, lo que llevó a una investigación de LA:

- *transacciones inconsistentes con el perfil del titular de la cuenta - en los primeros dos días después de la creación de una cuenta personal para un individuo joven, la cuenta recibió depósitos de naturaleza comercial de diferentes personas jurídicas en grandes cantidades;*
- *patrones de transacción: los fondos depositados se transfirieron inmediatamente a las cuentas de varios VASP (en un día) para la compra de VA (Bitcoin);*

[2] *La negociación extrabursátil se refiere a valores que se negocian para empresas que no cotizan en una bolsa formal y a través de un red de agentes de bolsa.*

• *perfil del cliente: el banco conocía a una de las partes que realizaba el pedido como sujeto de un caso de fraude. El banco también proporcionó a las autoridades las direcciones IP utilizadas para los servicios bancarios por Internet.*

Según una investigación, el titular de la cuenta personal parecía ser un mulé de dinero reclutado por crimináis en una plataforma de redes sociales para ayudar a recibir pagos reclamados por bienes vendidos en línea. Sin embargo, esos fondos parecían haber sido depositados por otras empresas víctimas y no eran pagos por bienes. Los fondos depositados se transfirieron inmediatamente de la cuenta bancaria personal a través de varios pagos divididos a otra cuenta de una sociedad anónima en la República Checa, y se cambiaron a VA (Bitcoin) en varios VASP locales. Estos VASP se retiraron inmediatamente de la cuenta. Además de presentar un RTS, el banco también suspendió las transferencias sospechosas, lo que hizo posible la posterior incautación de fondos.

El VASP local también notó irregularidades en los fondos recibidos y brindó información útil para ayudar en la investigación. La información incluía: circunstancias en las que se compraron los VA; transacción y otra información de DDC como la dirección de la billetera, copia del documento de identificación mal usado para la compra y nombre del supuesto comprador. Estos permitieron a las autoridades solicitar información adicional a los bancos (por ejemplo, extractos bancarios).

Fuente: República Checa

Transacciones relativas a todos los usuarios

- *Transacciones que involucran el uso de múltiples VA o cuentas múltiples, sin una explicación comercial lógica.*
- *Hacer transferencias frecuentes en un cierto período de tiempo (por ejemplo, un día, una semana, un mes, etc.) a la misma cuenta de VA -*

  o por más de una persona;

  o desde la misma dirección IP por una o más personas; o o en

  relación con grandes cantidades.
- *Transacciones entrantes de muchas billeteras no relacionadas en cantidades relativamente pequeñas (acumulación de fondos) con transferencia posterior a otra billetera o cambio completo por moneda fiduciaria. Tales transacciones de varias cuentas de acumulación relacionadas pueden usar inicialmente VA en lugar de moneda fiduciaria.*
- *Realizar un cambio de moneda VA-fiat con una pérdida potencial (por ejemplo, cuando el valor de VA fluctúa, o independientemente de las comisiones anormalmente altas en comparación con los estándares de la industria, y especialmente cuando las transacciones no tienen una explicación comercial lógica).*
- *Convertir una gran cantidad de moneda fiduciaria en VA, o una gran cantidad de un tipo de VA en otros tipos de VA, sin una explicación comercial lógica.*

Estudio de caso 4. Transferencias realizadas en un tiempo recurrente

Una IF (firma de valores) local presentó un STR sobre pagos no autorizados entre las cuentas de VA de su corredor y un ciudadano extranjero. La firma de valores informó de la actividad después de determinar que el ciudadano extranjero tenía la intención de realizar transferencias por un total de USD 4,8 millones (dos transacciones separadas que ocurrió con seis minutos de diferencia el mismo día), y presentó una solicitud al corredor para una cuenta comercial al siguiente día hábil. La billetera no estaba alojada en las Islas Caimán. El informe del STR condujo a un intercambio de información exitoso con UIF extranjeras y la devolución exitosa de la mayoría de los fondos a la víctima, ya que la plataforma en línea en una jurisdicción extranjera había podido congelar la cuenta del sospechoso antes de que se completara el delito.

Fuente: Islas Caimán

Indicadores de bandera roja relacionados con el anonimato

13. *Este conjunto de indicadores se basa en las características inherentes y vulnerabilidades asociadas con la tecnología subyacente de los AV. Las diversas características tecnológicas a continuación aumentan el anonimato y agregan obstáculos a la detección de actividades delictivas por parte de las LEA. Estos factores hacen que las VA sean atractivas para los criminales que buscan disfrazar o almacenar sus fondos. Sin embargo, la mera presencia de estas características en una actividad no sugiere automáticamente una transacción ilícita. Por ejemplo, el uso de una billetera de hardware o de papel puede ser legítimo como una forma de proteger a los asistentes virtuales contra robos. Nuevamente, la presencia de estos indicadores debe considerarse en el contexto de otras características sobre el cliente y la relación, o una explicación comercial lógica.*

- *Transacciones de un cliente que involucran más de un tipo de VA, a pesar de las tarifas de transacción adicionales, y especialmente aquellos VA que brindan un mayor anonimato, como las criptomonedas con anonimato mejorado (AEC) o las monedas de privacidad.*

- *Mover un VA que opera en una cadena de bloques pública y transparente, como Bitcoin, a un intercambio centralizado y luego intercambiarlo inmediatamente por una moneda AEC o de privacidad.*
- *Clientes que operan como un VASP no registrado / sin licencia en sitios web de intercambio peer-to-peer (P2P), particularmente cuando existe la preocupación de que los clientes manejen una gran cantidad de transferencias de VA en nombre de su cliente y cobren tarifas más altas a sus clientes que los servicios de transmisión. ofrecido por otros intercambios. Uso de cuentas bancarias para facilitar estas transacciones P2P.*
- *Actividad transaccional anormal (nivel y volumen) de VA cobrada en intercambios de billeteras asociadas a la plataforma P2P sin una explicación comercial lógica.*
- *VA transferidos hacia o desde billeteras que muestran patrones previos de actividad asociados con el uso de VASP que operan servicios de mezcla o caída o plataformas P2P.*

- *T ransacciones que hacen uso de servicios de mezcla y rotación, lo que sugiere la intención de ocultar el flujo de fondos ilícitos entre direcciones de billeteras conocidas y mercados de redes oscuras.*
- *Fondos depositados o retirados de una dirección o billetera de VA con enlaces de exposición directa e indirecta a fuentes sospechosas conocidas, incluidos los mercados de redes oscuras, servicios de mezcla / volteo, sitios de apuestas cuestionables, actividades ilegales (por ejemplo, ransomware) y / o informes de robo.*
- *El uso de carteras de hardware o de papel descentralizadas / no alojadas para transportar VA a través de las fronteras.*
- *Usuarios que ingresan a la plataforma VASP habiendo registrado sus nombres de dominio de Internet a través de proxies o utilizando registradores de nombres de dominio (DNS) que suprimen o censuran a los titulares de los nombres de dominio.*
- *Usuarios que ingresan a la plataforma VASP utilizando una dirección IP asociada con una darknet u otro software similar que permite la comunicación anónima, incluidos correos electrónicos cifrados y VPN. Transacciones entre socios que utilizan varios medios de comunicación anónimos encriptados (por ejemplo, foros, chats, aplicaciones móviles, juegos en línea, etc.) en lugar de un VASP.*
- *Una gran cantidad de billeteras VA aparentemente no relacionadas controladas desde la misma dirección IP (o dirección MAC), lo que puede implicar el uso de billeteras shell registradas para diferentes usuarios para ocultar su relación entre ellos.*
- *Uso de AV cuyo diseño no está adecuadamente documentado o que están vinculados a posibles fraudes u otras herramientas destinadas a implementar esquemas fraudulentos, como los esquemas Ponzi.*
- *Recibir fondos o enviar fondos a los VASP cuyos procesos de DDC o conozca a su cliente (KYC) son demostrablemente débiles o inexistentes.*
- *Uso de cajeros automáticos / quioscos de VA -*

  o a pesar de las tarifas de transacción más elevadas e incluidas las que suelen utilizar mulas o víctimas de estafas; o

  o en lugares de alto riesgo donde ocurren más actividades delictivas.

  Un solo uso de un cajero automático / quiosco no es suficiente en sí mismo para constituir una señal de alerta, pero lo sería si se combinara con la máquina en un área de alto riesgo o si se usara para transacciones pequeñas repetidas (u otros factores adicionales).).

Estudio de caso 5. Uso de la dirección IP asociada con Darknet Marketplace - Bahía Alpha

AlphaBay, el mercado criminal de redes oscuras más grande desmantelado por las autoridades en 2017, fue utilizado por cientos de miles de personas para comprar y vender drogas ilegales, documentos de identificación y dispositivos de acceso robados y fraudulentos, productos falsificados, malware y otras herramientas de piratería informática, armas de fuego y productos químicos tóxicos durante un período de dos años. El sitio operaba como un servicio oculto en la red TOR para ocultar las ubicaciones de sus servidores subyacentes, así como las identidades de sus administradores, moderadores y usuarios. Los proveedores de AlphaBay utilizaron varios tipos diferentes de VA, y tenían aproximadamente 200000 usuarios, 40000 proveedores, 250000 listados y facilitaron más de mil millones de dólares en transacciones de VA entre 2015 y 2017.

En julio de 2017, el gobierno de los EE. UU., Con la ayuda de contrapartes extranjeras, desmanteló los servidores que alojaban el mercado de AlphaBay, arrestó al administrador y, de conformidad con una orden de incautación emitida en el Distrito Este de California, confiscó los activos físicos y virtuales del mercado. sí mismo, y aquellos que representaron el producto ilegal de la empresa criminal AlphaBay. Los agentes federales obtuvieron las órdenes después de rastrear las transacciones de VA que se originaron en AlphaBay a otras cuentas de VA e identificaron cuentas bancarias y otros activos tangibles controlados por el supuesto administrador.

Fuente: Estados Unidos.

Estudio de caso 6. Uso de mezcla y volteo - Helix

Un VASP basado en darknet, Helix, proporcionó un servicio de mezcla o rotación que ayudó a los clientes a ocultar la fuente o los propietarios de los VA por una tarifa durante un período de tres años. Helix supuestamente transfirió más de 350.000 Bitcoin, con un valor al momento de la transmisión de más de USD 300 millones. El operador anunció específicamente el servicio como una forma de ocultar transacciones en la red oscura a las fuerzas del orden. En febrero de 2020, se presentaron cargos penales que incluían conspiración de LD y operación de un negocio de transmisión de dinero sin licencia contra una persona que operaba Helix.

Helix se asoció con AlphaBay, el mercado de la darknet, hasta que la policía lo incautó en 2017.

Fuente: Estados Unidos.

Estudio de caso 7. Uso de billetera descentralizada

Este caso demuestra cómo los criminales hacen uso de la billetera descentralizada para ofuscar el origen de los fondos ilícitos generados por las actividades del tráfico ilícito de drogas. En este caso, los criminái s realizaron una gran cantidad de venta de drogas en Internet y buscaron el pago no solo en moneda fíat sino también en forma de VA (Bitcoin, códigos EX, cheques EXMO).

Los fondos ilícitos recibidos en moneda fíat se convirtieron a VA con la ayuda de una cuenta anónima en una plataforma de comercio Blockchain en línea. Dichos fondos, en forma de VA, se volvieron a convertir en moneda fíat a través de un intercambiador, antes de ser transferidos nuevamente a las cuentas de tarjetas bancarias personales de los criminales. En cuanto a los fondos ilícitos recibidos en forma de VA, primero se transfirieron a billeteras Bitcoin descentralizadas en poder de los criminales involucrados, antes de ser transferidos a otras billeteras Bitcoin en diferentes intercambios. Esto aumenta la dificultad de rastrear y rastrear los fondos. Del mismo modo, los fondos blanqueados (en VA) se volvieron a convertir en fíat antes de ser acreditados en las cuentas de tarjetas bancarias criminales. El criminal fue declarado culpable y condenado a siete años de prisión y una multa penal después del juicio.

Fuente: Federación de Rusia.

Indicadores de bandera roja sobre remitentes o destinatarios

14. Este conjunto de indicadores es relevante para el perfil y comportamiento inusual de cualquiera el remitente o el destinatario de las transacciones ilícitas.

Irregularidades observadas durante la creación de la cuenta

- *Creación de cuentas separadas con diferentes nombres para eludir las restricciones sobre los límites comerciales o de retiro impuestos por los VASP.*
- *Transacciones iniciadas desde direcciones IP no confiables, direcciones IP de jurisdicciones sancionadas o direcciones IP previamente marcadas como sospechosas.*
- *Intentar abrir una cuenta con frecuencia dentro del mismo VASP desde la misma dirección IP.*
- *Con respecto a los comerciantes / usuarios corporativos, sus registros de dominio de Internet se encuentran en una jurisdicción diferente a la jurisdicción de su establecimiento o en una jurisdicción con un proceso débil para el registro de dominio.*

Irregularidades observadas durante el proceso de DDC

- *Información KYC incompleta o insuficiente, o un cliente rechaza solicitudes de documentos KYC o pregunta sobre la fuente de los fondos.*
- *El remitente / destinatario no tiene conocimientos o proporciona información inexacta sobre la transacción, el origen de los fondos o la relación con la contraparte.*
- *El cliente ha proporcionado documentos falsificados o ha editado fotografías y / o documentos de identificación como parte del proceso de incorporación.*

Estudio de caso 8. El cliente se niega a proporcionar información sobre la fuente de fondos

Un FI (banco) presentó un RTS relativo a una cuenta de una empresa local que tenía fondos generados por la venta de cupones que se pueden intercambiar con un producto (bioplásticos en este caso). Los fondos fueron depositados por personas físicas y jurídicas, algunos originalmente en VA. A pesar de nuevas consultas del banco, los representantes del titular de la cuenta no proporcionaron información sobre el origen de los fondos. Un análisis posterior de las autoridades indicó que los fondos enviados por la empresa mostraban vínculos con sujetos vinculados al crimen organizado y con fondos recibidos de un proyecto fraudulento.

Fuente: Italia

Perfil

- *Un cliente proporciona identificación o credenciales de cuenta (por ejemplo, una dirección IP no estándar o cookies flash) compartidas por otra cuenta.*
- *Surgen discrepancias entre las direcciones IP asociadas con el perfil del cliente y las direcciones IP desde las que se inician las transacciones.*
- *La dirección de VA de un cliente aparece en foros públicos asociados con actividades ilegales.*
- *Un cliente es conocido a través de información públicamente disponible para las fuerzas del orden debido a una asociación criminal previa.*

Estudio de caso 9. El perfil del cliente no coincide con el de alto valor habitual

Negociación de VA

Un VASP (intercambiador) y una FI (instituto de pagos) presentaron ROS ante la UIF sobre un alto valor de negociación de VA que comenzó cuando se abrió la cuenta en el intercambiador. Específicamente, el titular de la cuenta había estado realizando varias transacciones de compraventa de VA por más de 180 000 EUR, que no coincidían con el perfil del titular de la cuenta (incluida la ocupación y el salario).

El análisis encontró que los VA se utilizaron posteriormente para (i) transacciones en un mercado de redes oscuras; (ii) apuestas en línea; (ni) transacciones con VASP que no tenían controles ALD / CFT adecuados o que estaban bajo investigaciones previas de LD que involucraban millones de dólares; (iv) operaciones en plataformas que ofrecían transacciones peer-to-peer de VA; y (v) "mezclar". El titular de la cuenta también había hecho uso de una variedad de medios diferentes (por ejemplo, transferencia de dinero, banca en línea y tarjetas prepagas) para sacar una cantidad constante de fondos de su cuenta en el mismo período de tiempo. Los fondos recibidos por el titular de la cuenta parecían provenir de una red de individuos que compraron VA (Bitcoin) en efectivo y estaban ubicados en diferentes jurisdicciones en Asia y Europa (incluida Italia).

tanto a través de transferencia de dinero como del sistema bancario. También recibió fondos en sus tarjetas prepagas de sujetos en África y Medio Oriente, quienes a su vez recolectaron fondos de conciudadanos residentes en Italia y en el extranjero. Estos fondos se utilizaron luego para transferencias transfronterizas y juegos de azar en línea, y se retiraron en efectivo de los cajeros automáticos en Italia.

Fuente: Italia

Perfil de posibles víctimas de estafa o mulé de dinero

- *El remitente no parece estar familiarizado con la tecnología VA o las soluciones de billetera de custodia en línea. Estas personas podrían ser mulas de dinero reclutadas por lavadores de dinero profesionales, o víctimas de estafas convertidas en mulas que son engañadas para transferir ganancias ilícitas sin conocimiento de sus orígenes.*
- *Un cliente significativamente mayor que la edad promedio de los usuarios de la plataforma abre una cuenta y participa en un gran número de transacciones, lo que sugiere su papel potencial como mulé de dinero de VA o víctima de explotación financiera eider.*
- *Un cliente es una persona financieramente vulnerable, que a menudo es utilizada por los traficantes de drogas para ayudarlos en su negocio de tráfico.*
- *El cliente compra grandes cantidades de VA que no están respaldadas por la riqueza disponible o que no son consistentes con su perfil financiero histórico, lo que puede indicar lavado de dinero, mulé de dinero o víctima de estafa.*

Estudio de caso 10. Víctimas de estafa convertidas en mulas

En estas estafas de inversión, los ciudadanos extranjeros se pusieron en contacto con los jubilados y, en general, las personas mayores mediante llamadas telefónicas directas, correos electrónicos o redes sociales, y les ofrecieron oportunidades de inversión en Bitcoin u otros VA con la promesa de generar enormes ganancias debido a la creciente popularidad en los VA y sus aumento de precio. La inversión inicial en pequeñas cantidades (en muchos casos no más de 250 euros) se realizó desde la cuenta bancaria de las víctimas, tarjeta de crédito o por otros medios a varios servicios de pago y luego terminó en manos de los criminales. instruido para cambiar moneda fíat a Bitcoin usando un cajero automático VA y enviar los fondos a una dirección especificada por los criminales.

Las víctimas no eran muy hábiles tecnológicamente y, en general, no entendían la tecnología VA o en qué estaban invirtiendo realmente. Crimináis también les pidió a las víctimas que instalaran una aplicación de escritorio remoto en su dispositivo para que pudieran ayudar a transferir los fondos correctamente a cuentas específicas. Esto comprometió los dispositivos de las víctimas para que los criminales pudieran realizar transferencias de dinero no autorizadas sin que la víctima se enterara hasta que notara que faltaba dinero en la cuenta. En algunos casos, los crimináis también fabricaron artículos en los que afirmaban que celebridades famosas o empresarios o presentadores de noticias adinerados estaban promoviendo las inversiones de VA, dando así a las víctimas un sentido de confianza y legitimidad a las "inversiones".

Fuente: Finlandia

Otro comportamiento inusual

- *Un cliente cambia con frecuencia su información de identificación, incluidas las direcciones de correo electrónico, las direcciones IP o la información financiera, lo que también puede indicar la toma de control de la cuenta de un cliente.*
- *Un cliente intenta ingresar a uno o más VASP desde diferentes direcciones IP con frecuencia durante el transcurso de un día.*
- *El uso de lenguaje en los campos de mensajes de VA indicativos de las transacciones que se llevan a cabo en apoyo de actividades ilícitas o en la compra de bienes ilícitos, como drogas o información de tarjetas de crédito robadas.*
- *Un cliente realiza transacciones repetidamente con un subconjunto de individuos con ganancias o pérdidas significativas. Esto podría indicar una posible toma de control de la cuenta y un intento de extracción de los saldos de las víctimas a través del comercio, o un esquema de LD para ofuscar el flujo de fondos con una infraestructura VASP.*

Indicadores de bandera roja en la fuente de fondos o riqueza

15. *Como lo demuestran los casos presentados por las jurisdicciones, el uso indebido de los AV a menudo se relaciona con actividades delictivas, como el tráfico ilícito de estupefacientes y sustancias psicotrópicas, el fraude, el robo y la extorsión (incluidos los delitos cibernéticos). A continuación, se muestran señales de alerta comunes relacionadas con la fuente de fondos o riqueza vinculada a tales actividades delictivas:*

- *Transacciones con direcciones de VA o tarjetas bancarias que están conectadas a esquemas conocidos de fraude, extorsión o ransomware, direcciones autorizadas, mercados de redes oscuras u otros sitios web ilícitos.*
- *Transacciones de VA originadas o destinadas a servicios de juegos de azar en línea.*
- *El uso de una o varias tarjetas de crédito y / o débito que están vinculadas a una billetera VA para retirar grandes cantidades de moneda fíat (cripto-a-plástico), o los fondos para comprar VA se obtienen de depósitos en efectivo en tarjetas de crédito.*
- *Los depósitos en una cuenta o una dirección de VA son significativamente más altos de lo normal con una fuente de fondos desconocida, seguidos de la conversión a moneda fiduciaria, lo que puede indicar el robo de fondos.*
- *Falta de transparencia o información insuficiente sobre el origen y los propietarios de los fondos, como los que implican el uso de empresas ficticias o los fondos colocados en una Oferta Inicial de Monedas [ICO] donde los datos personales de los inversores pueden no estar disponibles o las transacciones entrantes en línea. sistema de pagos a través de tarjetas de crédito / prepago seguido de retiro instantáneo.*
- *Los fondos de un cliente que se obtienen directamente de servicios de mezcla de terceros o vasos de billetera.*
- *La mayor parte de la fuente de riqueza de un cliente se deriva de inversiones en VA, ICO o ICO fraudulentas, etc.*
- *La fuente de riqueza de un cliente se extrae desproporcionadamente de los AV que se originan en otros VASP que carecen de controles ALD / CFT.*

Estudio de caso 11. Uso de empresas ficticias: Deep Dot Web

En mayo de 2019, las LEA de EE. UU. Incautaron un sitio web, DeepDotWeb (DDW), de conformidad con una orden judicial. Los presuntos propietarios y operadores de DDW fueron acusados de una conspiración de ML relacionada con millones de dólares en sobornos que recibieron por remitir a individuos a los mercados de la darknet desde el sitio web de DDW. A través de enlaces de referencia, los presuntos propietarios y operadores de DDW recibieron pagos de sobornos, que representan comisiones sobre las ganancias de la compra de bienes ilegales, como fentanilo y heroína, realizadas por individuos referidos a un mercado de la red oscura desde el sitio de DDW.

Estos pagos de sobornos se realizaron en VA y se ingresaron en una billetera Bitcoin controlada por DDW. Para ocultar y disfrazar la naturaleza y el origen de los ingresos ilegales, que totalizaron más de USD 15 millones, los propietarios y operadores transfirieron sus pagos de sobornos ilegales de su billetera DDW Bitcoin a otras billeteras Bitcoin, así como a cuentas bancarias que controlaban en el nombres de empresas pantalla. Los acusados utilizaron estas empresas fantasma para trasladar sus ganancias ilícitas y realizar otras actividades relacionadas con DDW. Durante un período de cinco años, el sitio web recibió aproximadamente 8 155 Bitcoin en pagos de sobornos de los mercados de la darknet, por un valor aproximado de USD 8 millones, ajustado por el valor comercial de Bitcoin en el momento de cada transacción. El Bitcoin fue transferido a la billetera Bitcoin de DDW, controlada por los acusados, en una serie de más de 40 000 depósitos, y posteriormente fue retirado a varios destinos en más de 2 700 transacciones. El valor de Bitcoin en el momento de los retiros de la billetera DDW Bitcoin equivalía a aproximadamente USD 15 millones.

Fuente: Estados Unidos.

Estudio de caso 12. Uso de múltiples intercambios VA, identificación falsa documentos para CDD y tarjetas prepago

Los acusados en este asunto supuestamente operaban un esquema de LD en relación con los ciberdelincuentes que piratearon un intercambio de VA y robaron VA por valor de 250 millones de dólares. Los dos acusados supuestamente lavaron alrededor de USD 91 millones en los AV robados, así como USD 9,5 millones de otro robo cibernético.

Los VA robados luego se enrutaron a través de cientos de transacciones VA automatizadas y múltiples intercambios VA. Los lavadores utilizaron fotografías manipuladas y documentos de identificación falsificados en algunos casos para eludir los procedimientos de KYC en los intercambios de VA. En última instancia, unos 35 millones de dólares de los fondos ilícitos se transfirieron a cuentas bancarias extranjeras y también se utilizaron para comprar tarjetas prepagas, que podrían canjearse por VA. Los acusados operaban a través de cuentas independientes y vinculadas y proporcionaban servicios de transmisión de VA, como

convertir VA en moneda fiduciaria, a los clientes por una tarifa. Los acusados también realizaron negocios en los EE. UU. Pero en ningún momento se registraron en la Red de Ejecución de Delitos Financieros (FinCEN).

Fuente: Estados Unidos.

Indicadores de bandera roja relacionados con riesgos geográficos

dieciséis. Este conjunto de indicadores enfatiza cómo criminái, al mover sus ilícitos fondos, han aprovechado las distintas etapas de implementación por parte de las jurisdicciones de los Estándares revisados del GAFI sobre VA y VASP.[3] Con base en los casos reportados por las jurisdicciones, los criminales han explotado las brechas en los regímenes ALD / CFT en VA y VASP al mover sus fondos ilícitos a VASP domiciliados u operados en jurisdicciones con regulaciones mínimas o inexistentes ALD / CFT sobre VA y VASP. Es posible que estas jurisdicciones no tengan un régimen de registro / licencia, o no hayan extendido los requisitos de STR para cubrir los AV y VASP, o es posible que no hayan introducido el espectro completo de medidas preventivas como lo requieren los Estándares del GAFI. Si bien este informe no busca identificar una lista de jurisdicciones de "alto riesgo", se invita a las entidades informantes a tener en cuenta los siguientes indicadores al considerar los riesgos geográficos. Estos riesgos están asociados con las jurisdicciones de origen, destino y tránsito de una transacción. También son relevantes para los riesgos asociados con el originador de una transacción y el beneficiario de fondos que pueden estar vinculados a una jurisdicción de alto riesgo. Además, pueden ser aplicables a la nacionalidad, residencia o lugar de trabajo del cliente.

- *Los fondos del cliente se originan o se envían a un intercambio que no está registrado en la jurisdicción donde se encuentra el cliente o el intercambio.*
- *El cliente utiliza un intercambio de VA o un MVTS ubicado en el extranjero en una jurisdicción de alto riesgo que carece o se sabe que tiene regulaciones ALD / CFT inadecuadas para las entidades de VA, incluidas medidas inadecuadas de CDD o KYC.*
- *El cliente envía fondos a los VASP que operan en jurisdicciones que no tienen regulación de VA o que no han implementado controles ALD / CFT.*
- *El cliente establece oficinas o las traslada a jurisdicciones que no tienen regulación o no han implementado regulaciones que rigen los AV, o establece nuevas oficinas en jurisdicciones donde no existe una razón comercial clara para hacerlo.*

[3] *En julio de 2020, el GAFI publicó un Revisión de 12 meses de las Normas revisadas del GAFI sobre activos virtuales y servicio de activos virtuales Proveedores . La Sección 2 del Informe cubre el progreso de la implementación de las Normas revisadas desde junio de 2019.*

Estudio de caso 13. Distribuidor de Bitcoin opera transmisión de dinero sin licencia empresas (elementos transfronterizos)

En abril de 2019, el acusado recibió una sentencia de dos años de prisión por operar un negocio de transmisión de dinero sin licencia después de vender cientos de miles de dólares de VA (Bitcoin) a más de mil clientes en los EE. UU. USD 823 357 en utilidades.

El acusado anunció sus servicios en sitios web para usuarios de VA, y se reunió con algunos clientes en persona para aceptar efectivo a cambio de VA. Otros clientes le pagaron a través de cajeros automáticos a nivel nacional o servicios de transmisión de dinero. El acusado recibió una prima del cinco por ciento sobre el tipo de cambio vigente por sus servicios. Primero adquirió Bitcoin a través de un intercambio de EE. UU., Pero una vez que sus actividades despertaron sospechas y se cerró su cuenta, el acusado cambió a un intercambio en Asia. Utilizando ese intercambio, el acusado compró USD 3,29 millones en Bitcoin, en cientos de transacciones separadas, entre marzo de 2015 y abril de 2017. El acusado también admitió que cambió su efectivo estadounidense, que mantenía en otra jurisdicción fronteriza con EE.UU., con un precioso distribuidor de metáis, y que entre finales de 2016 y principios de 2018,

Fuente: Estados Unidos.

VASP traslada su operación a una jurisdicción que tiene un ALD / CFT inadecuado regulaciones

Antes de la implementación de una política para prohibir la operación de VASP en la Jurisdicción A en Asia en 2017, un VASP (intercambio) establecido en la Jurisdicción A transfirió su operación a la Jurisdicción B en la misma región. En 2018, la Jurisdicción B intensificó su régimen legal ALD / CFT sobre VA luego de importantes hackeos de algunos VASP (intercambios) importantes. En marzo de 2018, el VASP anunció sus intenciones de trasladar su sede a la Jurisdicción C en Europa (una jurisdicción que aún no había introducido un régimen integral ALD / CFT en relación con los VA y VASP en ese momento). Posteriormente, en noviembre de 2018, la Jurisdicción C introdujo ciertas regulaciones sobre los VASP, y en febrero de 2020, confirmó que no se otorgó autorización al VASP correspondiente para operar.

Fuente: dominio público

Conclusión

17. Este informe se basa en una amplia aportación de los miembros del GAFI en todo el mundo red, y busca proporcionar una herramienta práctica tanto para el sector público como para el privado en la identificación, detección y, en última instancia, prevención de actividades delictivas, LD y FT que involucren a AV.

18. La Los indicadores incluidos en este Informe son específicos de las vulnerabilidades caracteristicas inherentes y asociadas con los AV. No son exhaustivos en todas las situaciones. ñor aplicable Los indicadores son a menudo solo uno de los muchos elementos de un contribuyendo a panorama general más amplio del riesgo potencial de LA o FT y es importante que los indicadores (o cualquier indicador individual) no se consideren de forma aislada, sino que se contextualicen con la información obtenida de las autoridades pertinentes.

19. Un enfoque basado en el riesgo implementado con un diálogo bidireccional regular y dinámico entre los sectores público y privado sin duda mejoraría la efectividad de este Informe. Por lo tanto, se alienta a las autoridades competentes a difundir este Informe a las entidades informantes y a llevar a cabo sesiones de participación y sensibilización con ellas para promover su comprensión de este Informe.

20. Si bien los indicadores identificados evolucionan constantemente, es mejor utilizarlos cuando se aplica otra información contextual de fuentes públicas y policiales nacionales. Las autoridades competentes también pueden proporcionar a los sectores privados los indicadores y la información más relevante para esa jurisdicción. Por ejemplo, utilizar la información de este Informe para preparar sus propios avisos a las entidades informantes relevantes. Sin embargo, este Informe no debe ser utilizado como una herramienta regulatoria para propósitos de cumplimiento y fiscalización, o como una lista de verificación al supervisar las instituciones del sector privado, ya que no todos los indicadores son aplicables a todas las jurisdicciones o todas las instituciones.

Referencias

GAFI (junio de 2014], Informe del GAFI Definiciones de Kev de monedas virtuales y riesgos potenciales ALD / CFT

GAFI (junio de 2019), Orientación del GAFI para un enfoque basado en el riesgo de activos virtuales y proveedores de servicios de activos virtuales

GAFI (junio de 2020), Revisión de 12 meses de los estándares revisados del GAFI - Activos virtuales y VASP

Informes restringidos a miembros del GAFI

GAFI (junio de 2016), Informe confidencial del GAFI sobre la detección del financiamiento del terrorismo: indicadores de riesgo relevantes

GAFI (junio de 2019), Informe confidencial del GAFI sobre investigaciones financieras que involucran Activos

GAFI

www.fatf-gafi.org

Septiembre de 2020

Activos virtuales: indicadores de bandera roja de blanqueo de capitales y financiación del terrorismo

Los activos virtuales y los servicios relacionados tienen el potencial de estimular la innovación y la eficiencia financieras, pero sus características distintivas también crean nuevas oportunidades para que los lavadores de dinero, los financistas del terrorismo y otros criminales laven sus ganancias o financien sus actividades ilícitas.

El GAFI ha preparado este breve informe sobre los indicadores de alerta asociados con los activos virtuales para ayudar a las entidades informantes, incluidas las instituciones financieras, las empresas y profesiones no financieras designadas y los proveedores de servicios de activos virtuales, a identificar e informar sobre posibles actividades de lavado de dinero y financiamiento del terrorismo que involucren activos virtuales.