[Traducción de Cortesía]

Informe del GAFI

Activos Virtuales
Señales de alerta de LD/FT

Activos Virtuales
Señales de alerta de LD/FT

Introducción

1. Los Activos Virtuales (AV) y los servicios relacionados tienen el potencial de estimular la innovación y la eficiencia financiera, pero sus características distintivas también crean nuevas oportunidades para que los lavadores de dinero, los financiadores del terrorismo y otros criminales laven sus ganancias o financien sus actividades ilícitas. La capacidad de realizar operaciones transfronterizas rápidamente no solo permite a los criminales adquirir, mover y almacenar activos digitalmente, a menudo fuera del sistema financiero regulado, pero también disfrazar el origen o destino de los recursos y dificultar que los sujetos obligados identifiquen las actividades sospechosas de manera oportuna. Estos factores añaden obstáculos a la detección e investigación de la actividad criminal por las autoridades nacionales.

2. En octubre de 2018, el GAFI actualizó sus Estándares para aclarar su aplicación a las actividades de AV y a los Proveedores de Servicios de Activos Virtuales (VASP, por sus siglas en inglés) para, entre otras cosas, ayudar a las jurisdicciones a mitigar los riesgos de LD y FT asociados con las actividades de AV y en la protección de la integridad del sistema financiero global. En junio de 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 los AV y VASP, incluso con respecto a la notificación de operaciones sospechosas.

3. El GAFI ha preparado este informe sobre las señales de alerta de LD/FT asociados con los AV para ayudar a los sujetos obligados, 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/FT que involucren AV. Este informe también debe facilitar, por parte de los sujetos obligados, la aplicación de un enfoque basado en riesgos para sus requisitos de debida diligencia 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 los recursos.

4. Las agencias operativas, incluidas las Unidades de Inteligencia Financiera (UIF), las autoridades de procuración de justicia (LEA, por sus siglas en inglés) y los fiscales, pueden encontrar este informe como una referencia útil para analizar los Reportes de Operaciones Sospechosas (ROS) o mejorar la detección, investigación y aseguramiento de los AV involucrados en el uso indebido.

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

Metodología y fuentes utilizadas en la elaboración de las señales de alerta

6. Las señales de alerta incluidas en este informe se basan en más de cien estudios de casos aportados por las jurisdicciones de 2017-2020, los hallazgos del Informe Confidencial del GAFI sobre Investigaciones Financieras que involucran Activos Virtuales (junio de 2019) y el Informe de GAFI publicado sobre Monedas Virtuales: Definiciones Clave y Posibles Riesgos PLD/CFT (junio de 2014), así como información pública sobre el uso indebido de AV.

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

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

Los tipos de delitos informados 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 tramitadas directamente en AV o el uso de AV como técnica de estratificación de LD. La segunda categoría más común de uso indebido está relacionada con fraudes, estafas, *ransomware* (secuestro de archivos a cambio de un rescate) y extorsión. Más recientemente, las redes profesionales de LD han comenzado a explotar los AV como uno de sus medios para transferir, recolectar o acumular ganancias.

Fuente: Estudios de casos aportados por jurisdicciones de 2017-2020

Aspectos por considerar al leer este informe

7. Estos indicadores son específicos de la naturaleza de los AV y sus actividades financieras asociadas, y de ninguna manera son exhaustivos. 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 fiduciaria u otros tipos de activos. Por lo tanto, los sujetos obligados deben considerar los riesgos que plantean sus clientes, productos y operaciones, así como la presencia de indicadores de riesgo convencionales. Las señales de alerta siempre deben considerarse en contexto.

8. Las señales de alerta independientes, como las que se enumeran a continuación, pueden desarrollarse o combinarse con información de agencias operativas, que a su vez pueden desarrollarse más a través de una asociación público-privada, en un proceso cíclico y evolutivo que considere el riesgo y el contexto únicos de una jurisdicción, tipo de cliente o la propia entidad informante. La mera presencia de una señal de alerta no es necesariamente una base para una sospecha de LD/FT, pero podría impulsar un mayor monitoreo y examen. En última instancia, un cliente puede proporcionar una explicación para justificar las señales de alerta, los propósitos comerciales o económicos de una operación.

9. Al evaluar una actividad potencialmente sospechosa, las autoridades competentes, las IF, las APNFD y los VASP deben tener en cuenta que algunas señales 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 operación. 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 una o más señales de alerta están presentes, 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/FT.[1] Estos indicadores no deben ser el único determinante de si se debe presentar un ROS o no. Los sujetos obligados deben considerar la presentación de un ROS si saben, sospechan o tienen motivos razonables de que se ha cometido LD/FT.

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

Señales de alerta

10. Las siguientes secciones contienen una serie de señales de alerta de actividades sospechosas de AV o posibles intentos de evadir la detección de la aplicación de la ley, identificados a través de más de cien estudios de casos recopilados desde 2017 de toda la Red Global del GAFI, revisiones de literatura y fuentes abiertas. Como se mencionó anteriormente, la existencia de un solo indicador no necesariamente indica una actividad delictiva. A menudo, es la presencia de múltiples indicadores en una operación 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.

Señales de alerta relacionadas con las operaciones

11. Si bien los AV todavía no son ampliamente utilizados por el público, su uso se ha popularizado entre los criminales. 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 en general. Este conjunto de indicadores demuestra cómo las señales de alerta tradicionalmente asociadas con operaciones que involucran medios de pago más convencionales siguen siendo relevantes para detectar posibles actividades ilícitas relacionadas con los AV.

Tamaño y frecuencia de las operaciones

- Estructurar operaciones de AV (por ejemplo, cambios o transferencia) en pequeñas cantidades, o en cantidades por debajo de los umbrales de mantenimiento de registros o informes, similar a estructurar operaciones en efectivo.
- Realizar múltiples operaciones de alto valor:
    - en una sucesión breve, como en un período de 24 horas;
    - en un patrón escalonado y regular, sin más operaciones registradas durante un largo periodo posterior, lo cual es particularmente común en casos relacionados con *ransomware*; o
    - a una cuenta recién creada o previamente inactiva.
- Transferir AV inmediatamente a múltiples VASP, especialmente a VASP registrados u operados en otra jurisdicción donde:
    - no hay relación con el lugar donde vive o realiza negocios el cliente; o
    - regulación PLD/CFT inexistente o débil.
- Depositar AV en una oficina de cambios y luego, a menudo, inmediatamente:
    - retirar los AV sin actividad de cambios adicional a otros AV, lo cual es un paso innecesario e incurre en tarifas de operación;
    - convertir los AV en múltiples tipos de AV, incurriendo nuevamente en tarifas de operación adicionales, pero sin una explicación comercial lógica (por ejemplo, diversificación de la cartera); o
    - retirar los AV de un VASP inmediatamente a una cartera privada. Esto convierte efectivamente el intercambio / VASP en una mezcla para el LD.
- Aceptar recursos sospechosos de ser robados o fraudulentos:
    - depositar recursos de direcciones de AV que han sido identificadas como tenedoras de fondos robados, o direcciones de AV vinculadas a los tenedores de fondos robados.

Caso de Estudio 1. Múltiples transferencias inmediatas de una gran cantidad de AV a VASP en el extranjero

Un VASP local presentó un ROS tras sospechas sobre la compra de grandes cantidades de AV por parte de varias personas y sus posteriores transferencias inmediatas a VASP en una jurisdicción extranjera. En varios casos, las personas compartieron la misma dirección residencial; y se accedió a la mayoría de las direcciones de AV desde la misma dirección IP, lo que indica el posible uso de "mulas" por parte de los lavadores de dinero profesionales para lavar las ganancias ilícitas.
Además, se organizaron múltiples capas de los fondos fiduciarios antes de la compra de AV por las mulas. Para disfrazar el origen de los recursos, primero se depositó efectivo en varias cuentas en diferentes IF a lo largo del país.
Posteriormente, esos recursos se transfirieron a varias cuentas a nombre de entidades registradas en la jurisdicción. Los pagos electrónicos se realizaron en las cuentas en cantidades menores. Después de eso, los recursos se transfirieron a otro grupo de cuentas antes de llegar a las cuentas de las mulas en los VASP locales. Los AV se compraron inmediatamente y se transfirieron a VASP extranjeros. Más de 150 personas estuvieron involucradas en este caso, responsables de transferir un total de aproximadamente USD 108 352 900 (o BTC 11,960) a múltiples cuentas de AV mantenidas por dos VASP en el extranjero.
Fuente: Sudáfrica

Caso de Estudio 2. Múltiples AV y múltiples transferencias a VASP extranjeros

Una oficina de cambios local de AV informó que aproximadamente KRW 400 millones (EUR 301,170) fueron robados a víctimas de *phishing* y finalmente se intercambiaron por AV como una técnica de estratificación. Lo que desencadenó el reporte fue las múltiples operaciones de alto valor transferidas a un VASP extranjero en una sola cartera. Los recursos robados en moneda fiduciaria se intercambiaron primero a tres tipos diferentes de AV y luego se depositaron en la cartera AV del sospechoso en un VASP local. Luego, el sospechoso intentó ocultar la fuente de los recursos transfiriéndolos 55 veces adicionales a través de 48 cuentas separadas en diferentes VASP locales, y luego a una cartera AV diferente ubicada en el extranjero.
Fuente: Corea del Sur

Señales de alerta relacionadas con los patrones de operación

12. Al igual que en la sección anterior, las siguientes señales de alerta ilustran cómo el uso indebido de los AV para fines de LD/FT podría identificarse a través de patrones de operaciones irregulares, inusuales o poco comunes.

Operaciones 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 el depósito completo 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 un día después, o si el cliente retira el importe total al día siguiente. Como la mayoría de los AV 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 negociar el saldo completo de los AV, o retira los AV e intenta enviar el saldo completo fuera de la plataforma.

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

Caso de Estudio 3. Depósito inicial inconsistente con el perfil del cliente

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

- operaciones incompatibles con el perfil del titular de la cuenta: en los dos primeros días posteriores a la creación de una cuenta personal para un joven, la cuenta recibió depósitos de naturaleza comercial de diferentes personas morales en grandes cantidades;
- patrones de operación: los recursos depositados se transfirieron inmediatamente a las cuentas de varios VASP (en un día) para la compra de AV (Bitcoin);
- 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 una mula reclutada por criminales en una plataforma de redes sociales para ayudar a recibir pagos reclamados por productos vendidos en línea. Sin embargo, esos recursos parecían haber sido depositados por otras empresas víctimas y no eran pagos por bienes. Los recursos depositados se transfirieron inmediatamente desde 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 AV (Bitcoin) en varios VASP locales. Estos VASP se retiraron inmediatamente de la cuenta. Además de presentar un ROS, el banco también suspendió las transferencias sospechosas, lo que hizo posible la posterior incautación de recursos.

El VASP local también notó irregularidades en los recursos recibidos y brindó información útil para ayudar en la investigación. La información incluía: circunstancias en las que se compraron los AV; operación y otra información de DDC como la dirección de la cartera, 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

Operaciones relativas a todos los usuarios

- Operaciones que involucran el uso de múltiples AV, o múltiples cuentas, sin una explicación comercial lógica.
- Hacer transferencias frecuentes en un período de tiempo determinado (por ejemplo, un día, una semana, un mes, etc.) a la misma cuenta de AV:
    - por más de una persona;
    - desde la misma dirección IP por una o más personas; o
    - en relación con grandes cantidades.
- Operaciones entrantes de muchas carteras no relacionadas en cantidades relativamente pequeñas (acumulación de recursos) con transferencia posterior a otra cartera o cambio completo por moneda fiduciaria. Dichas operaciones de varias cuentas acumuladas relacionadas pueden utilizar inicialmente AV en lugar de moneda fiduciaria.
- Realizar un cambio de moneda VA-fiduciaria con una pérdida potencial (por ejemplo, cuando el valor de AV fluctúa, o independientemente de las comisiones anormalmente altas en comparación con los estándares de la industria, y especialmente cuando las operaciones no tienen una explicación comercial lógica).
- Convertir una gran cantidad de moneda fiduciaria en AV, o una gran cantidad de un tipo de AV en otros tipos de AV, sin una explicación comercial lógica.

Caso de Estudio 4. Transferencias realizadas en un tiempo recurrente

Una IF (empresa de valores) local presentó un ROS con respecto a los pagos no autorizados entre las cuentas de AV de su corredor y un ciudadano extranjero. La empresa de valores informó la actividad después de que determinó que el ciudadano extranjero tenía la intención de realizar transferencias por un total de USD 4.8 millones (dos operaciones separadas que ocurrieron con seis minutos de diferencia el mismo día), y presentó una solicitud al corredor para una cuenta comercial en el siguiente día hábil. La cartera no estaba alojada en las Islas Caimán. El informe de ROS condujo a un intercambio de información exitoso con las UIFs extranjeras y a la devolución exitosa de la mayoría de los recursos 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

Señales de alerta relacionadas con el anonimato

13. Este conjunto de indicadores se basa en las características inherentes y las vulnerabilidades asociadas con la tecnología subyacente de los AV. Las diversas características tecnológicas aumentan el anonimato y agregan obstáculos a la detección de actividades delictivas por parte de las LEA. Estos factores hacen que los AV sean atractivos para los criminales que buscan disfrazar o almacenar sus recursos. Sin embargo, la mera presencia de estas características en una actividad no sugiere automáticamente una operación ilícita. Por ejemplo, el uso de hardware o una cartera 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.

- Operaciones de un cliente que involucran más de un tipo de AV, a pesar de tarifas de operación adicionales, y especialmente aquellos AV que brindan mayor anonimato, como criptomonedas o monedas privadas.
- Mover un AV que opera en una cadena de bloques pública y transparente, como Bitcoin, a un intercambio centralizado y luego intercambiarlo inmediatamente por una criptomoneda de anonimato o moneda privada.
- 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 AV en nombre de su cliente y cobren tarifas más altas a su cliente que la transmisión de servicios ofrecidos por otros cambios. Uso de cuentas bancarias para facilitar estas operaciones P2P.
- Actividad transaccional anormal (nivel y volumen) de AV cobrados en intercambios de carteras asociadas a la plataforma P2P sin una explicación comercial lógica.
- AV transferidos hacia o desde carteras que muestran patrones previos de actividad asociados con el uso de VASP que operan servicios de mezcla o caída o plataformas P2P.
- Operaciones que hacen uso de servicios de mezcla y rotación, lo que sugiere la intención de ocultar el flujo de recursos ilícitos entre direcciones de carteras conocidas y mercados de redes oscuras.
- Recursos depositados o retirados de una dirección o cartera de AV con enlaces de exposición directa e indirecta a fuentes sospechosas conocidas, incluidos mercados negros, servicios de mezcla / volteo, sitios de apuestas cuestionables, actividades ilegales (por ejemplo, ransomware) y / o informes de robo.
- El uso de carteras de papel o hardware descentralizadas / no alojadas para transportar AV 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 usando registradores de nombres de dominio que suprimen o censuran a los propietarios de los nombres de dominio.
- Usuarios que ingresan a la plataforma VASP usando una dirección IP asociada con una red oscura u otro software similar que permite la comunicación anónima, incluidos correos electrónicos cifrados y VPN.

Operaciones 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 carteras AV aparentemente no relacionadas controladas desde la misma dirección IP (o dirección MAC), lo que puede implicar el uso de carteras 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 o enviar recursos a los VASP cuyos procesos de DDC o conocimiento de su cliente son débiles o inexistentes.
- Uso de cajeros automáticos / quioscos AV:
    - a pesar de las tarifas de operación más elevadas e incluidas las que suelen utilizar las mulas o las víctimas de estafas; 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 se usara para operaciones pequeñas repetidas (u otros factores adicionales).

Caso de Estudio 5. Uso de la dirección IP asociada con el mercado negro en la red - AlphaBay

AlphaBay, el mercado negro en la red 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 AV, y tenían aproximadamente 200,000 usuarios, 40,000 proveedores, 250,000 listados y facilitaron más de USD 1,000 millones en operaciones de AV entre 2015 y 2017.
En julio de 2017, el gobierno de EE. UU., con la ayuda de contrapartes extranjeras, desmanteló los servidores que alojaban el mercado 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, y aquellos que representaron el producto ilegal de la empresa criminal AlphaBay. Los agentes federales obtuvieron las órdenes después de rastrear las operaciones de AV que se originaron en AlphaBay a otras cuentas de AV e identificaron cuentas bancarias y otros activos tangibles controlados por el supuesto administrador.
Fuente: Estados Unidos

Caso de Estudio 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 AV por una tarifa durante un período de tres años. Helix supuestamente transfirió más de 350,000 Bitcoin, con un valor en el momento de la transmisión de más de USD 300 millones. El operador anunció específicamente el servicio como una forma de ocultar operaciones en el mercado negro en la red a las fuerzas del orden. En febrero de 2020, se presentaron cargos criminales 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 redes oscuras, hasta que las fuerzas del orden tomaron a AlphaBay en 2017.
Fuente: Estados Unidos

Caso de Estudio 7. Uso de cartera descentralizada

Este caso demuestra cómo los criminales hacen uso de una cartera descentralizada para disfrazar la fuente de recursos ilícitos generada por actividades de tráfico de sustancias ilícitas. En este caso, los criminales realizaron una gran cantidad de venta de drogas en Internet, solicitando el pago no solo en dinero fiduciario, sino también en forma de AV (Bitcoins, Códigos EX, Cheques EXMO).
Los recursos ilícitos recibidos en forma de divisas fiduciarias fueron convertidos a AV con la ayuda de una cuenta anónima en una plataforma de transacciones en línea de Blockchain. Dichos recursos, en la forma de AV, se convierten de vuelta a divisas fiduciarias a través de un cambiario, antes de ser transferidas nuevamente a las cuentas bancarias personales de los criminales. Por su parte, los recursos ilícitos recibidos en la forma de AV, primero fueron transferidos a carteras descentralizadas de Bitcoin en poder de los criminales en cuestión, antes de ser transferidos nuevamente a otras carteras de Bitcoin a diferente tasa cambiaria. Esto aumenta la dificultad de rastrear y monitorear los recursos. De manera similar, los recursos lavados (como AV) fueron convertidos de vuelta a fiduciarios antes de poder ser acreditados en las cuentas bancarias de los criminales. El criminal fue condenado y sentenciado a siete años en prisión y una multa criminal después del juicio.

Señales de alerta sobre remitentes o beneficiarios

14. Este conjunto de indicadores es relevante para el perfil y el comportamiento inusual tanto del remitente como del beneficiario de las transacciones ilícitas.

Irregularidades observadas durante la creación de cuenta

- Crear cuentas separadas bajo nombres diferentes para eludir las restricciones sobre transacciones o retiros impuestas por los VASP.
- Transacciones iniciadas desde direcciones IP que no son de confianza, direcciones IP de jurisdicciones sancionadas, o direcciones IP marcadas previamente como sospechosas.
- Intentar abrir una cuenta frecuentemente dentro del mismo VASP desde la misma dirección IP.
- Sobre los usuarios corporativos/comerciales, sus registros de dominio de Internet se encuentran en una jurisdicción distinta que su jurisdicción establecida o en una jurisdicción con un débil proceso de registro de dominio.

Irregularidades observadas durante el proceso de Debida Diligencia del Cliente

- Información KYC incompleta o insuficiente, o que un cliente decline solicitudes sobre documentos KYC o consultas relacionadas con la fuente de recursos.
- Falta de conocimiento de remitente/beneficiario o proveer información imprecisa sobre la transacción, la fuente de los recursos, 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 embarque.

Caso de Estudio 8. Cliente rechazando proveer información sobre la fuente de los recursos.

Una IF (banco) presentó un ROS en relación con una cuenta de una compañía local que contaba con recursos generados por la venta de cupones que podían ser comercializados con un producto (en este caso, bioplástico). Los recursos eran depositados tanto por personas físicas como morales, algunos originalmente como AV. A pesar de pesquisas posteriores realizadas por el banco, los representantes del propietario de la cuenta no proveyeron información sobre el origen de los recursos. Un análisis subsecuente por parte de las autoridades reveló que los recursos enviados por la compañía mostraban vínculos con sujetos conectados al crimen organizado y con recursos recibidos de un proyecto fraudulento.

Perfil

- Un cliente provee una identificación o credenciales de una cuenta (p.ej. una dirección IP atípica o cookies de Flash) compartidas con otra cuenta.
- Surgen discrepancias entre las direcciones IP asociadas con el perfil del cliente y las direcciones IP desde las cuales están siendo iniciadas las transacciones.
- La dirección de AV de un cliente aparece en foros públicos asociada con actividades ilegales.
- Un cliente es conocido a través de información pública disponible para las fuerzas del orden público debido a una asociación criminal previa.

Caso de estudio 9. El perfil del cliente no coincide con el comercio habitual de AV de alto valor.

Un VASP (cambiador) y una IF (instituto de pago) presentaron ROS ante la UIF relacionados con la comercialización de AV de alto valor que comenzó cuando se abrió la cuenta con el cambiador. De manera específica, el propietario de la cuenta había estado llevando a cabo varias transacciones de compra y venta de AV por más de 180,000 euros - lo cual no coincidía con el perfil del propietario de la cuenta (incluyendo ocupación y salario).
Los análisis realizados hallaron que los AV posteriormente fueron usados para (i) transacciones en un mercado de darknet; (ii) apuestas en línea; (iii) transacciones con VASP que no tenían controles adecuados de PLD/CFT o que tenían investigaciones previas sobre Lavado de Dinero por millones de dólares; (iv) operaciones en plataformas que ofrecían transacciones de AV entre pares; y (v) "mezclando". El propietario de la cuenta también había hecho uso de una variedad de diferentes medios (p.ej. transferencia de dinero, banca en línea y tarjetas prepagadas) para mover una consistente cantidad de recursos fuera de su cuenta en el mismo periodo de tiempo. Los recursos recibidos por el propietario de la cuenta parecían provenir de una red de individuos que compraban AV (Bitcoin) en efectivo y estaban localizados en diferentes jurisdicciones de Asia y Europa (incluyendo Italia), tanto a través de transferencias de dinero y del sistema bancario. Él también recibió recursos en sus tarjetas de prepago de sujetos en África y Medio Oriente, que a su vez recolectaban recursos de conciudadanos residiendo en Italia y en el extranjero. Después, dichos recursos fueron utilizados para transferencias transfronterizas y apuestas en línea, y se retiraron en efectivo de cajeros automáticos en Italia.

Perfil de potenciales mulas de dinero o víctimas de estafa

- El remitente parece no estar familiarizado con la tecnología de AV o soluciones en línea de custodia de cartera. Dichas personas podrían 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 su origen.
- Un cliente considerablemente mayor que la edad promedio de los usuarios de la plataforma abre una cuenta y participa en un gran número de transacciones, sugiriendo su potencial rol como mula de dinero de AV o como una víctima de explotación financiera de ancianos.
- Un cliente que es una persona financieramente vulnerable, usado con frecuencia por los traficantes de drogas para asistirlos en sus negocios de tráfico.
- El cliente compra grandes cantidades de AV no justificado por su patrimonio disponible ni consistente con su perfil financiero histórico, lo cual puede indicar lavado de dinero, mula de dinero o víctima de una estafa.

Caso de Estudio 10. Víctimas de estafa convertidas en mulas

En estas estafas de inversión, los ciudadanos extranjeros contactaron a pensionados o adultos mayores a través de llamadas telefónicas, correos electrónicos o a través de redes sociales, ofreciéndoles oportunidades de inversión en Bitcoin o algunos otros AV con la promesa de generar grandes ganancias dada la creciente popularidad de los AV y su aumento de precio. La inversión inicial en pequeñas cantidades (en muchos casos no más de 250 euros) fue hecha desde la cuenta bancaria de la víctima, su tarjeta de crédito u otros medios de servicios de pagos y terminaron en las manos de los criminales. De manera alternativa, las víctimas fueron instruidas a intercambiar divisas fiduciarias a Bitcoin usando un cajero automático de AV y enviar los recursos a una dirección proporcionada por los criminales.
Las víctimas no eran muy adeptas tecnológicamente y generalmente no comprendían la tecnología de los AV o qué era en realidad en lo que estaban invirtiendo. Los delincuentes también solicitaron a las víctimas instalar una aplicación de escritorio remoto en sus dispositivos para que los criminales pudieran ayudar a transferir los recursos de manera correcta a cuentas específicas. Esto comprometió los dispositivos de las víctimas, ocasionando que los delincuentes pudieran realizar transferencias no autorizadas de dinero sin el conocimiento de la víctima hasta que él o ella notaran el dinero faltante en la cuenta. En algunos casos, los delincuentes también creaban artículos en los que aseguraban que celebridades famosas, importantes empresarios o locutores estaban promocionando las inversiones en AV, generando un sentimiento de confianza y legitimidad de las víctimas hacia estas "inversiones".

Otros comportamientos inusuales

- Un cliente cambia frecuentemente su información de identificación, incluyendo direcciones de correo electrónico, direcciones IP o información financiera, lo cual también puede indicar la toma del control de una cuenta en contra del cliente.
- Un cliente intenta ingresar a uno o varios VASP desde diferentes direcciones IP de manera frecuente en el transcurso de un día.
- El uso del lenguaje en los campos de mensajes de AV como indicativo de las transacciones realizadas en apoyo a una actividad ilícita o en la compra de bienes ilícitos, como drogas o información de tarjetas de crédito robadas.
- Un cliente realiza transacciones repetidamente con un conjunto de personas con ganancias o pérdidas significativas. Esto podría indicar una posible toma del control de la cuenta y el intento de extracción del saldo de la víctima a través del comercio, o un esquema de LD para ofuscar el flujo de recursos con una infraestructura de VASP.

Señales de alerta en la procedencia de Recursos o Patrimonio

15. Como lo demuestran los casos presentados por jurisdicciones, el mal uso de los AV con frecuencia está relacionado con actividades criminales como el tráfico ilícito de narcóticos y sustancias psicotrópicas, fraude, robo y extorsión (incluyendo delitos cibernéticos). A continuación se presentan alertas comunes relacionadas con la procedencia de recursos o patrimonio vinculado con dichas actividades criminales:

- Realizar transacciones con cuentas de AV o tarjetas bancarias que están conectadas con esquemas conocidos de fraude, extorsión o ransomware, direcciones sancionadas, mercados de la darknet, u otros sitios web ilícitos.
- Transacciones de AV que se originaron o están destinadas a servicios de apuestas en línea.
- El uso de una o varias tarjetas de crédito o débito que están vinculadas a una cartera de AV para retirar grandes cantidades de divisas fiduciarias (cripto a plástico), o recursos para comprar AV que se originen como depósitos de efectivo hacia tarjetas de crédito.
- Los depósitos a una cuenta o a una dirección de AV es considerablemente mayor que lo común con una procedencia desconocida de los recursos, seguido por una conversión a una divisa fiduciaria, lo que podría indicar el robo de recursos.

- Falta de transparencia o información insuficiente sobre el origen y titulares de los recursos, como aquellos que involucran el uso de compañías ficticias, o los recursos que son colocados en una Oferta Inicial de Moneda (ICO) donde los datos personales de los inversores puede no estar disponible, o transacciones entrantes de un sistema de pago en línea a través de tarjetas de crédito o de prepago seguido por un retiro inmediato.
- Los recursos de un cliente que provienen directamente de servicios de mezcla de terceros o de tumblers de cartera.
- La mayor parte del origen del patrimonio de un cliente se deriva de inversiones en AV, Ofertas Iniciales de Monedas u Ofertas Iniciales de Monedas fraudulentas, etc.
- La fuente del patrimonio de un cliente se obtiene de manera desproporcionada de AV originados de otros VASP que carecen ce controles PLD/CFT.

Caso de Estudio 11. El uso de compañías ficticias - DeepDotWeb

En mayo de 2019, Agencias del Orden Público de EE.UU. incautaron un sitio web, DeepDotWeb (DDW), de conformidad con una orden judicial. Los supuestos propietarios y operadores de DDW estaban a cargo de una conspiración de LD relacionada con millones de dólares en sobornos que recibieron por referir a individuos a mercados de la darknet a través del sitio de DDW. A través de enlaces de referencia, los supuestos propietarios y operadores de DDW recibieron pagos de sobornos, lo que representaba comisiones sobre las ganancias generadas de la venta de bienes ilegales, como el fentanilo o la heroína, hecha por individuos referidos a mercados de la darknet a través del sitio DDW.

Estos pagos de sobornos fueron hechos en AV a una cartera de Bitcoin controlada por DDW. Para encubrir y disimular la naturaleza y la procedencia de las ganancias ilícitas, que superaban los 15 mdd, los propietarios y operadores transferían sus pagos ilegales de sobornos de su cartera de Bitcoin de DDW a otras carteras de Bitcoin, así como a cuentas bancarias que controlaban a través de compañías ficticias. Los acusados utilizaron estas compañías ficticias para mover sus ganancias ilícitas y realizar otra actividad relacionada con DDW. Durante un periodo de cinco años, el sitio web recibió aproximadamente 8,155 Bitcoin en pago de sobornos de mercados de la darknet, con un valor aproximado de 8 mdd, ajustado al valor comercial de Bitcoin en el momento de cada transacción. El Bitcoin fue transferido a la cartera de Bitcoin de DDW, controlada por los acusados, en una serie de más de 40,000 depósitos, y posteriormente retirado a varios destinos en más de 2,700 transacciones. El valor del Bitcoin al momento de los retiros de la cartera de Bitcoin de DDW equivalía aproximadamente a 15 mdd.

Caso de Estudio 12. El uso de múltiples intercambios de AV, documentos de identificación falsos para la Debida Diligencia del Cliente y tarjetas de prepago.

Los acusados en este asunto supuestamente operaban un esquema de LD en conexión con criminales cibernéticos que hackearon un intercambio de AV y robaron 250 mdd en AV. Supuestamente, los dos acusados lavaron cerca de 91 mdd de los AV robados, así como 9.5 mdd de otro delito cibernético.

Posteriormente, los Activos Virtuales robados fueron enviados a través de cientos de transacciones automática de AV y múltiples intercambios de AV. Los lavadores utilizaron fotografías manipuladas y documentos de identificación falsificados en algunos casos para eludir los procedimientos de KYC en los intercambios de AV. En última instancia, cerca de 35 mdd de los recursos ilícitos fueron transferidos a cuentas bancarias extranjeras y también fueron usados para comprar tarjetas de prepago, las cuales podían ser intercambiadas por AV. Los acusados operaban tanto con cuentas vinculadas como independientes, y prestaban servicios de transmisión de AV, como convertir AV en divisas fiduciarias para los clientes a cambio de una cuota. Los acusados también realizaban negocios en EE.UU., pero en ningún momento con registro ante FinCEN)

Señales de alerta relacionadas con riesgos geográficos.

16. Esta serie de indicadores enfatiza cómo los criminales, al mover sus recursos ilícitos, han tomado ventaja de las diversas etapas de implementación por parte de las jurisdicciones de los Estándares revisados del GAFI sobre AV y VASP. Con base en casos reportados por las jurisdicciones, los criminales han explotado las brechas en los regímenes PLD/CFT de AV y VASP moviendo sus recursos ilícitos a VASP que operan o están domiciliados en jurisdicciones con regulaciones mínimas o inexistentes PLD/CFT para AV y VASP. Estas jurisdicciones puede que no tengan un régimen de registro/licencia, o no han extendido sus requerimientos de ROS para cubrir AV y VASP, o incluso no han introducido el espectro completo de medidas preventivas requeridas por los Estándares del GAFI. A pesar de que este informe no busca identificar una lista de jurisdicciones de "alto riesgo", las entidades que reportan están invitadas a tomar en cuenta los siguientes indicadores al momento de considerar riesgos geográficos. Estos riesgos están asociados con las jurisdicciones de procedencia, destino y tránsito de una transacción. También son relevantes para riesgos asociados con el emisor de una transacción y el beneficiario de los recursos que puede estar vinculado a una jurisdicción de alto riesgo. Aunado a esto, pueden ser aplicables a la nacionalidad, residencia o lugar de trabajo del cliente.

- Los recursos del cliente se originan en o se envían a un cambiario que no está registrado en la jurisdicción donde está localizado el cambiario o el cliente.
- El cliente utiliza un cambiario de AV o un Servicio de Transferencia de Dinero o Valores extranjero en una jurisdicción de alto riesgo que carezca o que se sepa que tiene regulaciones PLD/CFT inadecuadas para entidades de AV, incluyendo medidas inadecuadas de Debida Diligencia del Cliente o KYC.
- El cliente envía recursos a VASP que operan en jurisdicciones que no tienen regulaciones para AV o no han implementado sus controles PLD/CFT.
- El cliente establece oficinas o reubica oficinas a jurisdicciones que no tienen regulaciones o que no han implementado regulaciones que gobiernen los AV, o establece nuevas oficinas en jurisdicciones donde no existe una razón comercial clara para hacerlo.

Caso de Estudio 13. Distribuidor de Bitcoin opera empresas de transmisión de dinero sin licencias (elementos transfronterizos).

En Abril de 2019, el acusado recibió una sentencia de dos años en prisión por operar un empresa de transmisión de dinero sin licencia, luego de vender cientos de miles de dólares de AV (Bitcoin) a más de mil clientes en EE.UU. Al acusado también se lo ordenó pagar una multa por 823,357 dólares en ganancias.
El acusado anunciaba sus servicios en sitios para usuarios de AV, llegando incluso a reunirse en persona con algunos clientes para aceptar dinero en efectivo a cambio de AV. Otros clientes le pagan a través de cajeros nacionales o de servicios de transferencia de dinero. El acusado recibía una prima del 5% sobre el tipo de cambio vigente por sus servicios. Primero adquirió Bitcoin a través de un cambiario estadounidense, pero una vez que sus actividades generaron sospecha y su cuenta fue clausurada, el acusado se cambió a un cambiario en Asia. Utilizando ese cambiario, el acusado compró 3.29 mdd en Bitcoin entre Marzo de 2015 y Abril de 2017 a través de cientos de transacciones por separado. El acusado también admitió que intercambió sus dólares en efectivo, los cuales mantuvo en otra jurisdicción fronteriza con EE.UU., con un distribuidor de metales preciosos, y que entre finales de 2016 y principios de 2018, él, junto con otras personas, ingresaron a EE.UU. un total de más de un mdd en cantidades ligeramente por debajo del requisito de reporte de 10,000 dólares.

VASP moviendo su operación a una jurisdicción con regulaciones inadecuadas PLD/CFT.

Previo a la implementación de una política para prohibir la operación de VASP en la Jurisdicción A de Asia en 2017, un VASP (cambiario) establecido en la Jurisdicción A transfirió sus operaciones a la Jurisdicción B en la misma región. En 2018, la Jurisdicción B intensificó su régimen legal PLD/CFT para AV luego de considerables hackeos a algunos de los mayores VASP (cambiarios). En Marzo de 2018, el VASP anunció sus intenciones de reubicar sus oficinas centrales en la Jurisdicción C de Europa (que, en ese momento, era una jurisdicción que aún no había introducido un régimen integral PLD/CFT para AV y VASP). En Noviembre de 2018, la Jurisdicción C introdujo ciertas regulaciones para los VASP y, en Febrero de 2020, confirmó que a dicho VASP no se le había otorgado la autorización para operar. Informes más recientes de 2020 indicaron que el VASP ya había reubicado el estatus de su registro y domicilio en la Jurisdicción D en África.

Conclusión

17. Este informe se basa en una amplia aportación por parte de los Miembros del GAFI en todo el mundo, 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 actividades de FT que involucran AV.

18. Los indicadores incluidos en este informe son específicos a las características y vulnerabilidades inherentes asociadas con los AV. No son ni exhaustivas ni aplicables en cada situación. Con frecuencia, los indicadores son solo uno de los muchos elementos que contribuyen a una imagen general más amplia del riesgo potencial del Lavado de Dinero y el Financiamiento al Terrorismo y es importante que los indicadores (o cualquier indicador) no sea visto de manera aislada. Deben ser contextualizados con información obtenida de las autoridades pertinentes.

19. Un enfoque basado en riesgo implementado con un diálogo regular y dinámico entre los sectores público y privado sin duda fortalecería la efectividad de este informe. Por lo tanto, se anima a las autoridades competentes a diseminar este informe con los sujetos obligados y a conducir con ellos sesiones de participación y sensibilización para promover la comprensión de este informe.

20. A pesar de que los indicadores identificados están en constante evolución, se les da un mejor uso cuando se aplica información contextual de los organismos nacionales de seguridad y de fuentes públicas. Las autoridades competentes también podrían proporcionar a los sectores privados la información y los indicadores más relevantes para la Jurisdicción. Por ejemplo, usar la información contenida en este informe para preparar sus propios avisos para los sujetos obligados relevantes. Sin embargo, este informe no debe estar destinado a ser utilizado como una herramienta reguladora para fines de cumplimiento o inspección, o como lista de control al momento de supervisar instituciones del sector privado ya que no todos los indicadores son aplicables para todas las jurisdicciones o todas las instituciones.