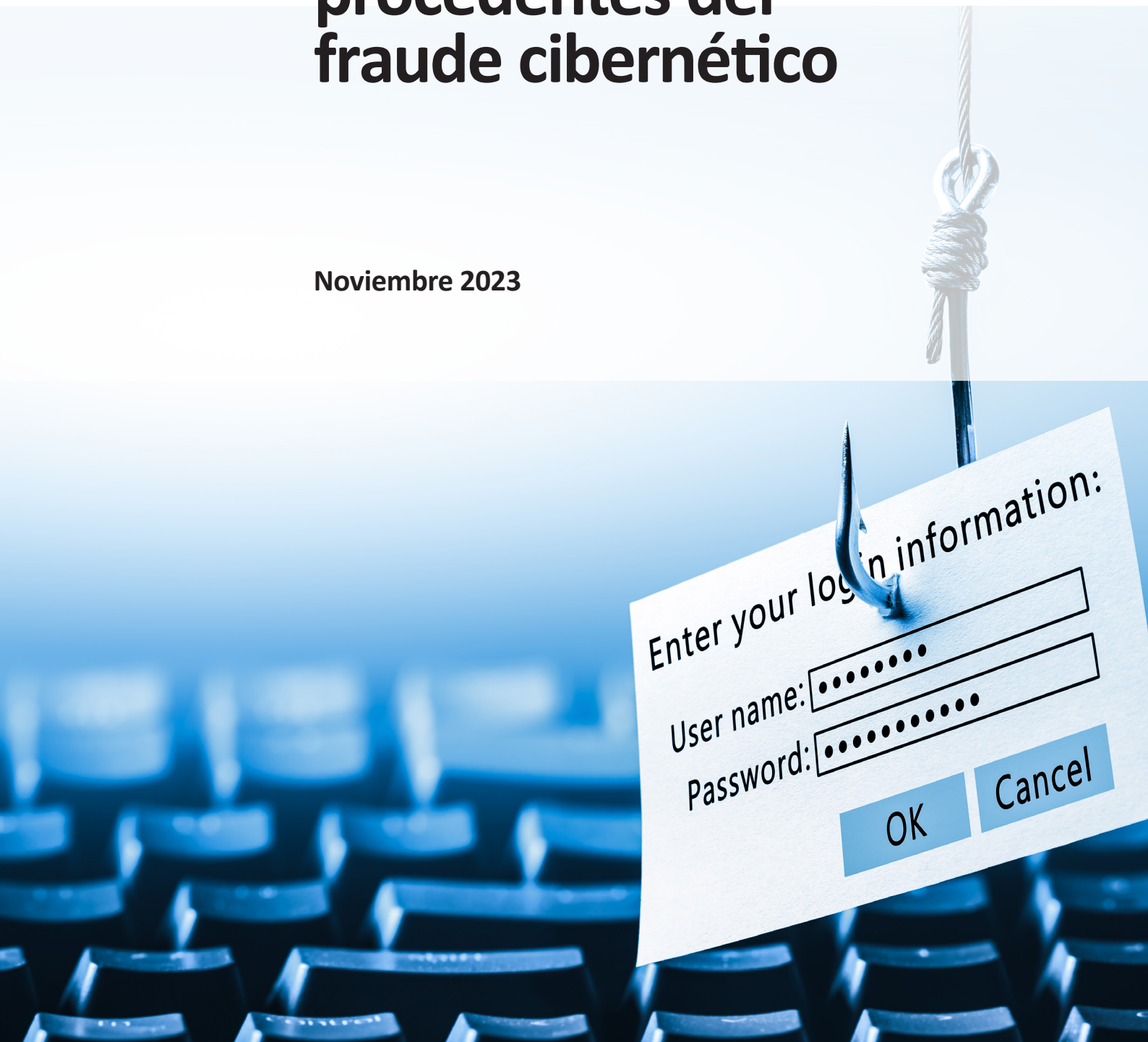
Flujos financieros ilícitos procedentes del fraude cibernético

Noviembre 2023



El Grupo de Acción Financiera (GAFI, o FATF por sus siglas en inglés) es un organismo intergubernamental independiente que desarrolla y promueve políticas para proteger al sistema financiero mundial del lavado de dinero, del financiamiento del terrorismo y de la financiación de armas de destrucción masiva. Las recomendaciones del GAFI son reconocidas como el estándar internacional anti-lavado de dinero y contra el financiamiento del terrorismo (ALD/CFT).

.

El objetivo del Grupo Egmont de Unidades de Inteligencia Financiera (Grupo Egmont) es proporcionar un foro a las unidades de inteligencia financiera (UIF) de todo el mundo para mejorar la cooperación en la lucha contra el blanqueo de capitales y la financiación del terrorismo y fomentar la aplicación de programas nacionales en este ámbito. Para más información sobre el Grupo Egmont, visite el sitio web: www.egmontgroup.org.

La función de INTERPOL es permitir que la policía de sus 195 países miembros trabaje conjuntamente para combatir la delincuencia transnacional y hacer del mundo un lugar más seguro. Mantenemos bases de datos mundiales que contienen información policial sobre delincuentes y delitos, y proporcionamos apoyo operativo y forense, servicios de análisis y formación. Estos servicios policiales se prestan en todo el mundo y sirven de apoyo a cuatro programas mundiales: delincuencia financiera y corrupción, lucha contra el terrorismo, ciberdelincuencia y delincuencia organizada y emergente.

Referencia para citas:

> FATF – Interpol - Egmont Group (2023), *Flujos financieros ilícitos procedentes del fraude cibernético*, FATF, Paris, France, www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html

Foto créditos, foto de portada: Getty.

Tabla de contenidos

Lista de acrónimos

ALA/CFT	Anti Lavado de Activos y Contra el Financiamiento del Terrorismo
ATM	Cajero automático
BEC	Ataques BEC/ Fraude de correo electrónico empresarial
DDC	Debida diligencia del cliente
FC	Fraude cibernético
APNFDs	Actividades y Profesiones No Financieras Designadas
IF	Institución financiera
UIF	Unidad de Inteligencia Financiera
IBAN	Código Internacional de Cuenta Bancaria
PI	Protocolo de Internet
LEAs	Autoridades encargadas de la aplicación de la ley
LD	Lavado de activos
ALM	Asistencia legal mutua
PSP	Proveedor de servicios de pago
APP	Asociaciones público-privadas
ROS	Reporte de Operaciones Sospechosas
FT	Financiamiento del Terrorismo
TBML	Lavado de activos basado en el comercio
AV	Activo virtual
PSAV	Proveedor de Servicios de Activos Virtuales
vIBAN	Código Internacional de Cuenta Bancaria virtual
VPN	Red privada virtual
VoIP	Protocolo de Voz por Internet

Resumen ejecutivo

El fraude cibernético (FC) es una forma de delincuencia organizada transnacional en desarrollo. Las organizaciones que lo llevan a cabo suelen encontrarse estructuradas en diversos subgrupos que cuentan con áreas especializadas con experiencia delictiva, incluyendo el Lavado de Activos (LA). Estos subgrupos también pueden encontrarse poco organizados y descentralizados en diferentes jurisdicciones, lo que complica aún más los esfuerzos para investigar la actividad del FC. También se ha comprobado que tales organizaciones se encuentran vinculadas a otros tipos de delitos, en particular en cuanto a la trata de personas y el trabajo forzado en los centros de llamadas de FC, así como en el financiamiento de la proliferación vinculado a actividades cibernéticas ilícitas procedentes de la República Popular Democrática de Corea (RPDC).

Los grupos de LA y los facilitadores profesionales participan en el proceso del FC-LA. La estructura de LA generalmente involucra personas reclutadas (mulas de dinero, en inglés "*money mules*"), así como empresas ficticias o negocios legítimos. Las estructuras de LA también involucran diferentes tipos de instituciones financieras (IFs), incluidos bancos, proveedores de pagos y remesas, y proveedores de servicios de activos virtuales (PSAVs). Para ocultar aún más el rastro financiero de sus ganancias mal habidas, los delincuentes emplean una combinación de varias técnicas de LA, como el uso de dinero en efectivo, el lavado de activos basado en el comercio (TMBL) y los servicios sin licencia.

Mediante la digitalización, la tecnología ha permitido a los delincuentes de FC desarrollar y aumentar la escala, el alcance y la velocidad de sus actividades ilícitas. Utilizan diversas herramientas y técnicas para engañar a las víctimas o aprovecharse de su estado psicológico y sus emociones para extraer la mayor cantidad de fondos posible. Las organizaciones de FC explotan los avances tecnológicos para facilitar y agilizar el lavado del producto de sus delitos. Los servicios virtuales, tales como la apertura remota de cuentas en línea, también permiten a los delincuentes abrir fácilmente cuentas en el extranjero y lavar las ganancias en el extranjero, con transacciones financieras que se ejecutan a velocidades casi instantáneas. Los delincuentes aprovechan las redes sociales y las plataformas de mensajería para reclutar mulas de dinero a través de las fronteras a gran escala. Los delincuentes también pretenden explotar las vulnerabilidades que surgen a través de nuevas instituciones y productos financieros digitales, así como de sectores no tradicionales tales como el comercio electrónico y las redes sociales y las plataformas de *streaming*.

Las jurisdicciones deben responder de manera más eficaz. Para ello, es necesario:

- emplear iniciativas para aumentar la cantidad de denuncias de las víctimas y mejorar el reporte de operaciones sospechosas;
- analizar eficazmente las voluminosas entradas de información para hacer frente al FC; y
- dada la naturaleza transversal del FC, se requieren mecanismos sólidos de coordinación nacional para combatir y prevenir de manera holística el FC y el LA relacionado.

La ubicación en la que se producen los delitos subyacentes del FC tiende a ser diferente de aquél donde se produce el proceso de LA. Las ganancias se pueden lavar rápidamente a través de una red de cuentas, que a menudo se extienden a través de múltiples jurisdicciones e IF. Las jurisdicciones deben colaborar multilateralmente

para interceptar de manera efectiva y rápida las ganancias del FC que se lavan a través de las fronteras. Para ello, las jurisdicciones deben aprovechar y apoyar los mecanismos multilaterales existentes (y futuros) (como el programa I-GRIP de INTERPOL y el proyecto BEC del Grupo Egmont) para lograr una rápida cooperación internacional y el intercambio de información con el fin de combatir más eficazmente el FC.

Finalmente, el informe incluye una lista de indicadores de riesgo, así como requisitos y controles útiles en materia de combate al fraude, que pueden ser útiles para que las entidades de los sectores público y privado detecten y prevengan el FC y el LA relacionado.

1. Introducción

1. El fraude y las estafas en línea han dominado el panorama de la delincuencia cibernética. En caso de no ser controlados, crecerían en sofisticación y representarán una mayor amenaza y riesgo a medida que organizaciones criminales con mayor organización se involucren en esa actividad ilícita y aprovechen las oportunidades que presentan las nuevas tecnologías, tales como la inteligencia artificial generativa[1].

2. Bajo la Presidencia de Singapur, el GAFI puso en marcha una nueva iniciativa para centrarse en la lucha contra los flujos financieros ilícitos procedentes del fraude cibernético. El presente informe es el resultado de un proyecto conjunto entre el Grupo Egmont, el GAFI e INTERPOL, el primer proyecto que estas tres organizaciones han emprendido conjuntamente, y refleja un fuerte compromiso colectivo para hacer frente a la delincuencia organizada transnacional y sus redes.

1.1. Enfoque y alcance

3. Este informe se centra en el financiamiento ilícito derivado del fraude que se posibilita a través del entorno cibernético o se lleva a cabo en él y que i) entraña delincuencia transnacional, como agentes transnacionales y flujos de fondos, e ii) incluye técnicas engañosas de ingeniería social (es decir, manipulación de las víctimas para obtener acceso a información confidencial o personal). Reconociendo las muchas variaciones de este tipo de fraude, este informe se centra en los siguientes tipos de actividades delictivas [denominadas colectivamente como fraude *cibernético* (FC)]:

   - **Fraude de Correo Electrónico Empresarial (BEC):** Las víctimas reciben instrucciones por correo electrónico que pretenden ser de sus clientes o proveedores en las que se les pide que transfieran fondos a nuevas cuentas de pago.
   - **Fraude de *phishing*:** Se engaña a las víctimas para que revelen información confidencial, tales como datos personales, datos bancarios o credenciales de inicio de sesión de cuentas. Luego, el delincuente utiliza la información para sustraer el dinero de las víctimas de sus cuentas de pago, abrir nuevas cuentas de pago o realizar transacciones fraudulentas.
   - **Fraude de suplantación de identidad en redes sociales y telecomunicaciones:** Esto incluye escenarios en los que delincuentes se ponen en contacto con las víctimas a través de aplicaciones móviles o de redes sociales haciéndose pasar por funcionarios gubernamentales, familiares o amigos, y se aprovechan de las emociones de las víctimas para inducir el pago o entregar el control de las cuentas de pagos o para llevar a cabo actividades financieras como una solicitud de préstamo o la apertura de una cuenta para recibir ganancias delictivas.
   - **Fraude en el comercio en línea/en plataformas comerciales:** Las víctimas son engañadas por anuncios falsos o asesores en línea a plataformas

[1] Véase también Fondo Monetario Internacional (agosto de 2023) *Nota Fintech: Inteligencia Artificial Generativa en Finanzas: Consideraciones de Riesgo*.

inexistentes o falsas (fraudulentas) para el comercio o la inversión relacionada con activos fiduciarios y virtuales.

- **Fraude romántico en línea:** Las víctimas son engañadas para que envíen dinero a los delincuentes después de estar convencidas de que se encuentran en una relación romántica.
- **Estafas de empleo:** Las ofertas de trabajo falsas en las plataformas de redes sociales engañan a las víctimas para que paguen a los estafadores con diversas excusas, incluido el pago por adelantado para comprar productos básicos para impulsar las ventas de una plataforma comercial o una tarifa de garantía para asegurar el empleo.

4. El financiamiento ilícito relacionado con el *ransomware* y otros delitos relacionados con el *malware* no está dentro del alcance de este informe. Los lectores deben consultar el informe del GAFI *sobre la lucha contra el financiamiento del ransomware* (marzo de 2023) para obtener más información sobre el *ransomware*, sobre el lavado a través de activos virtuales (AV) y PSAVs, así como los retos y las buenas prácticas para la mitigación de riesgos. Esta información es pertinente, ya que a veces se explotan los AV y los PSAV para lavar los ingresos del FC.

1.2. Objetivos y estructura

5. El presente informe tiene por objeto mejorar la comprensión de los riesgos por parte de las autoridades competentes de la amenaza que plantea el FC. El informe se basa en el trabajo ya realizado por el GAFI y otros organismos internacionales (incluidos el Grupo Egmont, Europol e INTERPOL), y pretende identificar desarrollos significativos y emergentes que sean relevantes para una mejor comprensión de los riesgos.

    - **En los capítulos 2 y 3** del informe se analiza el entorno actual de riesgo operativo en relación con el FC y se proporciona información sobre los riesgos, las técnicas y las tendencias del FC y el LD relacionado, incluido el impacto y las vulnerabilidades de la digitalización y las nuevas tecnologías.
    - **En los capítulos 4 y 5** del informe se identifican las buenas prácticas y las soluciones operativas utilizadas por las jurisdicciones para superar los desafíos que plantean y desbaratan el FC y el LD relacionado, incluidos los mecanismos de cooperación internacional y recuperación de activos.

1.3. Metodología

6. Este proyecto fue codirigido por expertos de Singapur (en nombre del GAFI), la UIF Hong Kong (en nombre del Grupo Egmont) e INTERPOL. Además, las siguientes jurisdicciones y entidades contribuyeron a la labor como parte del equipo del proyecto: Azerbaiyán, Brasil, Bélgica, Canadá, China, Consejo de Europa, Comisión Europea, Europol, Alemania, Grupo de Acción Intergubernamental contra el LD en África Occidental (GIABA), India, Italia, Israel, Japón, Malasia, México, Comité de Expertos sobre la Evaluación de las Medidas de Lucha contra el LD y FT (MONEYVAL), Arabia Saudita, Pakistán, Portugal, Togo, Reino Unido y Estados Unidos.

7. Las conclusiones del informe se basan en:

- Una revisión de la literatura existente y material de código abierto sobre este tema. Esto incluye datos e investigaciones realizadas por el Grupo Egmont e INTERPOL.
- Una solicitud a la Red Global del GAFI y al Grupo Egmont de más de 200 jurisdicciones y 170 de UIF, respectivamente, para obtener información sobre los riesgos, los marcos y estrategias de aplicación, así como los mecanismos nacionales e internacionales de cooperación y coordinación. En total, el equipo del proyecto recibió aportaciones de más de 80 delegaciones.
- Debates y reflexiones compartidos en la Reunión Conjunta de Expertos del GAFI (abril de 2023) y en el Foro Consultivo del Sector Privado (mayo de 2023), incluido un compromiso específico con el sector privado.

2. Entorno de riesgo: Fraude cibernético

2.1. Aumento de la amenaza del lavado de activos (LA)

8. El FC ha aumentado significativamente a nivel internacional. Si bien no existe una estimación completa de la magnitud y escala global del FC, muchas jurisdicciones informan de un crecimiento constante en los últimos años. Los ingresos ilícitos del FC a menudo se transfieren a jurisdicciones extranjeras. Estos ingresos pueden ser lavados a través de los sistemas financieros de otras jurisdicciones.

9. Según el Informe de INTERPOL sobre las tendencias mundiales de la delincuencia 2022[2], las estafas en línea son una de las tendencias de ciberdelincuencia que se perciben con mayor frecuencia como amenazas «altas» o «muy elevadas» a nivel mundial. La mayoría de las jurisdicciones que proporcionaron información para este proyecto reconocen los riesgos de LA derivados del FC en sus evaluaciones nacionales de riesgos. Se espera que las regiones que no utilizan el efectivo y se basan en lo digital (por ejemplo, donde la mayor parte de la intermediación financiera se realiza a través de servicios en línea) sean más vulnerables a los riesgos de LA asociados a este delito, aunque la naturaleza transnacional del FC implica que los delincuentes pueden atacar fácilmente a las víctimas independientemente de las fronteras internacionales. El siguiente cuadro reúne diversas fuentes de información[3] para proporcionar una visión regional del panorama de amenazas del FC.

Caso 1. Aumento de las amenazas de LA: tendencias regionales de FC

África: En África, el sector financiero rápidamente digitalizado ha abierto una multitud de oportunidades para que los delincuentes perpetren FC, lo que provoca un fuerte aumento del fraude bancario en línea, incluido el *phishing*, el robo de identidad y las estafas de AV. El aumento de las pérdidas financieras a través de estos delitos supone una mayor amenaza para el LA. Por ejemplo, en África Occidental, se considera que el FC es una fuente importante de producto del delito.

Américas: El FC ha sido identificado como un riesgo creciente o emergente. Una jurisdicción señaló que los informes del FC han aumentado año tras año, y señaló que el riesgo de LA relacionado aumentaría en consecuencia. Otro informó que el fraude de inversión en AV aumentó más del 180 por ciento entre 2021 y 2022, y los delincuentes se aprovecharon de la exageración y la publicidad en torno a los AV.

Asia-Pacífico: Las jurisdicciones han citado el FC como un riesgo alto o significativo de LA. Por ejemplo, una jurisdicción citó que la mayoría de los informes de fraude contienen algún tipo de FC y había observado un aumento en el LA vinculado al FC. Otra jurisdicción destacó el papel de los

[2] Véase INTERPOL (2022) *Informe Resumido de Tendencias Criminales Globales*

[3] Incluye información y datos proporcionados por las jurisdicciones, así como informes de INTERPOL y Europol.

actores transnacionales en el fraude a las víctimas a través de una variedad de aplicaciones de inversión ilegales. La pandemia de COVID-19 aceleró la digitalización de los servicios y comportamientos de los ciudadanos, los gobiernos y las empresas de la región. En consecuencia, el FC y el LA asociado se han intensificado y se espera que continúen aumentando.

Caribe: La región es muy susceptible al FC y al LA conexo, con un aumento del fraude general relacionado con el FC en los últimos cinco años. El creciente sector de AV en la cuenca del Caribe también crea vulnerabilidades, entre otras cosas, por la presencia de PSAVs, incluidos los mezcladores de monedas, que pueden utilizarse indebidamente para lavar fondos ilícitos a grupos de delincuencia organizada, incluido el FC.

Europa: Por lo general, se considera que el FC supone un riesgo de LA. Muchas jurisdicciones observaron un gran aumento de esta actividad, ya que se consideraba que el FC planteaba grandes amenazas. El uso de AV se observa comúnmente para lavar los ingresos de FC (particularmente en relación con el fraude comercial en línea relacionado con AV, por ejemplo, ofertas iniciales de monedas fraudulentas).

Oriente Medio y Norte de África (MENA): En consonancia con las tendencias en otras regiones del mundo, la región de Oriente Medio y Norte de África experimentó una aceleración de las tasas de digitalización durante la pandemia, ya que los gobiernos, las empresas y los ciudadanos trasladaron masivamente sus actividades a Internet. Los fraudes financieros en línea, incluidos el *phishing*, el fraude de suplantación de identidad y las estafas en línea, se clasifican como amenazas altas. La región de Oriente Medio y el Norte de África también es vulnerable a LA, ya que los países miembros del Consejo de Cooperación del Golfo (CCG), en particular, son importantes centros de transbordo para el comercio mundial y las actividades financieras.

10. La digitalización y el desarrollo de nuevas tecnologías son los principales impulsores del crecimiento del FC. Los servicios digitales son ahora parte integral de la vida cotidiana y de las funciones públicas. Como resultado, más ciudadanos (incluidos los grupos vulnerables) participan en la actividad en línea. Al mismo tiempo, la digitalización significa que las jurisdicciones están cada vez más conectadas con información y fondos que se mueven rápidamente a través de las fronteras. Estos dos factores han alterado fundamentalmente el panorama delictivo y han creado un entorno de aumento de las amenazas de FC.

11. La pandemia de COVID-19 aceleró la transición de las actividades financieras en persona a la apertura de cuentas, pagos y préstamos en línea. Actividades fraudulentas como estafas telefónicas y por correo electrónico; los fraudes bancarios, de personas de la tercera edad y de atención médica (por ejemplo, relacionados con equipos de protección personal y otros productos de atención médica) y las estafas de inversión fraudulentas han aumentado significativamente a través de Internet a través del uso de teléfonos inteligentes, correo electrónico y redes sociales. Estos cambios en los comportamientos financieros también han tenido un impacto en el panorama del aprendizaje automático, incluido el aumento

del uso de la banca digital y las plataformas de pagos y las transacciones remotas (véase también la sección «Impacto de la digitalización y las nuevas tecnologías» en la página 24)[4].

12. El uso cada vez más frecuente de los teléfonos inteligentes, la tecnología (con nuevas herramientas y aplicaciones en constante evolución), así como las transacciones financieras remotas, han aumentado enormemente la vulnerabilidad de los usuarios. Junto con la tecnología que mejora el anonimato, como las redes privadas virtuales (VPN) y 'The Onion Router'[5], esto puede proporcionar a los delincuentes un manto de anonimato para sus actividades ilícitas. Aprovechando la tecnología, los delincuentes pueden aumentar la escala, el alcance y la velocidad de sus actividades delictivas. Además, se observa que los delincuentes están adoptando un modelo de «delincuencia como servicio»[6], que también reduce significativamente las barreras de entrada para las organizaciones del FC, con una mayor especialización en diferentes aspectos del FC distribuidos en diferentes subgrupos (véase la sección 2.2 a continuación)[7].

13. En muchos casos, los grupos delictivos organizados han ampliado o adaptado sus actividades para incorporar el FC, utilizando las técnicas existentes para lavar sus otros fondos obtenidos ilícitamente.

[4] Véase GAFI (mayo de 2020) *Riesgos de lavado de activos y financiamiento del terrorismo relacionados con la COVID-19 y respuestas políticas* y (diciembre de 2020) *Actualización: Riesgos de lavado de activos y financiamiento del terrorismo relacionados con COVID-19*.

[5] También conocido como TOR, se trata de un software de código abierto que permite a los usuarios navegar por Internet de forma anónima.

[6] Aquí es donde se produce la división del trabajo, ya que los grupos delictivos desarrollan y ofrecen a otros capacidades, habilidades y conocimientos especializados en materia de delincuencia.

[7] Véase Europol (julio de 2023) *Evaluación de la Amenaza de la Delincuencia Organizada en Internet (IOCTA) 2023*; e INTERPOL (2022) *Los delitos financieros y cibernéticos son las principales preocupaciones de la policía mundial, según un nuevo informe de INTERPOL*

Caso 2. Red delictiva común de LA utilizada para el FC y otros delitos

Una red de LA ejecuta juegos de azar en línea y operaciones de FC en el edificio de su empresa en la Zona Económica Especial (ZEE) del país A. El complejo alberga alrededor de diez empresas que operan juegos de azar en línea y operaciones FC por sí mismas o han alquilado el espacio a otros para hacerlo. La red incluye empresas supuestamente legítimas en las regiones fronterizas del vecino país B. La red está dirigida por nacionales del país B que utilizan cuentas bancarias en la moneda del país B para facilitar el movimiento de dinero desde la zona económica especial hasta el país C, donde se encuentran los principales inversores de la empresa. Los dólares estadounidenses de la zona económica especial se lavan a través de casas de cambio en el país B, donde el dinero se convierte en la moneda del país B y luego se transporta al país C. En el lado de la frontera del país C, el dinero se transfiere a los inversores de la empresa.

Fuente: Delincuencia organizada transnacional, casinos y LD en el sudeste asiático: un análisis de amenazas (UNODC, 2022)

2.2. Características delictivas del FC

Elementos del FC

14. Con base en la experiencia de las jurisdicciones, los delincuentes de FC pueden basarse en uno o más de los siguientes elementos para engañar con éxito a las víctimas para que realicen una transferencia fraudulenta. Las diferentes variantes de FC pueden combinar los elementos anteriores de diferentes maneras.

    - Extracción de información (por ejemplo, a través de *phishing*);
    - Engaño social o ingeniería, y aprovecharse de emociones vulnerables (por ejemplo, haciéndose pasar por otra persona o entidad y usándola como premisa para generar urgencia, miedo o confianza; u ofreciendo afirmaciones falsas para ganar dinero fácilmente); y
    - Medio o plataforma en línea (que puede utilizarse para la comunicación o para que las víctimas realicen transacciones en casos de fraude comercial en línea).

15. Una víctima puede ser objeto de diversos tipos de FC. En última instancia, el objetivo es inducir una transferencia de fondos, y los delincuentes utilizarán una variedad de técnicas para lograrlo. Los delincuentes son creativos y pueden participar o hacer la transición a otros tipos de FC si el engaño inicial comienza a presentar fallas. Por ejemplo, una víctima de fraude de *phishing* o suplantación de identidad en las redes sociales podría ser convencida y dirigida a un esquema de fraude de inversión por el mismo delincuente aprovechando la "confianza" ya construida a través del esquema de fraude inicial.

Caso 3. Mismas víctimas, múltiples delitos

La matanza de cerdos (en inglés "*pig butchering*") es una combinación de estafa romántica y fraude de inversión. Con este *modus operandi*, los delincuentes construyen una relación de confianza con la víctima y la convencen de que invierta sus ahorros en plataformas fraudulentas de comercio de criptomonedas. La estafa se perpetra a lo largo del tiempo, lo que resulta en la pérdida de grandes cantidades de dinero.

Tras darse cuenta del fraude, los delincuentes suelen ponerse en contacto con sus víctimas haciéndose pasar por abogados o agentes de la ley que les ofrecen ayuda para recuperar sus fondos, a cambio de una comisión.

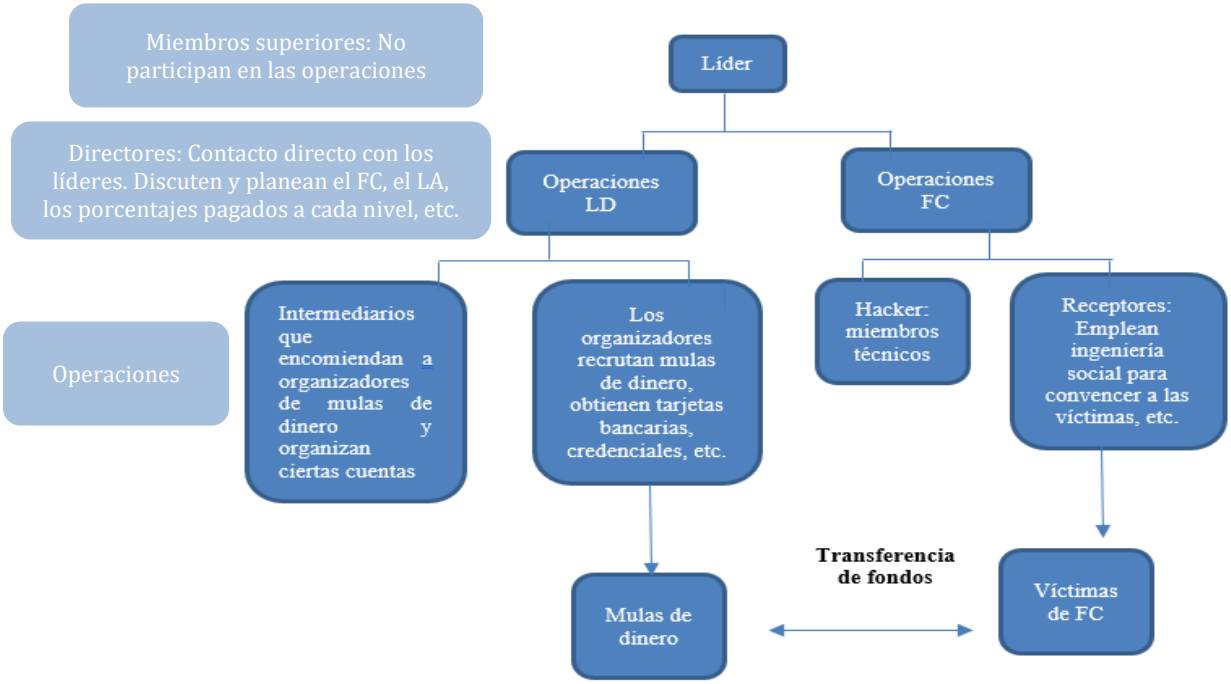
Fuente: Europol (2023), Evaluación de la Amenaza de la Delincuencia Organizada en Internet (IOCTA) 2023

Estructura delictiva organizada

16. El FC y el LA relacionados suelen ser ejecutados por grupos u organizaciones de delincuencia organizada transnacional. Si bien sus estructuras pueden variar, las organizaciones FC a menudo operan como organizaciones jerárquicas (véase el ejemplo en la Figura 1). También pueden estar organizados de forma flexible, con miembros que se unen y se van según sea necesario. Estas organizaciones también pueden organizarse en torno a distintos subgrupos con áreas especializadas de experiencia criminal (por ejemplo, en línea con los elementos del FC anteriores (extracción de información, engaño social; u otros conocimientos técnicos como la creación de una plataforma en línea o LA). En muchos casos, estas organizaciones se encuentran descentralizadas y nunca se han comunicado en persona (por ejemplo, a través de canales encriptados en línea), lo que dificulta que las autoridades los investiguen.

17. Además, las organizaciones del FC suelen encontrarse compuestas por profesionales bien formados y técnicamente competentes. Esto ha dado lugar a un enfoque cada vez más sofisticado del FC y del lavado de ganancias ilícitas. Las jurisdicciones señalaron cómo las organizaciones del FC pueden reclutar intencionalmente a personas que laboran en sectores profesionales (incluidas las IF), que pueden aprovecharse como fuentes de datos e información para ejecutar con éxito el FC y facilitar el LA. Para obtener más información sobre cómo se estructuran y operan las organizaciones de FC en el LA, consulte la sección 2.3 a continuación.

Figura1. Ejemplo de estructura criminal FC



Fuente: GAFI

Vínculos con otros delitos

18. Además del LA, las organizaciones FC pueden encontrarse vinculadas a otras formas de criminalidad. Los delitos comunes incluyen las actividades asociadas o necesarias para llevar a cabo el FC, incluidas las actividades de ciberdelincuencia como la piratería informática para obtener información personal, el desarrollo y la venta de software delictivo; falsificación de documentos, etc. Parte de las ganancias del delito pueden ser auto-lavadas por las organizaciones de FC en la compra de nuevos equipos y el desarrollo de herramientas tecnológicas aún más avanzadas.

Caso 4. Operación Falcón

Tres sospechosos fueron detenidos en Lagos (Nigeria) en 2020 tras una investigación conjunta del Grupo INTERPOL, la Oficina Internacional y la Fuerza de Policía de Nigeria. Se creía que los ciudadanos nigerianos eran miembros de un grupo más amplio de delincuencia organizada responsable de distribuir *malware*, llevar a cabo campañas de *phishing* y extensas estafas de *BEC*. Se alega que los sospechosos desarrollaron enlaces de *phishing*, dominios y campañas de correo masivo en las que se hicieron pasar por representantes de organizaciones. A continuación, utilizaron estas campañas para difundir 26 programas maliciosos, *spyware* y herramientas de acceso remoto.

Estos programas se utilizaron para infiltrarse y vigilar los sistemas de las organizaciones y personas víctimas, antes de lanzar estafas y desviar fondos. Según Group-IB, se cree que la prolífica banda ha comprometido a empresas gubernamentales y del sector privado en más de 150 países desde 2017. Group-IB también pudo establecer que la pandilla está dividida en subgrupos con varios individuos aún prófugos.

Las investigaciones paralelas de LA revelaron que los sospechosos también utilizaron cuentas bancarias y de AV en el Reino Unido, Estados Unidos y Tailandia para recibir pagos de las víctimas. Los tres sospechosos han sido acusados de sus actividades ilegales, incluidos fraude y el LA. Un vehículo de lujo ha sido confiscado y las cuentas de los sospechosos han sido congeladas y sometidas a decomiso en los tribunales.

Fuente: Nigeria

19. También existe un vínculo cada vez mayor entre el FC y la trata de personas, en el que las víctimas son atraídas a través de anuncios de trabajo falsos a centros de llamadas en línea y obligadas a comprometerse con el FC a escala industrial. Esto permite a las organizaciones FC aumentar la diversidad geográfica de las víctimas en línea a las que pueden dirigirse (ya que las víctimas de trata pueden ser explotadas por su conocimiento de los idiomas y su visión cultural). También puede aumentar la sofisticación de los centros de FC mediante la trata de profesionales cualificados, como trabajadores de tecnología de la información o "ejecutivos de ventas digitales"[8]. Estos centros de llamadas a veces operaban intencionadamente dentro de las zonas horarias de las víctimas previstas, y utilizaban propiedades de alquiler para operaciones delictivas temporales, lo que les permitía reubicarse y cambiar rápidamente las direcciones IP para evitar la detección de las fuerzas del orden[9].

[8] Véase INTERPOL, (junio de 2023) *INTERPOL lanza una alerta mundial sobre el fraude impulsado por la trata de seres humanos*

[9] Véase INTERPOL (julio de 2023) *Análisis Operacional Estafas en Línea y Trata de Personas en el Sudeste Asiático / Actualización 2 – De la amenaza regional a la global*; solo disponible para las autoridades policiales nacionales.

Caso 5. Hacedores de tormentas operacionales

En la Operación *Storm Makers*, las autoridades llevaron a cabo acciones coercitivas contra los grupos de delincuencia organizada que se cree que facilitan los viajes de hombres, mujeres y niños asiáticos a través de las fronteras con fines de explotación y/o lucro. La operación desencadenó 121 detenciones en 25 países, lo que dio lugar a 193 nuevas investigaciones.

A través de la Operación *Storm Makers*, la policía de Malasia y Camboya trabajó estrechamente en un caso que involucraba a 15 hombres y una mujer atraídos a Camboya con la promesa de un salario lucrativo para trabajar en un centro de llamadas. A su llegada, sin embargo, fueron encerrados y obligados a trabajar 14 horas al día como estafadores.

Nota: Para más detalles, véase INTERPOL (mayo de 2022) 121 *detenciones en operación contra el tráfico ilícito de migrantes y la trata de seres humanos*

Fuente: INTERPOL

20. En la mayoría de las jurisdicciones no se han visto pruebas sustanciales de actividades de financiamiento del terrorismo vinculadas al FC. Sin embargo, se han observado algunos casos en los que se han asociado elementos de las actividades terroristas y el financiamiento con agentes delictivos del FC. Por ejemplo, los Reportes de Operaciones Sospechosas (ROS) de una jurisdicción sugieren que el producto del FC se estaba transfiriendo en algunos casos a zonas o jurisdicciones específicas de conflicto conocidas por actividades relacionadas con el terrorismo.

21. También hay vínculos con el financiamiento de la proliferación, y se ha informado de que la ciberdelincuencia es una de las principales fuentes de generación de ingresos ilícitos para la RPDC. Las actividades cibernéticas ilícitas incluyen la venta de información personal recopilada o la provisión de herramientas y servicios de piratería informática y *phishing*, que pueden ser utilizados por otros delincuentes para cometer FC[10].

[10] Véase también Consejo de Seguridad de las Naciones Unidas (marzo de 2023) *S/2023/171 Carta de fecha 3 de marzo de 2023 dirigida al Presidente del Consejo de Seguridad por el Grupo de Expertos establecido en virtud de la resolución 1874 (2009)*

Caso 6. Uso de herramientas de *phishing* de la RPDC para que el FC financie programas de armamento

Según la información proporcionada por el Grupo de Expertos de las Naciones Unidas, los trabajadores de la tecnología de la información de la RPDC vinculados al Departamento de la Industria de Municiones han estado ganando divisas vendiendo aplicaciones de piratería informática de *phishing* de voz y operando múltiples servidores y direcciones de Protocolo de Internet en el extranjero.

En julio de 2020, cuatro nacionales de la República de Corea fueron detenidos por las autoridades de China y extraditados a la República de Corea. Uno de ellos testificó que los grupos delictivos habían comprado información personal de ciudadanos de la República de Corea, así como aplicaciones de piratería informática de *phishing* de voz a un trabajador de IT de la RPDC.

Los grupos criminales habían engañado a las víctimas para que descargaran estas herramientas desarrolladas para robarles más información. Posteriormente, se hicieron pasar por empleados de IF para engañar a las víctimas para que enviaran dinero.

Nota: Para más detalles, véase Consejo de Seguridad de las Naciones Unidas (septiembre de 2022) S/2022/*668 Carta de fecha 2 de septiembre de 2022 dirigida al Presidente del Consejo de Seguridad por el Grupo de Expertos establecido en virtud de la resolución 1874 (2009)*

Fuente: Panel de Expertos de las Naciones Unidas y Corea del Sur

2.3. Técnicas y tipologías de LA

Estructura de las redes de LA

22. Al lavar los ingresos generados por varios tipos de FC, los delincuentes deben ser rápidos y eficientes. Las jurisdicciones han observado la participación de grupos profesionales de LA, así como de facilitadores profesionales externos, incluidos abogados, contadores, asesores fiscales, secretarios de empresas y banqueros. Los grupos profesionales de LA pueden formar parte de organizaciones FC, o de una organización descentralizada independiente que preste servicios de LA bajo el modelo de "delincuencia como servicio" (redes profesionales de LA).

Caso 2. Red QQAAZZ

El QQAAZZ anunció sus servicios como un "servicio global de entrega de bancos cómplices" en foros de ciberdelincuentes en línea de habla rusa, donde se reúnen para ofrecer o solicitar habilidades o servicios especializados necesarios para participar en una variedad de actividades delictivas. La red QQAAZZ había abierto y mantenido cientos de cuentas bancarias personales y de empresas ficticias en IFs de todo el mundo, que se utilizaban para recibir dinero de los ciberdelincuentes de FC. Luego, los fondos se transfirieron a otras cuentas bancarias controladas por QQAAZZ y, a veces, se convirtieron en criptomonedas utilizando servicios de "tumbling" diseñados para ocultar la fuente original de los fondos. Después de cobrar una tarifa de hasta el 50 por ciento, QQAAZZ devolvió el saldo de los fondos robados a su clientela criminal.

En noviembre de 2020, una operación policial internacional en la que participaron 16 países derivó en la detención de 20 personas sospechosas de pertenecer a la red criminal QQAAZZ, que intentaba lavar decenas de millones de euros en nombre de los ciberdelincuentes más importantes del mundo. Se llevaron a cabo unos 40 registros domiciliarios en Letonia, Bulgaria, el Reino Unido, España e Italia, y se iniciaron procedimientos penales contra las personas detenidas por los Estados Unidos, Portugal, el Reino Unido y España.

Fuente: Portugal y Europol

23. Por lo general, los ingresos del FC se lavan rápidamente a través de una red de cuentas. Los estudios de casos muestran que estas redes pueden ser complejas al extenderse a través de múltiples fronteras e IFs, aunque esto puede variar según el nivel de sofisticación del grupo criminal.[11]

24. Las redes de cuentas de LA relacionadas con FC suelen involucrar tanto a personas físicas como jurídicas.

- **Los delincuentes suelen reclutar a las mulas de dinero individuales** a través de diversos medios, como ofertas de trabajo y anuncios, así como interacciones en las redes sociales en línea. Los reclutadores de mulas de dinero también se conocen como "pastores" de mulas. Las mulas de dinero pueden ser cómplices teniendo conocimiento del lavado de fondos o trabajar involuntariamente (mediante engaño) o negligentemente, y también se les pueden ofrecer incentivos u honorarios para manejar los fondos ilícitos. Es difícil identificar al controlador de la mula (es decir, el pastor de mulas), que recluta a participantes conscientes e involuntarios, o determinar el origen de los fondos fraudulentos. Algunas jurisdicciones señalaron casos de reclutamiento de extranjeros sin conexión aparente con la jurisdicción, y se ordenó a estas personas que establecieran cuentas de mulas, ya sea mediante viajes físicos o mediante la apertura de cuentas virtuales.

[11] Para obtener más información sobre el uso de mulas en redes y lavadores de activos profesionales, consulte GAFI (julio de 2018) *Lavado de Activos profesional*

Caso 3. Reclutamiento de mulas: Oferta de trabajo

La Sra. RS es propietaria de una tienda de sari-sari que fue reclutada por un tal Sr. O en lo que ella pensó que era una oferta de trabajo legítima. El Sr. O es un ciudadano nigeriano que fue detenido en 2019 por presuntamente operar una estafa romántica multimillonaria en línea, lo que resultó en más de 8 millones de PHP (unos 129 000 euros) en pérdidas.

El Sr. O le había prometido a la Sra. RS una parte por cada transacción bancaria que ella manejara. En total, la Sra. RS gestionó 83 transacciones por un importe de 3,6 millones de pesos filipinos (unos 58.000 euros) durante un período de seis meses. Todas las transacciones se realizaron en efectivo (es decir, depósitos en efectivo, retiros en cajeros automáticos y en ventanilla). El Sr. O fue finalmente arrestado gracias a la colaboración de la Sra. RS a través de una operación de trampa.

Fuente: Filipinas

- **Las empresas ficticias** están bajo el control de los delincuentes del FC, por lo general a través de testaferros o directores nominales. Las mulas de dinero individuales reclutadas también pueden ser instruidas para que actúen como tales testaferros y abran cuentas corporativas en un intento por oscurecer aún más la propiedad criminal. Algunas jurisdicciones señalaron que las empresas ficticias utilizaban direcciones comerciales virtuales[12] para ocultar aún más sus actividades delictivas. En los casos de fraude comercial en línea, los delincuentes también pueden utilizar estas empresas ficticias para abrir cuentas virtuales de punto de venta con empresas de servicios comerciales para procesar pagos y transferencias de las víctimas.

[12] Las direcciones comerciales virtuales son direcciones físicas reales ofrecidas por algunos proveedores de servicios que permiten a las empresas recibir correo postal y paquetes.

Caso 4. Empresas ficticias en el fraude de plataformas comerciales en línea

Se presentaron varios ROS ante la UIF de Turquía en relación con un esquema de fraude en una plataforma comercial en línea en la que se contactaba a las víctimas para que realizaran inversiones en divisas por teléfono o en las redes sociales. Este esquema se basaba en una red de 209 empresas que habían lavado las ganancias entre sí. Las empresas contaban con cuentas mutuas y en su mayoría se constituyeron en la misma fecha y se liquidaron al cabo de un breve período.

El análisis realizado por la UIF de Turquía reveló que las empresas ficticias también actuaban en tres subgrupos distintos, basados en las transferencias de fondos y los cómplices individuales de terceros asociados con ellas. Se descubrió que un total de aproximadamente 10.000 millones de liras turcas (unos 336,7 millones de euros) habían sido adquiridos y lavados de forma fraudulenta.

- Ciento treinta y cinco empresas recibieron 9.600 millones de liras turcas (unos 323,2 millones de euros) de ingresos procedentes del fraude a través de empresas de pago. Para facilitar la recepción de transacciones de las víctimas, estas empresas establecieron cuentas virtuales en el punto de venta. Se retiraron 100 millones de liras turcas (unos 3,4 millones de euros) en efectivo y unos 6.000 millones de liras turcas (unos 202 millones de euros) se transfirieron a una empresa de oro.
- Cincuenta y nueve empresas recibieron 700 millones de liras turcas (unos 23,6 millones de euros) de ingresos procedentes del fraude. Se retiraron 200 millones de liras turcas (unos 6,7 millones de euros) en efectivo, y los demás se transfirieron a PSAVs tras ser lavados a través de cuentas mantenidas por terceros cómplices individuales.
- Veintitrés empresas recibieron 875 millones de liras turcas (unos 29,5 millones de euros) procedentes del fraude. Se retiraron 220 millones de liras turcas (unos 7,4 millones de euros) en efectivo, y los demás se transfirieron a PSAVs tras ser lavados a través de cuentas mantenidas por terceros cómplices individuales.

Fuente: Turquía

- **Las empresas legítimas,** similares a las mulas de dinero individuales, también pueden ser engañadas para que reciban los ingresos del FC (por ejemplo, como una inversión o una oportunidad de negocio) y se les puede pedir que redirijan los fondos o que se les reembolse a una cuenta separada controlada por delitos. En algunos casos, se observó que las empresas legítimas aceptaban de buen grado esas "oportunidades comerciales", especialmente en tiempos de dificultades económicas. La participación de

empresas legítimas proporciona una fachada adicional para enmascarar las actividades ilícitas para que no se detecten.

25. Hay similitudes en la forma en que se establecen las mulas de dinero en las redes de LA para FC y otros tipos de delitos. Sin embargo, las jurisdicciones han observado algunas diferencias que pueden ser más relevantes para las mulas relacionadas con el FC.

- **Método de reclutamiento**: Es más probable que las mulas de dinero del FC sean reclutadas en línea, incluso a través de anuncios de empleo de empresas falsas o a través de correos electrónicos no deseados. Los delincuentes también pueden explotar las condiciones económicas y enmascarar esto como una oportunidad de trabajo legítima para obtener "dinero fácil". Las víctimas de FC (por ejemplo, a través de un fraude romántico) a menudo pueden ser engañadas para que actúen como mulas de dinero. En algunos casos, las víctimas de trata de personas (como los migrantes ilegales o los trabajadores) también son utilizados para abrir esas cuentas.
- **Uso de cuentas**: Las mulas de dinero vinculadas al FC son empleadas por sus cuentas en IFs, ya que los fondos fraudulentos pueden recibirse y enviarse rápidamente a través de métodos de pago electrónicos, en lugar de transferencias físicas o depósitos de efectivo. Es probable que esto se deba a la forma en que se estafa a las víctimas (es decir, a través de transferencias de fondos). Dada la conveniencia que ofrecen los servicios bancarios digitales en el movimiento de fondos, es probable que las personas a las que se dirigen las mulas relacionadas con el FC tengan algún nivel básico de conocimiento o competencia en informática y tecnología.

Caso 5. Víctima de estafa romántica convertida en mula

Entre abril y mayo de 2022, una anciana que abrió su cuenta bancaria originalmente para recibir su pensión recibió dos pagos por un monto superior. Una de las remesas fue desde una cuenta bancaria nacional, mientras que la segunda fue de una víctima reportada desde el extranjero.

La investigación posterior de las autoridades eslovacas reveló que la mujer se comunicó con un individuo a través de las redes sociales y fue víctima de una estafa romántica. La anciana proporcionó sus credenciales bancarias por Internet al estafador y su cuenta bancaria se utilizó para lavar otras ganancias del delito. Parte del dinero recibido se cambió a una criptomoneda a través de una plataforma extranjera de PSAVs.

Fuente: Eslovaquia

Tipologías y técnicas de LA

26. El lugar en el que se produce el FC (es decir, donde se encuentra la víctima) suele ser diferente del lugar en el que se produce el LA del FC, y las redes de mulas de dinero pueden abarcar múltiples jurisdicciones. Las organizaciones FC son conscientes de que es posible que las IFs o las autoridades competentes ya hayan identificado cuentas de actividades fraudulentas antes del lavado, lo que podría dar

lugar a la interceptación de sus ganancias delictivas antes de que puedan llegar a las cuentas de los delincuentes. Para mejorar su éxito, los delincuentes pueden realizar "pruebas" realizando transacciones de pequeño valor para poder cambiar el destino de los fondos si las pruebas fallan.

27. El tipo de cuenta de primer nivel utilizada para recibir los ingresos del FC suele depender del tipo de FC para continuar con la fachada de legitimidad. También se han observado cambios a lo largo del tiempo en el tipo de cuenta de primer nivel. Por ejemplo, en los casos de fraude BEC, las organizaciones de FC han pasado del uso de cuentas de personas individuales al uso de cuentas de empresas para reducir el riesgo de detección.

Tabla 1. Relación entre el tipo de FC y la cuenta de primer nivel

Tipo de FC	Tipo de cuenta de primera capa
Fraude BEC	Corporativo (por ejemplo, empresas fantasma o recién registradas)
Fraude de phishing	Mulas de dinero individuales
Fraude de suplantación de identidad en las telecomunicaciones de las redes sociales	Mulas de dinero individuales
Comercio en línea / fraude en plataformas comerciales	Corporativo (por ejemplo, empresas ficticias o recién registradas)
Fraude romántico en línea	Mulas de dinero individuales
Estafas de empleo	Mulas de dinero individuales

Nota: Esta tabla intenta presentar algunas tendencias generales basadas en la experiencia de las jurisdicciones sobre los tipos de cuentas de primera capa encontradas para el tipo de FC. Sin embargo, es posible que esto no se aplique a todos los casos.

28. Una vez que organizaciones de FC establecen una cuenta, los fondos adquiridos de manera fraudulenta se procesan rápidamente para ingresar a la red de LA. A partir de entonces, los fondos se transfieren rápidamente a través de una serie de transacciones de "transferencia" a través de cuentas nacionales o extranjeras controladas por las propias mulas/testaferros o por organizaciones de FC. En este último caso, las mulas de dinero entregarían credenciales bancarias, tarjetas y fichas, o proporcionarían un poder notarial a organizaciones de FC para permitirles el control directo de las cuentas. La participación de facilitadores profesionales en el proceso, como durante la creación de un poder notarial, da a las transacciones un aire de legitimidad y facilita la ofuscación del delito.

29. Para evadir aún más la detección y permanecer en el anonimato, organizaciones de FC emplean diversas técnicas y mecanismos: por ejemplo, el *smurfing*, el salto a través de cuentas de diferentes proveedores de servicios financieros, de remesas o de pago, y la conversión a otros tipos de activos financieros (por ejemplo, dinero electrónico (e-money),[13] tarjetas prepagadas, AVs). Esto puede aumentar el tiempo necesario para que las UIF y las autoridades encargadas de la aplicación de la ley (LEAs) accedan a los datos financieros necesarios a través de las fronteras, los

[13] El dinero electrónico es una representación digital de la moneda fiduciaria que se utiliza para transferir electrónicamente valor denominado en moneda fiduciaria. El dinero electrónico es un mecanismo de transferencia digital de moneda fiduciaria, es decir, transfiere electrónicamente un valor que tiene curso legal; GAFI (junio de 2014) *Definiciones clave de monedas virtuales y riesgos potenciales de ALA/CFT*

sectores y las instituciones, con el fin de rastrear, asegurar y, finalmente, recuperar las ganancias ilícitas. Es posible que algunas mulas de dinero solo permitan que sus cuentas se usen durante un período de tiempo específico y limitado. El período de tiempo limitado, junto con los procedimientos legítimos de incorporación, hacen que sea relativamente difícil para las instituciones detectar actividades anormales.

Caso 6. Empresas ficticias, cuentas bancarias y AV

Se presentaron múltiples quejas ante la policía de la India de que se estaba utilizando una aplicación móvil para estafar a las personas bajo la apariencia de una plataforma de inversión para la minería de criptomonedas. La aplicación prometía una parte de las ganancias obtenidas de dicha inversión. La empresa había atraído a las víctimas para que invirtieran más en el plan y, a partir de entonces, se detuvieron los retiros y pagos. El sitio web y la aplicación se volvieron inaccesibles, y los operadores de la aplicación dejaron de responder a los inversores. Múltiples LEAs que investigaban las quejas presentadas por clientes en diferentes partes del país solicitaron información a la UIF de la India en este caso. El análisis realizado por la UIF de la India identificó dos entidades que operaban la aplicación en Google Play Store, que posteriormente fueron eliminadas. Se identificaron otras 34 entidades vinculadas a estas dos entidades. De las 36 entidades, 28 tenían como directores a extranjeros.

La Dirección de Ejecución (DE) de la India también inició investigaciones paralelas de LA, que revelaron una conspiración criminal a gran escala y la participación de varias entidades ficticias en la operación de aplicaciones/sitios web fraudulentos similares para engañar a personas desprevenidas y desviar el producto del delito. En la verificación física, las entidades no pudieron ser encontradas en la dirección registrada. Siguiendo el rastro financiero, también se descubrió que varias de estas entidades estaban involucradas en el funcionamiento de aplicaciones ilegales de apuestas y préstamos y también estaban engañando al público bajo la apariencia de estas aplicaciones. El dinero ilícito recaudado de las víctimas se trasladó a cuentas de varias entidades ficticias y parte del producto del delito también se convirtió finalmente en AVs. Se encontraron y congelaron productos del delito en forma de saldos disponibles en las cuentas bancarias de varias entidades ficticias por valor de 865 millones de rupias (9,9 millones de euros).

Fuente: India

30. Las jurisdicciones informaron además del uso de otros tipos de técnicas de LA, destinadas a ofuscar el vínculo entre los diferentes grupos criminales de FC y LA.

- **Dinero en efectivo:** Múltiples estudios de caso en este informe incluyen el retiro de efectivo por parte de mulas y organizaciones de FC. El movimiento de efectivo fuera de las IFs puede ser difícil de rastrear. El efectivo se puede retirar a través de cajeros automáticos después de ser lavado a través de una red de LA, lo que permite a los delincuentes evitar el contacto cara a cara con las IFs. Estos fondos pueden ser enviados a través de las fronteras por

mensajeros de dinero en efectivo y ser depositados para su posterior lavado. El producto del delito también puede utilizarse para comprar objetos de valor e instrumentos que luego pueden revenderse por dinero en efectivo, como tarjetas de prepago o metales preciosos.

Caso 7. Retiro de efectivo y compra de oro y tarjetas de combustible

En marzo de 2023, un contador de una empresa china fue víctima de un fraude de suplantación de identidad bancaria. Fue agregado a un grupo en una aplicación de mensajería con el argumento de que se debía realizar una inspección anual de la cuenta de la empresa.

Posteriormente, los delincuentes del grupo de mensajería se hicieron pasar por los representantes legales y accionistas de la empresa y solicitaron a la víctima que transfiriera 7,8 millones de yuanes (unos 996 000 euros) a dos cuentas corporativas designadas bajo el control del grupo delictivo. Las investigaciones policiales mostraron que los fondos se transfirieron a 26 cuentas bancarias secundarias y luego se retiraron en efectivo en las ventanillas bancarias o a través de cajeros automáticos, se transfirieron a plataformas de pago de terceros y se utilizaron para comprar oro y tarjetas de combustible.

Fuente: China

- **LA basado en el comercio/servicios:** Existen varias técnicas de LA basadas en el comercio/servicios que los delincuentes pueden emplear para mover el producto del delito a través de las fronteras[14]. En el caso de los productos del FC, algunas jurisdicciones han observado que los delincuentes utilizan técnicas de LA basadas en el comercio, como la facturación ficticia o falsa, así como el uso de ingresos ilícitos para comprar bienes de alto valor o fácilmente comercializables (por ejemplo, piezas de vehículos, billetes, artículos para el hogar, etc.). Por ejemplo, algunas jurisdicciones informaron de transferencias electrónicas fraudulentas a empresas legítimas, que van desde conocidas marcas de lujo o electrónica, hasta pequeñas empresas locales para la compra de bienes. Estos bienes pueden trasladarse a través de las fronteras y volver a convertirse en dinero en efectivo para una mayor estratificación e integración. Es posible que las empresas comerciales fuera del régimen ALA/CFT no tengan la conciencia o el conocimiento suficientes para realizar la verificación de identidad o el monitoreo de transacciones, y que los delincuentes las exploten involuntariamente. La entrega de facturas ficticias o sobrevaloradas por servicios informáticos o de consultoría, también puede formar parte de las técnicas de LA adoptadas.

[14] Véase también GAFI – Grupo Egmont (diciembre de 2020) *Lavado de activos en el comercio: tendencias y evolución*; y GAFI (julio de 2018) *Lavado de activos profesional*

Caso 8. FC, mulas y TBML

Las autoridades irlandesas arrestaron a una persona clave, Persona MS, en un esquema de LA procedente de estafa romántica y de BEC de Irlanda a Nigeria a través de TBML. Las investigaciones aún se encuentran en curso. Hasta el momento, las autoridades creen que el esquema de lavado involucra al menos 60 nombres y 64 cuentas bancarias.

En este esquema, el producto de este fraude se transfiere primero a las cuentas bancarias de las mulas irlandesas. A continuación, los fondos se retiran en efectivo y se transfieren a cuentas irlandesas directamente vinculadas o propiedad de la persona MS. Se descubrió que muchas de las cuentas vinculadas a la persona MS se encontraban abiertas con identidades falsas.

Una empresa nigeriana (controlada por un nigeriano que se cree que tiene su sede en los Estados Unidos) encarga productos a empresas europeas o chinas legítimas. Estas empresas legítimas se ocupaban de bienes que se pueden comprar y enviar para su reventa, como alcohol, ropa, productos electrónicos y productos farmacéuticos. Las cuentas irlandesas de la persona MS realizarían el pago de las facturas pertinentes, y las mercancías se enviarían finalmente a la empresa cómplice en Nigeria.

En un caso, una empresa farmacéutica alemana recibió fondos de más de 1,7 millones de euros para pagar los bienes adquiridos por la empresa nigeriana. Estos fondos se rastrearon directamente hasta las ganancias provenientes del fraude BEC y las del fraude romántico en Europa y los EE. UU., y provenían de varias cuentas vinculadas o propiedad de la persona MS, o directamente de las víctimas. Estos productos fueron finalmente enviados a Nigeria.

Fuente: Irlanda

- **Remitentes y PSAVs sin licencia o no registrados:** Las ganancias del delito pueden transferirse fuera de la jurisdicción utilizando remitentes de dinero clandestinos o servicios de *hawala* con poco o ningún control ALA/CFT. Cuando se trata de AVs, las organizaciones de FC pueden obtener beneficios de PSAVs con sede en jurisdicciones sin controles ALA/CFT o con controles débiles o nulos.
- **Técnicas de mejora del anonimato de AVs:**[15] El uso de billeteras no alojadas, transacciones *peer-to-peer*, cadenas *peel* (en inglés *"peel chains"*) e intercambios de alto riesgo son los métodos preferidos para lavar rápidamente los ingresos de FC relacionados con AVs fuera de una jurisdicción y, a menudo, se usan en combinación. Los delincuentes también utilizan cada vez más los cajeros automáticos de Bitcoin para transferir valor y ocultar la identidad de quienes controlan los fondos, lo que incluye proporcionar documentos de identificación falsificados o alterados, como diferentes identificadores, números de teléfono o fechas de nacimiento al

15 Estas técnicas se exploran en profundidad en GAFI (marzo de 2023) *Lucha contra el financiamiento del ransomware*

depositar o retirar fondos. También emplean técnicas de ofuscación, incluido el uso de mezcladores o *tumbler*, así como AVs mejorados para el anonimato (también llamados monedas de privacidad, por ejemplo, Monero) y servicios de finanzas descentralizadas (DeFi).

Caso 9. LA complejo en múltiples sectores

Una organización de fraude romántico en el extranjero se dirigió a aproximadamente 70 víctimas de nacionalidad japonesa. Se transfirieron fondos por valor de 3 millones de dólares a varias cuentas bancarias de mulas de dinero en Japón. Un japonés, que actuaba como pastor de mulas local, lavó los fondos en Ghana, donde tenía su sede la organización de estafadores. El japonés fue finalmente detenido gracias a la cooperación de Ghana a través de INTERPOL.

Los fondos de las cuentas de mulas se transfirieron posteriormente a la cuenta del pastor de mulas japonés. El análisis de ROS encontró que los fondos fueron lavados a través de tres canales por el pastor de mulas japonés:

- Se hicieron transferencias bancarias a una cuenta bancaria del pastor de mulas japonés en Ghana. Luego, los fondos se retiraron físicamente en efectivo en Ghana y se entregaron personalmente al líder de la organización, que todavía está prófugo. Al realizar las transferencias bancarias, el japonés presentó facturas ficticias a su banco japonés y declaró falsamente que eran para una actividad comercial legítima (compra de granos de cacao).
- Algunos fondos se intercambiaron en AVs a través de un PSAV en Japón.
- También se transfirieron fondos a Ghana a través de un banco clandestino vinculado a la comunidad ghanesa en Japón.

Fuente: Japón

Impacto de la digitalización y las nuevas tecnologías en el LA

31. Las nuevas tecnologías han proporcionado nuevos beneficios y oportunidades para los consumidores. Se está produciendo un profundo cambio hacia la digitalización de los servicios financieros, que se aceleró durante la pandemia de COVID-19. La reducción en el uso de efectivo y el aumento de la actividad en línea han dado lugar a nuevas herramientas y procesos innovadores. La cadena de pagos financieros también es cada vez más dinámica y fragmentada, con una mayor diversidad de proveedores de servicios que ofrecen servicios de pago y transacciones (véase también la sección 3.1).

32. Sin embargo, el desarrollo tecnológico también puede ser una ventaja para los grupos criminales, que aprovechan estas oportunidades para mejorar drásticamente sus técnicas de LA. Las transacciones financieras se ejecutan cada vez más a velocidades casi instantáneas, impulsadas en parte por las expectativas de los consumidores de una experiencia sin fricciones. Como se mencionó anteriormente, junto con las técnicas digitales como las VPN, esto dificulta que las autoridades

identifiquen a los delincuentes finales que realizan estas transacciones de LA en rápida sucesión.

33. La digitalización ha aumentado la facilidad y la velocidad a la que se pueden crear cuentas para LA y amplía el alcance transfronterizo de organizaciones de FC. Algunas jurisdicciones señalaron el aumento de los procesos virtuales remotos en dos ámbitos: la apertura de cuentas y la creación de empresas. Estos procesos virtuales remotos niegan la necesidad de viajar físicamente. Los delincuentes pueden aprovechar estas oportunidades para el aprendizaje automático.

Caso 10. Escalado a través de la digitalización

El análisis de la UIF encontró una extensa red compuesta por 147 personas y 276 cuentas bancarias de ocho bancos. Estas personas habían cedido su identidad digital nacional, destinada a la identificación de usuarios en el gobierno y otras plataformas en línea, a organizaciones criminales. A continuación, las organizaciones de FC utilizaron la identidad digital para abrir cuentas bancarias a distancia y ejercer un control directo sobre estas cuentas mula para lavar los ingresos del FC. La UIF detectó la red mediante la identificación de puntos en común, como transacciones bancarias comunes, puntos de datos (información de contacto extranjera e identificación del dispositivo), así como detalles de contacto (correo postal, correo electrónico, teléfono).

La información de inteligencia fue remitida al Comando Anti-Estafa (ASCom), la unidad dedicada de Singapur a combatir el FC y el LA relacionado bajo la Fuerza de Policía de Singapur. Las investigaciones de ASCom finalmente resultaron en el arresto de 6 sujetos y el enjuiciamiento de 3 personas por su papel en el esquema criminal.

Fuente: Singapur

34. Los delincuentes pueden expandir rápidamente la magnitud (a menudo transnacional) de una red de mulas de dinero aprovechando las herramientas digitales para ampliar el reclutamiento de mulas a través de las fronteras. Las redes sociales y las aplicaciones de voz sobre protocolo de Internet (VoIP) también se han identificado como los medios preferidos en el proceso de reclutamiento de mulas. Tradicionalmente, puede haber cierto grado de fricción en el LA a través de redes de mulas, ya que se necesita tiempo para que las mulas reciban y cumplan las instrucciones proporcionadas por otras organizaciones delictivas. Estos lapsos de tiempo se han reducido significativamente gracias al uso de plataformas de mensajería instantánea por parte de las organizaciones de FC.

35. Cada vez más, los delincuentes pueden robar identidades a través de diversas técnicas y herramientas tecnológicas, como el *phishing*, la compra o el engaño a alguien para que entregue voluntariamente su identidad. A veces, pueden utilizar identidades falsificadas e identidades sintéticas, que implican la combinación de información de identidad real y falsa para crear cuentas de forma fraudulenta. A continuación, los delincuentes crean y controlan directamente las cuentas utilizando estas identidades robadas o falsificadas. Esto hace que sea más difícil

rastrear las actividades de LA, ya que es posible que los titulares de las cuentas ni siquiera sean conscientes de su participación.

36. Una delegación señaló los riesgos de que los *deepfakes* se utilicen potencialmente para el fraude de apropiación de cuentas. Con la ayuda de algoritmos de aprendizaje automático, un estafador puede crear un *deepfake* de la voz o el video de alguien, que luego se puede usar para hacerse pasar por esa persona por teléfono o en sistemas de autenticación biométrica. Los *deepfakes* también se pueden utilizar en combinación con técnicas de ingeniería social para engañar a las víctimas para que entreguen las credenciales de su cuenta. La tecnología *deepfake* es todavía relativamente nueva, lo que significa que el riesgo de fraude de apropiación de cuentas basado en *deepfake* puede ser algo limitado en la actualidad. Sin embargo, puede suponer un riesgo significativo en el futuro si la tecnología sigue desarrollándose y está más disponible.

Caso 11. Robo de identidad remoto para control directo

En una serie de fraudes relacionados con el *phishing*, los delincuentes engañaron a las víctimas para que instalaran herramientas de acceso remoto en sus computadoras. En muchos de los casos, las cuentas se crearon con PSAVs a nombre de la víctima, sin su conocimiento. Los delincuentes lo hicieron utilizando datos robados a través de las herramientas de acceso remoto. También se sospecha que los delincuentes guiaron a las víctimas a través del proceso de apertura de cuentas de verificación en línea, utilizando las herramientas de acceso remoto para ocultar las interfaces reales.

Las víctimas finalmente fueron engañadas para transferir fondos a estas cuentas de PSAVs. Los delincuentes pudieron utilizar directamente estas cuentas para su posterior lavado. En total, se estima que las víctimas perdieron más de 600 000 euros.

Fuente: Austria

3. Otras vulnerabilidades emergentes de LA

37. Las medidas preventivas requeridas para las IF, las APNFDs y los PSAVs en virtud de los Estándares del GAFI (Recomendaciones 9 a 23) proporcionan una base para evitar que los ingresos del FC ingresen a los sectores financiero y de otro tipo. Esta sección se centra en las vulnerabilidades emergentes de LA que podrían ser explotadas por las organizaciones de FC.

3.1. Riesgos derivados de las IFs digitales[16]

38. La evolución de los pagos financieros ha dado lugar a la aparición de nuevas IF digitales, como los proveedores de servicios de pago (PSPs), la emisión de dinero electrónico, etc. Las IFs tradicionales pueden tener más recursos a su disposición, lo que puede dar lugar a controles relativamente más sólidos en comparación con estas nuevas IFs digitales. Esto puede conducir al desplazamiento, donde los delincuentes buscan explotar las vulnerabilidades de estos proveedores financieros alternativos para lavar fondos.

39. La red de pagos también puede estar fragmentada. Puede haber varias relaciones financieras anidadas entre estas instituciones, por ejemplo, con varias instituciones de pago que realizan transacciones entre sí o que proporcionan cuentas a proveedores más pequeños, que a su vez prestan otros tipos de servicios financieros (véase también el recuadro 17). Esta fragmentación también puede intensificar las dificultades para rastrear las transacciones entre varios tipos de instituciones en la "cadena de pagos". Esto también puede plantear dificultades a la hora de garantizar la disponibilidad inmediata de información básica sobre el originador y el beneficiario de las transferencias a lo largo de la cadena de pagos[17].

40. De acuerdo con los Estándares del GAFI, debe haber una supervisión regulatoria sólida sobre las IFs más nuevas, incluida la concesión de licencias o el registro adecuados, y evitar que los delincuentes o sus asociados controlen estas entidades. Las autoridades reguladoras deben asegurarse de que todas las instituciones que realizan transacciones tengan una supervisión suficiente sobre su respectivo perímetro: todas las instituciones tienen la responsabilidad de llevar a cabo o garantizar la debida diligencia del cliente (DDC) y el monitoreo de las transacciones en los nodos de ordenante y beneficiario.

[16] Este informe también reconoce los riesgos de LA que emanan de los AV y PSAVs. Para obtener más información sobre los riesgos regulatorios y los desafíos relacionados con los PSAVs, consulte GAFI (marzo de 2023) *Combate al financiamiento del ransomware* así como (junio de 2023) *Activos virtuales: actualización específica sobre la implementación de los Estándares del GAFI sobre activos virtuales y proveedores de servicios de activos virtuales*.

[17] El GAFI también está considerando posibles revisiones de la Recomendación 16 (sobre transferencias electrónicas) para tener en cuenta los desarrollos recientes y futuros en la arquitectura de los sistemas de pago.

Caso 12. Abuso en el sector de PSP

El análisis realizado por las autoridades de supervisión francesas en el primer semestre de 2021 identificó los principales PSP utilizados para recibir transferencias bancarias fraudulentas. Por lo general, estos principales proveedores de servicios de pago ofrecen "banca como servicio", y algunos tienen una sucursal en Francia con el único propósito de ofrecer IBANs franceses, con una presencia física mínima.

El análisis encontró que estos principales PSP eran aproximadamente 200 veces más riesgosos que otras instituciones. La mayoría de estos PSP tenían una verificación de identidad y un monitoreo de transacciones deficientes. Los delincuentes han abierto cuentas con una identidad mal utilizada y pueden comprobar rápidamente si algunas de las cuentas abiertas son identificadas como fraudulentas por el PSP, intentando primero realizar transacciones de pequeñas cantidades y cambiar el destino de los fondos si es necesario. A continuación, transfieren rápidamente los fondos adquiridos de forma fraudulenta a una o varias cuentas. Dividir los importes entre varias cuentas permite a los delincuentes eludir las restricciones impuestas por el PSP con respecto a sus servicios, como los límites de retiro de efectivo o permanecer por debajo del umbral de monitoreo de operaciones definido internamente por el PSP.

Fuente: Francia

3.2. Abuso del IBAN virtual[18]

41. Otro ejemplo de cómo se puede explotar la innovación financiera para los fines del FC es el uso de Códigos Internacionales de Cuentas Bancarias virtuales (vIBANs). Hay varias instituciones que emiten vIBANs a los clientes, incluidos los bancos y los PSP. Si bien los vIBANs se utilizan de muchas maneras legítimas diferentes, como facilitar y categorizar los pagos de múltiples partes, varias jurisdicciones han señalado el abuso de los vIBANs como una herramienta utilizada para el LA relacionado con FC.

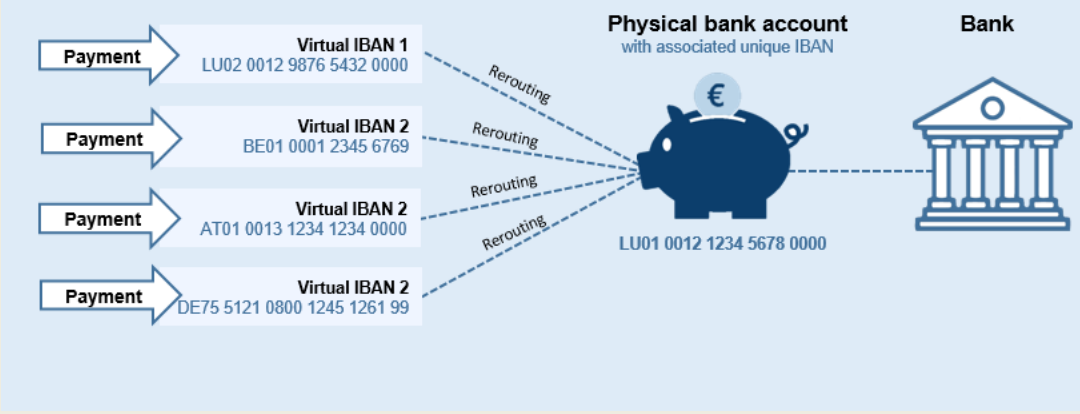
[18] Para obtener más información sobre los riesgos y desafíos asociados con los IBANs, consulte: (junio de 2023) *Información de inteligencia público-privada de Europol Financial Intelligence Public Private Partnership (EFIPPP) sobre IBAN virtuales (disponible solo para miembros de EFIPPP).*

Caso 13. ¿Qué es un vIBAN?

Los vIBAN son funcionalmente idénticos a los IBAN convencionales en el sentido de que se pueden utilizar para enviar y recibir pagos a escala global. Incluso tienen el mismo aspecto que su homólogo tradicional y también están compuestos por hasta 34 caracteres alfanuméricos. Por lo tanto, funcional y visualmente, son indistinguibles de los IBAN normales.

La diferencia clave entre los IBAN normales y los virtuales radica en la coincidencia de cuentas. Un IBAN normal se compara 1:1 con una cuenta bancaria, lo que significa que solo hay una cuenta bancaria física vinculada a cada número IBAN individual. Por lo tanto, si una persona utiliza un IBAN para realizar un pago, los fondos acabarán automáticamente en la cuenta bancaria a la que está vinculado el IBAN.

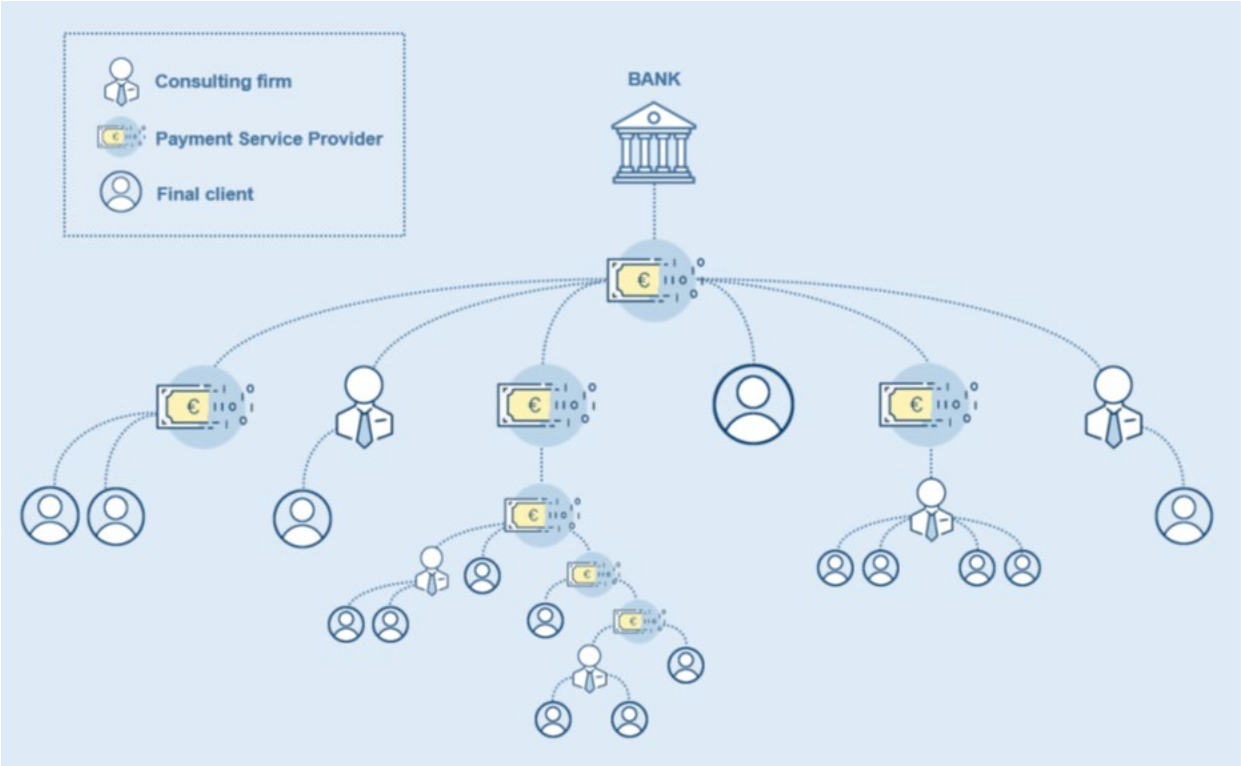
Por el contrario, un IBAN virtual es un número virtual que no coincide con una cuenta en un banco físico. Son números de referencia emitidos por el banco que permiten redirigir los pagos entrantes a un IBAN físico, que a su vez está vinculado a una cuenta bancaria física. No pueden tener fondos y su saldo es constantemente cero. Los titulares de vIBAN también pueden tener varios IBAN virtuales únicos, que redirigen y centralizan todos los pagos en una única cuenta bancaria física, como se ve en la Figura 3.



Fuente: Asociación público-privada de Europol Financial Intelligence

42. Dado que los IBAN y los vIBAN son ópticamente idénticos, los delincuentes los utilizan para engañar a las víctimas haciéndoles creer que están transfiriendo fondos a una cuenta bancaria, cuando en cambio, por ejemplo, podría ser un vIBAN utilizado con el fin de acreditar un monedero electrónico. Para complicar aún más las cosas, los vIBAN pueden ser reemitidos por el cliente de una institución financiera, especialmente si el cliente es otra institución financiera. Esto dificulta la identificación del país de origen del vIBAN y la ubicación de la cuenta maestra.

Figura2. Red en cascada de proveedores de vIBAN que emiten y reemiten vIBAN



Fuente: Europol Financial Intelligence Public Privâtes Partnership

43. En resumen, los delincuentes pueden abusar de los vIBANs para enmascarar la información final sobre los beneficiarios finales y ocultar el movimiento de dinero ilícito. Esto puede dificultar la identificación de dónde se encuentra la verdadera cuenta y la institución financiera emisora, así como garantizar un seguimiento adecuado de las transacciones. En última instancia, esto da lugar a dificultades para que las autoridades competentes localicen las cuentas físicas y congelen los fondos (ya que los vIBANs son simplemente números de referencia emitidos por los bancos y no cuentas reales que contienen saldos físicos). Como buena práctica, algunas jurisdicciones han trabajado con los bancos emisores de vIBANs para identificar rápidamente la entidad de pago vinculada a dichas cuentas maestras cuando se ha identificado el FC.

Caso 14. Se abusa de los vIBANs para el FC

Entre febrero y marzo de 2023, la UIF de Luxemburgo recibió varios informes de las estafas denominadas "Hola mamá", en las que las víctimas recibían mensajes de WhatsApp de un número de teléfono desconocido pero local de estafadores que se hacían pasar por su hijo. Las víctimas recibieron mensajes de texto en luxemburgués a través de números de teléfono móvil luxemburgueses, con la inclusión de un IBAN de Luxemburgo.

Durante la investigación de este caso, la UIF de Luxemburgo descubrió que los IBAN facilitados por los estafadores eran vIBANs. Estos vIBANs fueron emitidos por una entidad bancaria luxemburguesa a un proveedor de servicios de pago con sede en Luxemburgo que ofrece tarjetas de crédito de prepago a clientes europeos. Estas tarjetas de crédito prepago se pueden cargar transfiriendo dinero a los IBAN virtuales, que los delincuentes pretendían utilizar para seguir lavando ganancias ilícitas.

De los seis vIBAN identificados utilizados en la estafa, la UIF de Luxemburgo pudo bloquear o recuperar 40 000 EUR de los 55 000 EUR defraudados. La acción de la UIF se vio facilitada por la cooperación con el banco emisor de los vIBANs, que permitió identificar rápidamente a la entidad de pago titular de la cuenta subyacente del cliente final.

Fuente: Luxemburgo

3.3. Sectores no tradicionales

44. Muchas jurisdicciones destacaron la importancia de trabajar con sectores no tradicionales, incluidas las plataformas de redes sociales, el comercio electrónico, las telecomunicaciones y los proveedores de servicios de Internet, en el combate contra el LA relacionado con el FC. Si bien estos sectores no tradicionales no están regulados para la lucha contra el LA y el FT, poseen información útil que puede ayudar a avanzar en las investigaciones de LA, especialmente cuando se utilizan para perpetrar FC y reclutar mulas. Las plataformas de redes sociales, así como los proveedores de servicios de telecomunicaciones e Internet, pueden proporcionar información forense digital vital, incluidas direcciones IP, números de teléfono, direcciones de correo electrónico, etc., que pueden ayudar a identificar a los autores penales finales. Cuando se utilicen sitios web o anuncios fraudulentos para FC, estos sectores también poseerán información sobre transacciones financieras y pagos vinculada a los delincuentes (por ejemplo, detalles de pago para el alojamiento de sitios web, anuncios).

45. La experiencia y los estudios de casos de las jurisdicciones también han demostrado cómo se puede abusar del comercio electrónico o de las redes sociales, la transmisión o las plataformas de juegos como conducto para lavar los ingresos del FC. El uso generalizado de las redes sociales, el *streaming* o las plataformas de juegos permite a los usuarios recibir donaciones, regalos, *tokens* o créditos de los espectadores y del público. Los delincuentes pueden aprovecharse de la ausencia de requisitos en materia de lucha contra el LA y el FT y utilizar esas plataformas para lavar el producto del delito.

Caso 15. Las ganancias del *phishing* se lavan a través de las redes sociales y plataformas de streaming

Se descubrió que diecinueve cuentas bancarias habían sufrido pérdidas a través de un ataque de *phishing* dirigido a clientes de ciertos bancos. El análisis realizado por la UIF alemana reveló que las transacciones de estas cuentas bancarias se realizaban a través de cuentas de pago propiedad de dos usuarios. Posteriormente, estos fondos se enviaron a una red social y a una plataforma de *streaming*. Los fondos se utilizaron para recargar las cuentas de los usuarios en la plataforma de *streaming* con "monedas" (que sirven como un tipo de moneda nativa entre los usuarios de la plataforma) que se pueden utilizar para comprar regalos virtuales. Esos regalos se pueden transferir a los creadores de contenido que pueden convertir estas monedas en moneda regular y retirar el valor monetario equivalente.

Las investigaciones están en curso. Los datos de direcciones IP mostraron que las transacciones fraudulentas se realizaron a través de las mismas direcciones IP de inicio de sesión. El análisis de la UIF sugiere que un delincuente común está lavando gran parte de las ganancias del *phishing* a través de las redes sociales y la plataforma de *streaming* para cobrarlas posteriormente.

Fuente: Alemania

4. Respuestas y estrategias operacionales nacionales

46. En este capítulo se analizan en primer lugar las principales fuentes de información en las que se basan las jurisdicciones para detectar e investigar el FC. A continuación, se exploran las estructuras nacionales de coordinación y cooperación, y cómo las jurisdicciones aprovechan estas estructuras para investigar y prevenir el FC y el LA relacionado.

4.1. Fuentes clave de detección

47. Sobre la base de la experiencia de las jurisdicciones y los estudios de casos, existen dos fuentes principales de información para detectar e investigar el LA relacionado con el FC: la denuncia de las víctimas y los Reportes de Operaciones Sospechosas.

48. Las jurisdicciones también tienen varias iniciativas para mejorar la presentación de reportes con el fin de maximizar la cantidad total de información a la que pueden tener acceso para una aplicación efectiva. Con esta información y estos datos, las autoridades competentes aprovechan las estrategias y herramientas digitales para analizar e identificar los grupos delictivos con el fin de lograr una aplicación más eficaz y específica[19].

Denuncia de víctimas

49. La denuncia de las víctimas es una importante fuente de información para detectar e investigar el producto ilícito relacionado con el FC. En ciertos fraudes, como el fraude BEC y el *phishing*, las víctimas suelen descubrir con relativa rapidez que han sido estafadas (por ejemplo, cuando su contraparte legítima comienza a solicitar pagos atrasados). En otros tipos de casos de FC, como las estafas de inversión, el fraude romántico o el *phishing*, es posible que las víctimas solo se den cuenta de que fueron estafadas después de un tiempo.

50. La denuncia oportuna de las víctimas es importante para que las autoridades competentes puedan actuar con rapidez para rastrear el producto ilícito y puede aumentar la probabilidad de que se logren resultados satisfactorios en la aplicación de la ley. Las víctimas pueden denunciar presuntos delitos a lasLEAs, incluidas las unidades dedicadas a gestionar las denuncias de fraude. Las víctimas también pueden notificar a sus IFs, proveedores de pagos y PSAVs, sobre presuntas transacciones fraudulentas en sus cuentas. Otras jurisdicciones señalaron que las víctimas también podían dirigirse a los organismos de protección del consumidor financiero en lugar de a las LEAs.

51. Sin embargo, es probable que las víctimas no denuncien lo suficiente sobre el FC, especialmente cuando solo habían sufrido una pérdida insignificante. Junto con

[19] Para obtener más información sobre cómo las UIF y las Autoridades encargadas de la aplicación de la ley pueden aprovechar la transformación digital para lograr capacidades efectivas de análisis e investigación ALA/CFT, consulte Informes confidenciales sobre la transformación digital de ALA/CFT para autoridades operativas: Grupo Egmont-GAFI (octubre de 2021) *Detección de actividades sospechosas y análisis de inteligencia financiera (Fase 1);* y GAFI (mayo de 2022) *Autoridades encargadas de la aplicación de la ley e intercambio de información (Fase 2).*

factores emocionales, como la vergüenza o el miedo, las víctimas pueden decidir no denunciar.

52. Como una buena práctica para aumentar la denuncia de las víctimas, algunas jurisdicciones han creado plataformas específicas para que las víctimas denuncien el FC, incluidos portales en línea. Las plataformas pueden proporcionar un formato estructurado de denuncia para estandarizar la captura de datos, lo que facilita el análisis por conglomerados de las denuncias de las víctimas y puede ayudar a identificar tendencias y patrones delictivos. Las plataformas también pueden incluir recursos útiles para la prevención del FC y la asistencia a las víctimas.

Caso 16. *The Action Fraud* del Reino Unido

The Action Fraud es el centro nacional de denuncias de fraude y ciberdelincuencia del Reino Unido. Proporciona un punto de contacto central para el fraude y los delitos en Internet por motivos financieros y está dirigido por la Policía de la Ciudad de Londres, junto con la Oficina Nacional de Inteligencia contra el Fraude (ONIF). El sitio web de *The Action Fraud* proporciona varios recursos de divulgación pública para la prevención del delito, así como para la protección y el apoyo a las víctimas.

The Action Fraud también administra un portal de denuncia en vivo en línea las 24 horas del día, los 7 días de la semana para las víctimas. Los informes de fraude de acción se transmiten a la ONIF, que evalúa y analiza en diferentes partes del país para identificar a los autores finales. Estos informes se envían a las fuerzas policiales locales correspondientes en el Reino Unido para que las investiguen. La ONIF también utiliza estos informes para eliminar cuentas bancarias, sitios web y números de teléfono utilizados por los estafadores.

Fuente: Reino Unido

Reportes de Operaciones Sospechosas

53. Dada la posibilidad de que las víctimas no reporten, los ROS son una fuente independiente vital de detección de los flujos financieros relacionados con el FC.

54. Sobre la base de los datos recopilados de las UIF, la mayoría de los ROS relacionados con el FC fueron presentados por el sector bancario. No obstante, los bancos deben seguir reforzando sus capacidades para detectar el FC y el LA relacionado, ya que las organizaciones de FC evolucionan continuamente su *modus operandi*. Los datos también revelaron que los Servicios de Transferencia de Dinero (MVTS, por sus siglas en inglés) y los PSAVs presentan menos ROS. Esto último podría deberse al hecho de que en algunas jurisdicciones, el sector de PSAVs no está totalmente regulado de acuerdo con los Estándares del GAFI[20].

[20] Véase también GAFI (junio de 2023) *Activos virtuales: actualización específica sobre la implementación de las normas del GAFI sobre activos virtuales y proveedores de servicios de activos virtuales*.

55. Es importante garantizar un análisis oportuno de los informes relacionados con el FC, dada la posible disipación de los ingresos del FC. Algunas UIF despliegan un sistema de priorización para examinar el gran volumen de informes y centrarse en los de mayor riesgo, lo que incluye los informes relacionados con el FC. Otros capacitan a los funcionarios en sus UIF sobre los riesgos de LA relacionados con el FC, lo que les permite detectar y clasificar los informes entrantes relacionados con el FC. Todas estas medidas facilitan el análisis oportuno de la UIF, lo que permite a las fuerzas del orden hacer un seguimiento rápido de los incidentes de FC.

Caso 17. Priorización y agrupación de los ROS relacionados con el FC

La UIF de Chile recibió más de 1.500 ROS entre 2021 y 2022 relacionados con un esquema de fraude en plataformas comerciales en línea. Para hacer frente a este volumen, la UIF de Chile aplicó técnicas de *clustering* para el análisis y se descubrieron ciertos patrones a través de estos ROS.

La UIF aplicó una herramienta de minería de textos, utilizando palabras clave y frases conocidas detectadas. Posteriormente, se identificaron conglomerados geográficos, lo que permitió una remisión selectiva y combinada al Ministerio Público. La agrupación permitió a las investigaciones descubrir que los fondos se retiraban posteriormente a través de cajeros automáticos y luego pasaban a una persona de mayor jerarquía en el grupo de delincuencia organizada.

Fuente: Chile

56. Más allá de la detección, las jurisdicciones también han tratado de crear conciencia y mejorar la presentación de informes. Muchas jurisdicciones han emitido algún tipo de directrices relacionadas con el FC u organizado seminarios educativos para el personal de los bancos y otros sectores con el fin de promover el conocimiento en toda la industria de las últimas tendencias del FC y las tipologías de LA. Véase también en el anexo A una recopilación de indicadores de riesgo que pueden ayudar a mejorar la detección de FC. Las UIF de otras jurisdicciones han elaborado documentos de análisis estratégico sobre el FC. Estas iniciativas tienen como objetivo mejorar la detección y prevención de los delitos de FC y las actividades de LA por parte del personal bancario de primera línea, etc.

Caso 18. Análisis estratégico de las mulas relacionadas con el FC

Un análisis estratégico realizado por la UIF española se centró en comprender el perfil de una mula de dinero descubierta: cuentas bancarias abiertas por un solo individuo en tres o más IFs en un plazo de 20 días. Basándose en la información obtenida entre diciembre de 2020 y febrero de 2022 del Registro de Cuentas Bancarias (BAR), el estudio encontró casi 40,000 cuentas bancarias vinculadas a unas 10 000 personas. El 15% de las cuentas bancarias identificadas tenían coincidencias en las bases de datos de la UIF de España. Estas cuentas se clasificaron como de alto riesgo, y se puso en marcha un estudio piloto en

colaboración con cuatro IFs para reforzar la comprensión del perfil de riesgo basado en estas cuentas.

El proyecto piloto tenía por objeto prevenir el FC y otros posibles fraudes, así como mejorar la cooperación con el sector privado. El proyecto piloto también tenía por objeto reforzar la capacidad de las IFs para detectar lagunas en sus sistemas y obtener más información sobre el FC para detectar y prevenir nuevos delitos. En última instancia, el piloto también dio lugar a la implementación de un sistema de verificación cruzada para detectar de forma proactiva las redes de aprendizaje automático relacionadas con FC.

Fuente: España

4.2. Coordinación y colaboración a nivel nacional

Coordinación entre las autoridades competentes

57. Dada la naturaleza transversal del FC, existe una clara necesidad de una fuerte coordinación nacional entre los organismos. Algunas jurisdicciones han abordado la coordinación a través de un enfoque estratégico de todo el gobierno que guía las políticas relacionadas con el FC de una jurisdicción. Se trata de un órgano multifuncional global, integrado por ministerios clave de los sectores judicial, de la aplicación de la ley, regulatorios y de las comunicaciones de la información. El enfoque coordinado permite a las jurisdicciones identificar vulnerabilidades clave y diseñar respuestas políticas holísticas en todos los sectores clave.

58. La coordinación de las operaciones nacionales también puede involucrar a los organismos técnicos para impulsar la detección y la investigación. Esto incluye:

- Desarrollar canales de comunicación entre las UIF, la policía y los fiscales para garantizar la centralización de la presentación de informes, el intercambio racional de información y pruebas, así como las instrucciones para congelar e incautar activos. Esto también puede incluir el uso de clasificación automatizada de datos para ayudar a identificar posibles asuntos de interés e identificar rápidamente una LEA adecuada para la investigación. Esta coordinación también mitiga la duplicidad de los esfuerzos de aplicación de la ley, ya que los delincuentes de FC pueden atacar a las víctimas en varias partes de una jurisdicción (véase la sección sobre Delimitación adecuada de responsabilidades más adelante).
- Aprovechar a los expertos técnicos en ciberdelincuencia, en particular en relación con las intrusiones en la red y otros delitos de infraestructura técnica, así como a las agencias de protección de la privacidad. Esto refleja la naturaleza multifacética del FC y la relevancia de las pruebas forenses digitales (como direcciones IP, identificadores vinculados a dominios de Internet, etc.) para identificar las organizaciones de FC y avanzar en las investigaciones de LA.

Caso 19. Centro Conjunto de Coordinación de la Ciberdelincuencia Policial

La Policía Federal Australiana (AFP) dirige el Centro Conjunto de Coordinación de la Policía Cibernética (JPC3). Entre los miembros del JPC3 se encuentran las fuerzas del orden federales y estatales, los analistas del gobierno, incluido AUSTRAC, y los socios de la industria, como los analistas de los bancos australianos. El JPC3:

- Coordina la respuesta policial de Australia a la ciberdelincuencia de alto volumen y alto daño para maximizar el impacto en el entorno delictivo;
- Mejora el intercambio de inteligencia y el desarrollo de objetivos en la policía y la industria del Commonwealth, los estados y territorios;
- Coordina grupos de trabajo conjuntos con la policía y los socios de la industria para contrarrestar las amenazas prioritarias de la ciberdelincuencia;
- Proporciona coordinación nacional para el aumento de capacidades a través de la capacitación cruzada, la capacitación conjunta y el desarrollo de herramientas colaborativas; y
- Comunica a la industria y al público actividades coherentes a nivel nacional en materia de prevención, sensibilización y medios de comunicación.

El JPC3 tiene una capacidad de prevención que trabaja con la industria y el dominio público en la lucha contra el cibercrimen. Para respaldar eficazmente el JPC3, AUSTRAC también cuenta con un equipo de ciberdelincuencia financiera, que se centra específicamente en proporcionar inteligencia financiera sobre la delincuencia cibernética y la ciberdelincuencia dependiente con un nexo financiero, que incluye el LA del FC.

En enero de 2020, la AFP estableció la Operación DOLOS, que es un grupo de trabajo multiagencial[1] dirigido por la AFP que contrarresta a los ciberdelincuentes transnacionales que realizan o facilitan el BEC. La Operación DOLOS trabaja con australianos individuales y pequeñas y medianas empresas que han sido atacadas por BEC e interrumpe el flujo de ingresos hacia y desde las organizaciones que realizan BEC. Desde el comienzo de la Operación DOLOS, el grupo de trabajo desarrolló nuevas técnicas que redujeron el daño a los australianos y a las empresas. Entre el 1 de julio de 2022 y el 30 de junio de 2023, la Operación DOLOS ha evitado que se perdieran más de 30,6 millones de dólares australianos de víctimas australianas e internacionales al alterar el modelo operativo financiero utilizado por los delincuentes.

Fuente: Australia

1 El grupo de trabajo incluye varias agencias estatales y territoriales de policía, inteligencia y seguridad cibernética, la UIF, así como el sector financiero.

Asociaciones operacionales con el sector privado

59. Las jurisdicciones también han buscado colaborar con el sector privado a través de asociaciones público-privadas (APP). Estas APP pueden ayudar a mejorar los esfuerzos de detección, identificar redes de LA ocultas a través del intercambio de información táctica y mejorar la respuesta operativa de recuperación de activos.

Caso 20. Proyecto: Acciones Rápidas para Prevenir Estafas

La UIF de Sri Lanka ha puesto en marcha un proyecto, llamado "Acciones Rápidas para Prevenir las Estafas" (RAPS, por sus siglas en inglés), para actuar inmediatamente una vez que la víctima denuncia un posible FC. El objetivo es desbaratar las estafas en el sistema financiero de Sri Lanka, incluido el FC, reuniendo a las UIF y a los funcionarios encargados del cumplimiento de las IFs para detectar rápidamente las actividades ilícitas de las cuentas utilizadas por los delincuentes y sus cómplices.

El mecanismo consiste en identificar las credenciales de los estafadores en función de las denuncias públicas recibidas, y las credenciales de dichos estafadores se comparten con los oficiales de cumplimiento de las IFs. Sobre la base de esta información, las IFs supervisan las actividades de las cuentas de los posibles defraudadores y toman las medidas adecuadas para interrumpir el uso del sistema financiero a fin de evitar cualquier fraude. Además, la información de los estafadores se comparte con la Policía de Sri Lanka para llevar a cabo investigaciones sobre los sujetos.

Fuente: Sri Lanka

60. En vista del notable aumento de los FC, así como del riesgo asociado de LA, muchas jurisdicciones han establecido centros de respuesta centralizados en las LEAs o los reguladores para intensificar las acciones contra el FC y mejorar la concientización pública (véase también la sección sobre unidades anti-FC a continuación). Como buena práctica, los representantes de las IFs y los PSAVs podrían ubicarse en estos centros de respuesta centralizados, proporcionando acceso casi en tiempo real a los datos financieros y el rastreo en diversas entidades y sectores financieros, y acelerando la capacidad de las autoridades competentes para interceptar y congelar fondos.

Caso 21. Ubicación conjunta de los funcionarios bancarios

Arabia Saudita estableció una Sala de Operaciones Conjuntas (SOC) para los bancos. La SOC tiene la tarea de hacer un seguimiento y monitoreo de los casos de fraude financiero a los que pueden estar expuestos los clientes bancarios. La SOC reúne a todos los bancos e IF relacionadas bajo un mismo paraguas para hacer frente a los casos confirmados de fraude financiero.

La SOC es organizada por bancos de Arabia Saudita para facilitar los esfuerzos conjuntos para la estabilidad del sector bancario. Además, opera las 24 horas del día, los 7 días de la semana y tiene como objetivo proporcionar una cooperación e integración rápidas y efectivas entre todos los bancos sauditas para limitar el desarrollo de casos de fraude, así como proporcionar una respuesta rápida a las quejas de fraude y, cuando sea posible, tomar medidas inmediatas para evitar actos fraudulentos.

Fuente: Arabia Saudita

61. Estas asociaciones también proporcionan una plataforma útil para intercambiar las mejores prácticas y tipologías comunes y desarrollar conjuntamente medidas recomendadas para interrumpir la actividad ilícita.

Caso 22. Asociación Público-Privada "Inteligencia Financiera de Europol"

La Asociación Público-Privada de Inteligencia Financiera de Europol (EFIPPP, por sus siglas en inglés) es el primer mecanismo público-privado transnacional de intercambio de información para fines ALA/CFT. La EFIPPP reúne a las autoridades encargadas de la aplicación de la ley, las UIF y entidades privadas de varios países de la UE y de terceros países.

El Grupo de Trabajo de Amenazas y Tipologías dentro de la EFIPPP tiene líneas de trabajo dedicadas a diversos temas relacionados con FC y sus diferentes modus operandi, incluidos BEC, fraude de inversión, cuentas de mulas, IBAN virtuales y criptoactivos. Aunque el objetivo de la EFIPPP es crear reportes estratégicos de tipologías, también proporciona una plataforma para debatir la facilitación de la cooperación operativa entre sus miembros.

Fuente: Europol

62. La composición de las APP puede variar. Muchas jurisdicciones siguen centrándose en las partes interesadas tradicionales (en particular, los bancos y otras IF), pero hay una participación cada vez mayor de las APNFDs, los PSAVs y otros sectores no tradicionales (por ejemplo, los operadores de empresas de telecomunicaciones y los proveedores de servicios de Internet). La composición específica dependerá de las metas y objetivos de la APP.

Caso 23. Cooperación con el sector de las telecomunicaciones

En los últimos años, China ha seguido promoviendo el fortalecimiento de la lucha y la gestión del fraude en las redes de telecomunicaciones, y el 1° de diciembre de 2022 implementó oficialmente la "Ley contra el fraude en las redes de telecomunicaciones de la República Popular China", que ha proporcionado sólidas salvaguardias del Estado de Derecho para

combatir y frenar las actividades delictivas de fraude en las redes de telecomunicaciones y los actos delictivos relacionados.

La ley reúne a las autoridades del sector público (incluidos las LEA, los organismos financieros, de telecomunicaciones y de información de Internet), así como las IFs (bancos y proveedores de servicios de pago no bancarios), los operadores de empresas de telecomunicaciones y los proveedores de servicios de Internet para establecer un sistema de alerta temprana y disuasión. Este sistema identifica a las víctimas potenciales mediante una alerta temprana, lo que permite tomar medidas disuasorias adecuadas y oportunas.

Las IFs también pueden utilizar este sistema al abrir cuentas bancarias, cuentas de pago y prestar servicios de pago y liquidación. El sistema se utiliza para mejorar los procesos de diligencia debida del cliente y permite a las IFs tomar medidas de mitigación de riesgos para evitar que las cuentas bancarias y de pago, etc., se utilicen para actividades fraudulentas.

Fuente: China

4.3. Estrategias útiles de observancia a nivel nacional

63. En esta sección se examinan algunas buenas prácticas y estrategias útiles de aplicación de la ley que han sido empleadas por las jurisdicciones. En general, estas estrategias aprovechan las fuentes de información analizadas en la sección 4.1 anterior para identificar, investigar y prevenir el FC y el LA relacionado de manera más efectiva.

64. Estas útiles estrategias de aplicación de la ley suelen involucrar a múltiples agencias y entidades del sector privado. Esto significa que normalmente se requiere una fuerte coordinación y cooperación internas para implementar estas estrategias (como se discutió en la sección 4.2 anterior).

Delimitación adecuada de la responsabilidad

65. En los últimos años, muchas jurisdicciones han informado de un aumento de la cuantía de las pérdidas y del volumen de los casos de FC. Si bien algunos casos individuales pueden implicar pequeñas pérdidas, el volumen de tales estafas significa que el producto total del delito acumulado por cada organización es potencialmente grande.

66. Varias jurisdicciones indicaron que el gran volumen de informes del FC hacía necesario delimitar la responsabilidad de las investigaciones. Como buena práctica, las jurisdicciones con diversas agencias de lucha contra el fraude o la ciberdelincuencia que supervisan los casos de FC han tratado de identificar a la autoridad o autoridades competentes para manejarlos. Otras jurisdicciones introdujeron legislación para consolidar investigaciones complejas que involucran a múltiples víctimas de la misma organización, de modo que una sola autoridad competente supervise toda la investigación. Estas iniciativas evitan la duplicación de esfuerzos por parte de las diferentes autoridades competentes y evitan que los

casos "caigan por las grietas", así como para abordar la naturaleza transnacional del delito.

Caso 24. Uso de la tecnología para delinear la responsabilidad de la investigación

La Fuerza de Policía de Hong Kong (HKPF, por sus siglas en inglés) estableció el Centro de Procesamiento y Análisis de Delitos Electrónicos (e-Hub, por sus siglas en inglés) en septiembre de 2022 con el objetivo de mejorar la eficacia en el manejo de informes relacionados con delitos y engaños tecnológicos. El e-Hub utiliza un sistema informático mejorado para realizar análisis de correlación con tipos comunes de casos de fraude cibernéticos e identifica grupos de casos.

En 2022, el número de casos de fraude aumentó un 45,1% hasta los 27 923 casos, lo que representa casi el 40% del número total de delitos. Casi el 80% de los casos de fraude estaban relacionados con FC. Cada vez son más las personas que denuncian el FC en línea y la mayoría de los casos denunciados electrónicamente están correlacionados, por ejemplo, con el mismo grupo delictivo. Los casos correlacionados se asignan a un solo equipo de investigación para una investigación consolidada, de modo que los recursos puedan coordinarse mejor.

Mediante el uso de algoritmos de agrupación, e-HUB puede identificar patrones y similitudes en los datos que podrían no ser evidentes de inmediato para obtener una comprensión más profunda del alcance y la naturaleza de los casos. Esto incluye los tipos comunes de herramientas digitales delictivas y las cuentas de mulas de dinero utilizadas, y cómo se planifica, ejecuta y oculta el FC.

Fuente: Hong Kong, China

Unidades dedicadas anti-FC y LA relacionadas

67. Con el fin de fortalecer las capacidades de lucha contra el LA y el FT frente a la evolución del panorama penal, muchas jurisdicciones establecieron una unidad o grupo de trabajo específico para investigar el FC y el LA relacionado. Estas jurisdicciones asignaron recursos adicionales para fortalecer las capacidades de investigación financiera, recopilación de inteligencia y capacitación para las LEAs y el desarrollo de capacidades para el sector privado. Estas unidades centralizadas consolidan la experiencia anti-FC en todas las fuerzas del orden y las hacen más capaces de interrumpir las operaciones de FC, rastrear los fondos lavados y recuperar los ingresos relacionados.

68. Las jurisdicciones han compartido que los beneficios de un equipo de este tipo son múltiples. La consolidación de todos los casos de FC por una sola unidad de aplicación permite un mejor análisis, implementación de análisis de datos y análisis de enlaces de red para identificar organizaciones FC. Además, puede servir como un punto de contacto singular para las partes interesadas del sector privado y las contrapartes extranjeras, y ayuda a desarrollar relaciones estratégicas a largo plazo. Esto mejora los esfuerzos de intervención de las LEAs, como la interrupción de las

líneas telefónicas, la eliminación de alias y anuncios sospechosos en línea, y mejora los resultados de la recuperación de activos.

Caso 25. Centro Nacional de Respuesta a Estafas

El Centro Nacional de Respuesta a Estafas de Malasia (NSRC, por sus siglas en inglés), es una respuesta multifacética que reúne una amplia gama de recursos y conocimientos especializados del Centro Nacional de Lucha contra la Delincuencia Financiera, la Real Policía de Malasia (RPM, por sus siglas en inglés), el Banco Central y otras entidades de los sectores público y privado.

El NSRC sirve como un centro para la información sobre fraudes recibida de diversas fuentes y aprovecha el análisis de redes para identificar redes de mulas y LA. Las entidades del sector privado, incluidas las IsF, rastrearán los fondos de un nivel a otro y posteriormente retendrán las cuentas de mulas. La RPM investigará más a fondo el caso y tomará medidas coercitivas, como la emisión de una orden de congelación de las cuentas.

Fuente: Malasia

Mejora del acceso a la información financiera

69. Debido al efecto voluminoso e instantáneo de los casos de FC, el acceso oportuno a la información financiera y bancaria es crucial para acelerar la investigación y el rastreo de los ingresos del FC. Algunas jurisdicciones han empleado la tecnología para seguir el ritmo de los rápidos flujos de ingresos del FC, a menudo colaborando con el sector privado en el proceso. Otros se basan en registros centrales o desarrollan bases de datos para agilizar el proceso de recuperación de información. Estas buenas prácticas suelen basarse en la creación de una plataforma centralizada que reúna a múltiples partes interesadas para un intercambio de información más rápido.

- **Recuperación de información gracias a la tecnología:** Para que las IFs puedan proporcionar rápidamente información pertinente a las LEA, puede ser útil que las autoridades competentes de una jurisdicción se pongan de acuerdo sobre los campos de datos que serían pertinentes para sus investigaciones. La emisión de solicitudes variadas, cada una de las cuales requiere una respuesta personalizada de la institución financiera correspondiente, puede llevar mucho tiempo para que el sector privado la procese. Como buena práctica, las LEAs de algunas jurisdicciones han desarrollado una plantilla estandarizada que comprende campos de datos previamente acordados que exigen a las IFs. Las solicitudes pueden agregarse, enviarse a las IFs en lotes y estar en formato legible por máquina. Las IFs también pueden proporcionar respuestas a solicitudes legales de forma digital a las LEAs, lo que permite un análisis más eficiente de los datos.

Caso 26. Aprovechar la automatización robótica de procesos para acelerar el acceso a los registros financieros de las IF

El acceso oportuno a la información bancaria y financiera es fundamental para la interceptación y recuperación de activos eficaces. Singapur está aprovechando la automatización robótica de procesos (RPA, por sus siglas en inglés) para obtener información bancaria en una fracción del tiempo que tardaba antes. Los pedidos ahora se notifican electrónicamente a los bancos a través de una plantilla estandarizada. Los bancos automatizan el proceso de recuperación de información financiera y luego la envían de vuelta a las LEAs electrónicamente. Los datos electrónicos también se pueden utilizar inmediatamente para el análisis de la LEA.

El proceso ha mejorado el tiempo de respuesta hasta en un 97%, lo que lleva a investigaciones más eficientes. La información se proporciona ahora en formato digital, que está lista para su análisis. En cuanto a los bancos, esta iniciativa ha supuesto un importante ahorro de costes al eliminar los flujos de trabajo manuales. Del mismo modo, ha permitido la minería de datos para los bancos a través de sus procesos automatizados, que se pueden utilizar para detectar aún más redes de LA ocultas.

Fuente: Singapur

- **Facilitar el rastreo de activos entre las IFs:** Las transacciones de transferencia y el salto de cuenta entre varias IFs aumentan los esfuerzos de rastreo de las fuerzas del orden, ya que se requiere tiempo para recopilar información de las IFs respectivas, analizar las capas de transacciones e identificar el origen y el destino final de los fondos. Esto puede ser un desafío, dada la velocidad de las transacciones. Las buenas prácticas incluyen el desarrollo de plataformas para facilitar el rastreo rápido y el intercambio de información entre diferentes IFs para interceptar ganancias ilícitas.

Caso 27. Sistema de Gestión y Reporte de Fraude Cibernético Financiero Ciudadano (CFCFRMS)

El CFCFRMS es un sistema en línea desarrollado por el Centro de Coordinación de Delitos Cibernéticos de la India para informar rápidamente sobre fraudes cibernéticos financieros y prevenir el flujo de ingresos por fraude en los sectores financieros. El sistema ha integrado a las LEAs de todo el país y a las entidades financieras (es decir, bancos, billeteras, agregadores de pagos, vías de pago, plataformas de comercio electrónico, etc.) para trabajar en conjunto y tomar medidas inmediatas sobre las quejas reportadas en el CFCFRMS. En la actualidad, todas las LEAs estatales y territoriales de la Unión y 243 entidades financieras están incorporadas en el módulo.

Una vez que una víctima denuncia un fraude a la LEA, los detalles del beneficiario de la transacción fraudulenta se registran y se envían al sistema del CFCFRMS en forma de boleto. Este ticket se remite a la entidad financiera correspondiente (banco, billetera de pago, etc.), que verá el ticket en el panel de control de su sistema. La Entidad comprobará si el dinero defraudado sigue en la cuenta y la suspenderá. Si el dinero se ha disipado a otra entidad, el ticket se escala a la siguiente capa de entidad. El proceso se repite hasta que el dinero es interceptado. Si se retira el dinero, las IFs completan los detalles del retiro para que las LEAs tomen medidas adicionales.

El sistema ha sido muy eficaz para evitar que las transacciones fraudulentas caigan en manos de los estafadores. Desde su creación en abril de 2021, el sistema ha sido capaz de interceptar más de 6.020 millones de rupias (unos 66,1 millones de euros).

Fuente: India

- **Aprovechamiento de los registros centrales** Los registros de los bancos centrales permiten a las LEAs un acceso rápido a la información bancaria básica y ayudan a acelerar las investigaciones del FC. La información permite a las LEAs verificar los bancos en los que el sospechoso tiene cuentas o la identidad del titular de la cuenta. Esto ayuda a agilizar el proceso de recuperación de información al permitir que dichas autoridades delimiten sus investigaciones en una fase temprana y centrarse únicamente en las IFs en las que el sospechoso mantiene cuentas.

Caso 28. Identificación de cuentas de mulas ocultas

En Malta, se presentó una denuncia contra una presunta mula de dinero después de una serie de transacciones sospechosas a diferentes beneficiarios. Los fondos estaban siendo transferidos a varios bancos locales e internacionales vinculados a un presunto fraude romántico.

Las búsquedas en el Registro Nacional de Cuentas del Banco Central permitieron a la UIF identificar inmediatamente otra cuenta activa propiedad de la mula sospechosa en un banco diferente. La UIF pudo establecer rápidamente una imagen holística y el alcance de un análisis financiero adicional requerido. En última instancia, esto ayudó a la UIF a identificar rápidamente los puntos en común del LA posterior a otros individuos extranjeros.

Fuente: Malta

- **Desarrollo de bases de datos para el intercambio de información privada:** En los casos de redes profesionales de LA, muchas cuentas de mulas pueden ser conocidas o sospechosas como parte de estafas anteriores (por ejemplo, romance, lotería y empleo) o actividades de apropiación de identidad. También hay superposiciones similares en los datos y procesos

utilizados para identificar el fraude y los que se utilizan para identificar las redes de mulas. Como buena práctica, algunas jurisdicciones han tratado de centralizar los datos que atraviesan las bases de datos antifraude y de lucha contra el LA para identificar redes de aprendizaje automático más profundas en varias IFs con el fin de prevenir el fraude y fomentar la recuperación de activos.

Caso 29. Base de datos privada-privada centralizada

Brasil ha aprobado recientemente una Resolución que hace obligatoria una base de datos que centralice la información sobre el fraude (incluidos los intentos) por parte de todas las IFs y de pago. Esta base de datos es administrada por el Banco Central do Brasil (BCB) y se prevé que comience a operar en noviembre de 2023.

La Resolución establece que el intercambio de información sobre fraudes (incluidos los intentos) es obligatorio para las instituciones y define la información mínima que debe compartirse. Esto incluye la identificación de las personas involucradas en la comisión del fraude (incluidas las mulas de dinero), la(s) institución(es) financiera(s) involucrada(s) y la(s) cuenta(s) utilizada(s). El sistema tiene por objeto facilitar el intercambio de información entre el sector privado, con el objetivo de prevenir y combatir el fraude, así como recuperar el producto del fraude ilícito.

Fuente: Brasil

Disuadir a las mulas de dinero

70. Como se ha comentado anteriormente, las mulas de dinero desempeñan un papel importante en las redes de LA relacionadas con el FC. Las mulas se reclutan a través de múltiples técnicas. Dependiendo de cómo se les contrate y de si han sido engañados o explotados involuntariamente, pueden tener distintos niveles de conocimiento y participación en el esquema de FC subyacente (véase la sección 2.3 anterior).

71. En consecuencia, las autoridades competentes pueden tener dificultades para presentar cargos por LA. Puede ser difícil desarrollar pruebas suficientes para demostrar la intención criminal de la mula para llevar a cabo el LA (es decir, el nivel de conciencia sobre su participación en el proceso de LA). Para hacer frente a este problema, algunas jurisdicciones han promulgado leyes para reducir la *mens rea* requerida en el delito de LA, por ejemplo, de "conocimiento" a "sospecha".

Caso 30. Artículo 9, apartado 3, del Convenio de Varsovia del Consejo de Europa

Una de las cuestiones subyacentes en el enjuiciamiento efectivo de un delito de LA es la necesidad de probar *mens rea*, es decir, que el lavador de dinero sabía que los productos con los que operaba eran productos del delito. En casos complejos de LA en los que están involucrados lavadores de dinero profesionales, un acusado comúnmente niega que tuviera un conocimiento firme de que los fondos con los que operaba eran producto del delito. En consecuencia, demostrar que el "elemento mental" del acusado ha alcanzado el umbral pertinente es una de las tareas más difíciles para probar el delito de LA.

Conscientes de las dificultades para probar *la mens rea,* los redactores de la Convención de Varsovia introdujeron nuevos elementos en su artículo 9, donde se establece el delito de LA. Aparte de los elementos ya incorporados en los Convenios de Viena y Palermo, el artículo 9 del Convenio de Varsovia, en su párrafo 3, va un paso más allá al establecer que el delito de LA se produce incluso cuando el delincuente sólo sospechaba o debería haber supuesto que el producto era generado por el delito.

Fuente: MONEYVAL

72. Otras jurisdicciones han abordado el desafío que presentan las mulas de dinero generalmente a través de la educación pública y el alcance a las mulas potenciales. Las campañas mundiales en las redes sociales, como la campaña *#DontbeaMule,* apoyada por Europol y #YourAccountYourCrime de INTERPOL, pueden servir como plataformas útiles para coordinar la sensibilización internacional contra las actividades de las mulas de dinero, especialmente cuando los fondos pueden ser fácilmente lavados por mulas a través de las fronteras. La colaboración con el sector privado puede maximizar el efecto y los resultados de estos esfuerzos de divulgación. Las autoridades también pueden aprovechar los mecanismos de detección existentes (ROS y denuncias de las víctimas) para identificar posibles mulas de dinero que puedan haber manejado los ingresos del FC. Las actividades de divulgación y las advertencias específicas pueden aconsejar a esas mulas potenciales que se abstengan de repetir ese comportamiento en el futuro. Los registros de divulgación o advertencias pasadas pueden aprovecharse como evidencia útil para determinar la intención criminal de LA en caso de reincidencia.

4.4. Prevención y disrupción

73. Dada la rapidez con la que se disipan los fondos, muchas jurisdicciones han trabajado para explorar iniciativas para evitar que se produzcan FC y LA relacionados. Este enfoque reduce la rentabilidad general de las organizaciones de FC y mitiga significativamente la dedicación de recursos posteriores, desde la investigación hasta la gestión de las víctimas.

Educación pública y divulgación

74. Se puede adoptar un enfoque preventivo educando al público y aumentando la vigilancia contra la explotación, incluidas campañas nacionales de concientización que promuevan la alfabetización cibernética. Para apoyar este objetivo, algunas jurisdicciones han aprovechado la tecnología para poner en marcha campañas de información a los ciudadanos con el fin de ayudarles a detectar operaciones fraudulentas, concientizar sobre las señales reveladoras y fomentar la denuncia de las víctimas.

Caso 31. Aprovechar la tecnología para la educación pública en FC

La Fuerza de Policía de Hong Kong (HKPF, por sus siglas en inglés) lanzó el motor de búsqueda integral de estafas y trampas, "Scameter", en septiembre de 2022. La aplicación tiene como objetivo ayudar al público a identificar fraudes y trampas en línea.

Cuando el público se encuentra con llamadas sospechosas y vendedores en línea, solicitudes de amistad no solicitadas, mensajes de contratación arbitrarios, sitios web de inversión sospechosos de fraude y similares, pueden ingresar en *Scameter* el nombre o número de cuenta, el número de cuenta de pago, el número de teléfono, la dirección de correo electrónico, la URL, etc., de los presuntos estafadores para evaluar el riesgo de fraude y la seguridad cibernética.

Los datos y la calificación del *Scameter* provienen de varias fuentes confiables, incluidos informes públicos a la policía, información proporcionada por organizaciones, base de datos de números de teléfono sospechosos, así como la base de datos y el análisis en tiempo real de las empresas de seguridad de la información.

Fuente: Hong Kong, China

Seguridad y controles antifraude para los resultados de la lucha contra el LA y el FT

75. Las experiencias de los sectores público y privado comienzan a mostrar que los procesos antifraude y ALA son complementarios. Esto incluye aprovechar la tecnología para ayudar a los usuarios a rechazar automáticamente la recepción de mensajes fraudulentos, trabajar con el sector privado para el escaneo del horizonte a fin de mitigar de forma proactiva las tendencias de fraude emergentes, crear funciones, controles y reglas de seguridad de las cuentas, así como mensajes de advertencia en el software antivirus para posibles sitios de *phishing* (véase el Anexo B, que recopila buenos ejemplos de cómo los reguladores financieros han adoptado requisitos antifraude junto con los controles ALA/CFT).

76. Otra buena práctica es alentar a las IFs a adoptar el monitoreo de transacciones en tiempo real para identificar y prevenir actividades fraudulentas o ilícitas en tiempo real. Al monitorear la información anormal del titular de la cuenta (por ejemplo, direcciones físicas, IP y de correo electrónico, números de teléfono móvil, etc.) y las transacciones en tiempo real, las IFs pueden identificar, investigar y reportar rápidamente cualquier actividad inusual o sospechosa.

77. El monitoreo de transacciones en tiempo real, que implica el uso de software y algoritmos sofisticados para monitorear transacciones financieras, se considera útil para detectar y prevenir el FC. Dado el desbordamiento de información causado por la digitalización, el FC puede ser difícil de detectar a través de procesos manuales. El monitoreo de transacciones en tiempo real puede ayudar a las IFs a identificar e investigar patrones de actividad sospechosa en múltiples cuentas o transacciones, incluso si esas cuentas o transacciones no están directamente vinculadas, lo que evita futuros delitos[21].

Eliminación de instrumentos delictivos

78. Dado que el FC también puede perpetrarse a través de sectores no tradicionales (véase la sección 3.3.), algunas jurisdicciones han reforzado la prevención y los controles de lucha contra el fraude en esos sectores no tradicionales. Esto incluye atacar los instrumentos de FC, como el cierre de las líneas móviles y las páginas web fraudulentas utilizadas por los delincuentes, el filtrado de mensajes de *phishing* y enlaces web maliciosos, etc.

[21] Para obtener más información sobre cómo se puede utilizar la tecnología para el combate contra el LA y el FT, consulte también el GAFI (julio de 2021) *Oportunidades y desafíos de las nuevas tecnologías para la lucha contra el lavado de activos y el financiamiento del terrorismo.*

Caso 32. Eliminación de sitios web sospechosos y campañas de *phishing*

En Arabia Saudita, las LEAs y las autoridades reguladoras adoptan un enfoque de colaboración con los proveedores de telecomunicaciones para mejorar significativamente su capacidad de predecir, prevenir, detectar y responder a eventos fraudulentos de manera efectiva. Para combatir los instrumentos delictivos, la Autoridad Nacional de Seguridad Cibernética de Arabia Saudita ha impuesto estrictos requisitos de protección de marca centrados en contrarrestar los sitios web clonados y los mensajes de *phishing* en las plataformas sociales. Además, el Banco Central de Arabia Saudita (SAMA, por sus siglas en inglés) ha establecido un sólido marco de ciberseguridad y lucha contra el fraude, respectivamente, que describe los requisitos obligatorios de control de referencia para las entidades reguladas. Este marco tiene como objetivo proteger de forma proactiva contra las amenazas de fraude emergentes, garantizando así la estabilidad y la salvaguardia del sector financiero del reino.

Un aspecto crucial de estos requisitos nacionales y reglamentarios es la supervisión proactiva de los instrumentos delictivos por parte de las organizaciones. Esto implica una vigilancia continua de posibles actividades fraudulentas, como sitios web sospechosos y campañas de *phishing* a través de tecnologías sofisticadas y medidas de protección de marca implementadas por las organizaciones. Cuando se detectan, estas actividades se informan rápidamente a las autoridades pertinentes. La notificación oportuna garantiza una acción rápida para investigar y cerrar las operaciones delictivas, evitando más daños y reduciendo el impacto de los eventos fraudulentos.

Fuente: Arabia Saudita

Prevención de la disipación de activos

79. Muchas jurisdicciones han descubierto que uno de los aspectos más desafiantes de las investigaciones del FC es la rápida velocidad a la que se pueden lavar los ingresos del FC. Existe consenso en que es fundamental que las autoridades competentes puedan intervenir rápidamente para alcanzar los ingresos del FC antes de que se disipen de las distintas cuentas bancarias. Las jurisdicciones han aplicado diversas medidas para recuperar de manera más eficaz los activos vinculados al FC (véase la sección 5.1).

80. También puede ser beneficioso involucrar a representantes clave del sector financiero privado para facilitar y alentar su interceptación proactiva de fondos ilícitos una vez que se recibe una notificación de fraude de un cliente víctima, antes de que las autoridades competentes se hayan puesto en contacto con él. Esto incluye los intercambios de información entre IFs o PSAVs nacionales y extranjeros (véase también el recuadro 41).

Caso 33. Boletín del Grupo Egmont sobre el fraude BEC

En julio de 2019, el Grupo Egmont emitió un boletín para alertar a las UIF miembros y a sus jurisdicciones sobre la creciente amenaza que representa el fraude BEC a través del intercambio de escenarios clave e indicadores de riesgo vinculados a BEC. El boletín identificó además cómo las IFs pueden desempeñar un papel importante en la identificación, prevención y denuncia del fraude BEC mediante la promoción de una mayor comunicación y colaboración entre sus unidades internas de lucha contra el LA, negocios, prevención del fraude y ciberseguridad.

Para ayudar en la investigación de los incidentes BEC y la recuperación de los fondos de las víctimas, se aconsejó a las IFs beneficiarias que recibieron información de que se había ejecutado una transferencia fraudulenta a una de las cuentas de sus clientes (por ejemplo, un mensaje de recuperación de *SWIFT*) que no realizaran ninguna transacción que pudiera conducir a la pérdida de fondos y que se pusieran en contacto con las LEAs o la UIF para evaluar la validez de la transacción recibida.

Fuente: Grupo Egmont

5. Cooperación internacional y recuperación de activos

81. Como ya se ha señalado previamente, la jurisdicción en la que se produce el FC (es decir, en la que generalmente se encuentra la víctima) tiende a ser diferente de la jurisdicción en la que se lava el producto. Esto puede dar lugar a dificultades en las investigaciones transfronterizas y a una cooperación internacional eficaz para obtener con éxito información y pruebas, desmantelar las organizaciones sindicales del FC y recuperar las ganancias ilícitas. Por ejemplo, una jurisdicción en la que se han lavado los ingresos relacionados con el FC puede tener dificultades para identificar a todas las víctimas asociadas a una cuenta de LA, ya que pueden estar repartidas en varias jurisdicciones.

82. La naturaleza descentralizada del FC añade más complejidad. Puede haber discrepancias en las respectivas prioridades de cooperación internacional de las jurisdicciones, por ejemplo, en los casos en que las víctimas de la Jurisdicción A transfieren dinero a la Jurisdicción B, pero las víctimas de la Jurisdicción B se encuentran ubicadas en la Jurisdicción C (es decir, lo que significa que A puede priorizar la colaboración con B, pero B puede priorizar la cooperación con C). La necesidad de involucrar a múltiples partes interesadas y socios, tanto públicos como privados, en el extranjero también dificulta la identificación y el rastreo de fondos ilegales.

    - Las organizaciones de FC utilizan diversos servicios financieros y clases de activos. Las transacciones se pueden realizar casi instantáneamente a través de las fronteras entre diferentes proveedores y sectores. Esto hace que las transferencias de fondos sean difíciles de rastrear y atribuir.
    - También es probable que las pruebas forenses digitales pertinentes se distribuyan en diferentes jurisdicciones, lo que dificulta la reconstrucción de una imagen completa de cómo operan y lavan las ganancias de las organizaciones delictivas. Esto se complica aún más por las características volátiles de la evidencia forense digital, que puede disiparse fácilmente si no se conserva rápidamente.

83. La cooperación formal, incluida la Asistencia Legal Mutua (ALM), suele llevar mucho tiempo. Dada la naturaleza rápida de los delitos digitales y las actividades de LA asociadas (donde las pruebas podrían disiparse rápidamente si no se conservan), confiar en la cooperación formal puede ser significativamente menos eficaz. Con el fin de seguir prestando asistencia transfronteriza para frenar con éxito la actividad delictiva del FC, las autoridades competentes recurren cada vez más a mecanismos informales de cooperación mediante el intercambio de información directamente con sus homólogos extranjeros. Esto puede ocurrir a nivel de las LEAs o de la UIF a través de diversos canales, como la Red Segura de Egmont (ESW, por sus siglas en inglés), la I-24/7 de INTERPOL, así como otras redes informales como la Red Interinstitucional de Recuperación de Activos de Camden (CARIN) y las Redes Interinstitucionales Regionales de Recuperación de Activos (ARINs).

Caso 34. Interceptación de los ingresos del FC a través de redes multilaterales informales

Para luchar contra el aumento del FC, las autoridades de investigación francesas recurren activamente a redes informales, entre las que se encuentra la subred de Oficinas Europeas de Recuperación de Activos (AROs) de CARIN para una cooperación internacional eficaz y la correspondiente recuperación de activos. La AROs francesa trabaja en estrecha colaboración con los miembros de estas dos redes, que permiten el intercambio rápido de información a través de múltiples jurisdicciones entre las contrapartes de las LEAs y la UIF especializadas en el rastreo, la incautación y el decomiso de activos delictivos, especialmente en casos de emergencia en los que las solicitudes se responden en un plazo de 8 horas. Esta cooperación permite que los fondos se conserven rápidamente en la cuenta de destino identificada inicialmente y en todas las demás cuentas estratificadas posteriores.

En 2022, por ejemplo, la AROs francesa se puso en contacto con la AROs eslovaca en relación con una transferencia bancaria fraudulenta por valor de 1 875 000 EUR en detrimento de una empresa víctima francesa y solicitó que los fondos se congelaran en la cuenta bancaria del beneficiario en Eslovaquia. Los intercambios entre las dos AROs dieron lugar a la congelación de los fondos y permitieron a las autoridades eslovacas obtener toda la información necesaria para elaborar y ejecutar una solicitud de congelamiento judicial. Al final, la suma de 1.874.907 libras esterlinas fue congelada y posteriormente devuelta a la empresa víctima.

Fuente: Francia

84. A fin de maximizar la eficacia en la investigación del LA relacionado con el FC y la recuperación de los activos, la cooperación debe tener un enfoque multilateral en lugar de bilateral. En esta sección se examinan los desafíos y las buenas prácticas en relación con la cooperación internacional a través de dos resultados operacionales: i) la recuperación de activos y ii) la aplicación de la ley y el enjuiciamiento.

5.1. Recuperación de activos

85. Un reto clave en la recuperación de activos del FC es el rápido ritmo del LA. Para mitigar este problema, existen programas multilaterales de "respuesta rápida" creados por diversos organismos para rastrear y recuperar los ingresos procedentes del FC, como el Programa Mundial de Intervención Rápida de Pagos (I-GRIP) de INTERPOL, el proyecto BEC del Grupo Egmont y la cadena de eliminación del fraude financiero de los Estados Unidos. La experiencia de estos organismos muestra generalmente que la intervención es más eficaz dentro de las 24 a 72 horas posteriores a una transacción fraudulenta. Estas buenas prácticas mitigan el riesgo de que los fondos se disipen en múltiples capas posteriores, lo que reduce drásticamente el alcance de la investigación de LA y facilita la recuperación de las ganancias ilícitas.

Caso 35. Equipo de Recuperación de Activos y Cadena de Eliminación del Fraude Financiero

La Cadena de Eliminación del Fraude Financiero (FFKC, por sus siglas en inglés) fue creada por el FBI y la Red de Control de Delitos Financieros (FinCEN) (UIF de EE.UU.) en 2016 en respuesta al aumento de los esquemas de BEC. La FFKC intenta ayudar en la recuperación de las transferencias electrónicas internacionales enviadas de conformidad con esquemas de fraude aprovechando las relaciones de FinCEN con el Grupo Egmont de Unidades de Inteligencia Financiera. Este proceso solo se puede implementar si la transferencia bancaria fraudulenta cumple con los siguientes criterios: (1) la transferencia bancaria es de USD 50 000 o más; (2) la transferencia bancaria es internacional; (3) se ha iniciado un aviso de retirada de SWIFT; y (4) la transferencia bancaria se ha producido en las últimas 72 horas.

En 2018, el Centro de Denuncias de Delitos en Internet (IC3) del FBI estableció el Equipo de Recuperación de Activos (RAT, por sus siglas en inglés) para abordar las vulnerabilidades en las transferencias electrónicas nacionales. El RAT agiliza la comunicación con las IFs y ayuda a las oficinas de campo del FBI con el congelamiento de fondos para transferencias nacionales realizadas bajo pretextos fraudulentos. El RAT ha experimentado una serie de éxitos notables, congelando el 73% de los fondos reportados como fraudulentos al IC3 (USD 433,3 millones de USD 590,62 millones) hasta la fecha. De acuerdo con un ejemplo de caso en los Estados Unidos, este programa puede, en algunos casos, identificar rápidamente las cuentas de segundo salto y congelar los fondos, lo que hace posible una recuperación completa.

Fuente: Estados Unidos

86. Principalmente, estos programas multilaterales tienen por objeto hacer dos cosas: reunir el nivel mínimo de información necesario para la acción de las LEAs y pasar esa información a las "manos correctas". Para garantizar una respuesta transfronteriza eficaz, todos los nodos de las redes multilaterales también acuerdan normas y procedimientos de gobernanza. Si bien esas redes multilaterales suelen ser de carácter global, las iniciativas regionales también pueden ser útiles para mitigar los desafíos aprovechando la colaboración regional ya establecida.

Caso 36. Proyecto Antifraude Multijurisdiccional

Dada la naturaleza transfronteriza del fraude, se desarrolló una iniciativa regional dentro del Grupo Consultivo de Inteligencia Financiera (FICG por sus siglas en inglés)[1] denominada Proyecto Multijurisdiccional de Lucha contra el Fraude. Esta iniciativa está codirigida por las UIF de Malasia, Indonesia y Singapur, y tiene como objetivo detectar, rastrear y recuperar fondos para las víctimas.

Se construyó un mecanismo de respuesta que involucra transacciones transfronterizas entre los países miembros del FICG. Este proyecto ayudará a los miembros del FICG a compartir información de inteligencia financiera de forma rápida y sencilla, apoyando así las acciones rápidas de las autoridades para combatir el fraude y recuperar el dinero robado.

Fuente: Malasia

1 El GCIF es un organismo regional de UIF del Sudeste Asiático, Nueva Zelandia y Australia.

Recopilación e intercambio transfronterizos de información: "recopilar un nivel mínimo de información"

87. Cuando el FC se considera un delito grave con arreglo a la legislación nacional, debe tipificarse como delito determinante para el LA en virtud de la Recomendación 3 del GAFI. Además, a diferencia de las formas tradicionales de fraude cometidas entre conocidos, en las que es difícil distinguir el fraude de las posibles controversias civiles entre deudores y acreedores, es relativamente más fácil establecer la criminalidad *prima facie* en los casos de FC, en los que el fraude suele producirse entre desconocidos. Esto mitiga la necesidad de una larga solicitud de asistencia para articular y definir el nexo penal, como suele ser necesario para otros tipos de delitos (que no son universalmente reconocidos como delitos determinantes).

88. Como buena práctica, los diversos programas de respuesta rápida utilizan plantillas para acelerar la recopilación y el intercambio de información. Las plantillas permiten la recopilación rápida de un nivel mínimo de información requerido para establecer la criminalidad. Esto ayuda a centrar los esfuerzos de las unidades de respuesta terrestre en los tipos vitales de pruebas o información que se deben proteger en las etapas iniciales de una denuncia penal. Estas plantillas también mitigan los desafíos en la calidad de la información intercambiada y mejoran la respuesta transfronteriza de las fuerzas del orden.

89. Además de un resumen para describir el delito del FC, las plantillas generalmente buscan asegurar los datos básicos necesarios para avanzar en los esfuerzos de rastreo de fondos. La estandarización de las solicitudes permite a las jurisdicciones requeridas procesar rápidamente cualquier solicitud entrante, lo que acelera la capacidad de las LEAs para interceptar fondos ilícitos que han ingresado a su jurisdicción.

90. Los campos de datos de las plantillas pueden incluir información de la cuenta del originador y del beneficiario, así como información de la transacción (fecha, hora, importes transferidos). Para mejorar aún más la eficacia, las plantillas también podrían incluir información sobre el próximo destino de los fondos si los fondos ya se han transferido de la cuenta del beneficiario. También puede ser útil reducir al

mínimo las restricciones impuestas a las jurisdicciones para difundir cualquier información que se intercambie con las autoridades competentes pertinentes a nivel nacional en el momento de su recepción.

Caso 37. INTERPOL I-GRIP

INTERPOL ha desarrollado el programa de Intervención Global Rápida de Pagos (I-GRIP), que es un mecanismo mundial de suspensión de pagos que permite a los países miembros presentar y tramitar solicitudes de seguimiento, interceptación o congelamiento provisional de los ingresos ilícitos del FC. Conocido como I-GRIP, el mecanismo se puso a prueba originalmente como el Protocolo de Respuesta Rápida contra el LA (ARRP, por sus siglas en inglés) en 2022 y se lanzó oficialmente en noviembre de 2022 gracias a muchos casos de éxito de suspensión de pagos durante la fase piloto.

I-GRIP facilita una comunicación rápida entre las Oficinas Centrales Nacionales (NCBs, por sus siglas en inglés) de INTERPOL para evitar la transferencia de activos presuntamente ilícitos entre los países miembros. Las solicitudes presentadas a través de I-GRIP deben incluir detalles suficientes sobre los que pueda actuar la NCB receptora, tales como: – Fecha de la operación, moneda e importe, números de cuenta y nombres de las IFs de las cuentas beneficiaria y remitente.

Fuente: INTERPOL

91. Además, los campos de datos estandarizados en las plantillas permiten a las organizaciones internacionales con capacidades centralizadas analizar fácilmente los datos y maximizar los esfuerzos de investigación y recuperación de activos. Por ejemplo, INTERPOL aprovecha la información intercambiada a través de sus canales para crear una base de datos interna, el Fichero Analítico de Delitos Financieros (FINCAF, por sus siglas en inglés), para facilitar el análisis de información de inteligencia con una dimensión transnacional sobre diversas formas de delitos financieros y para identificar vínculos entre los casos transfronterizos y las investigaciones, las amenazas, las tendencias delictivas y las redes delictivas (véase también el recuadro 45).

92. Para acelerar aún más las acciones de recuperación de activos, algunas jurisdicciones han permitido que las víctimas extranjeras presenten una queja de FC directamente ante sus LEAs, incluso a través de su plataforma de informes en línea para capturar directamente los campos de datos necesarios para la acción de cumplimiento (consulte la sección sobre Denuncias de las víctimas más arriba). Esto elimina una capa adicional de comunicación y permite a las autoridades competentes adoptar rápidamente las medidas disponibles contra las transacciones sospechosas realizadas a las cuentas de los beneficiarios en sus jurisdicciones.

Poderes necesarios para actuar: "las manos correctas"

93. Dado que la velocidad es esencial, lo ideal es que cualquier información recopilada se entregue directamente a las autoridades que ya están equipadas con el poder y la experiencia adecuados para el rastreo y la recuperación de activos. Esto permite

que se adopten medidas provisionales inmediatamente después de recibir una solicitud para evitar que se siga lavando o disipando activos. Esto proporciona a las LEAs el tiempo vital necesario para continuar sus investigaciones, desarrollar y reunir pruebas y hacer un seguimiento de las solicitudes formales de combate al LA.

Caso 38. Solicitud de aplazamiento a la entidad regulada

La UIF de Italia recibió una solicitud de aplazamiento de una entidad regulada en relación con cuatro transferencias electrónicas sospechosas por un importe de 490 000 EUR. Las transacciones fueron ordenadas por una empresa italiana de comercio al por mayor de prendas de vestir a favor de varias empresas en un país del Lejano Oriente Asiático.

La entidad regulada había considerado que las cuatro transacciones eran sospechosas, ya que los fondos procedían de transferencias entrantes que estaban siendo retiradas por el banco ordenante sobre la base de que los fondos se habían enviado debido a un "fraude del director general" de una empresa víctima de Europa occidental. La UIF de Italia también había recibido un intercambio internacional espontáneo de información de la UIF de ese país de Europa occidental. La empresa italiana también fue denunciada ante la UIF por su posible conexión con esquemas de fraude del IVA que involucraban a dicho país asiático a través de un país separado de Europa del Este, lo que proporcionó más indicios de vínculos entre FC y otros tipos de delincuencia organizada.

Las transacciones se pospusieron con éxito. Esto permitió a las autoridades extranjeras emitir una orden extranjera de incautación para recuperar los fondos en Italia.

Fuente: Italia

94. Sin embargo, esta interfaz directa puede encontrar desafíos debido a las diferencias en los marcos legislativos y de aplicación entre las jurisdicciones. Algunas buenas prácticas para mitigar estos desafíos incluyen el establecimiento de mecanismos de coordinación nacional para facilitar la transmisión de solicitudes a las autoridades correctas, así como el aprovechamiento de los canales de colaboración público-privada y la capacidad de las IFs para adoptar voluntariamente medidas provisionales una vez que las autoridades competentes les informan de transacciones sospechosas.

Gobernanza y Normas: "el Convenio Colectivo"

95. La gobernanza y las normas de los marcos multilaterales ofrecen garantías y el compromiso de reconocer mutuamente la actividad delictiva y actuar con rapidez al recibir la información. Esto ayuda a superar el problema de que puede haber un desajuste de prioridades entre los organismos internacionales, ya que las condiciones para adherirse y prestar asistencia se han acordado de antemano. Como buena práctica, estas reglas y criterios deben ser claros y fáciles de entender.

96. Los principios anteriores se aplican a los mecanismos informales de cooperación internacional, pero también a los formales. Como buen ejemplo, el Reglamento (UE) 2018/1805 del Parlamento Europeo y del Consejo, permite el reconocimiento

mutuo de las resoluciones extranjeras de congelamiento y decomiso. Este mecanismo de ejecución directa permite una rápida intervención transfronteriza.

97. El intercambio acelerado de información no debe ir en detrimento de la protección de datos y la confidencialidad. Para garantizar la seguridad de la información transmitida, los marcos multilaterales suelen aprovechar los canales seguros de comunicación existentes, como los proporcionados por INTERPOL, Europol y el Grupo Egmont. Estos canales de comunicación seguros existentes también permiten que estos marcos multilaterales se amplíen fácilmente, ya que eluden la necesidad de desarrollar canales de comunicación bilaterales.

Caso 39. El equipo del proyecto Egmont BEC

Para hacer frente a la creciente y grave amenaza que representa el BEC para las IFs y sus clientes, 11 UIF pusieron en marcha el "Equipo del Proyecto Egmont BEC", que se centró en el análisis de las tendencias, los indicadores y las metodologías de BEC, así como en compartir las principales conclusiones con las UIF. Las tipologías financieras comunes de BEC y los estudios de casos muestran que una reacción rápida para detener y seguir las transferencias bancarias es la forma más efectiva de abordar este tipo de delito.

Como tal, el Equipo del Proyecto[1] establece protocolos entre las LEAs y las UIF, y entre las UIF internacionales para seguir y congelar los ingresos del BEC.

- Al recibir un reporte relativo a presuntos flujos BEC transfronterizos, la UIF originadora elabora una solicitud de "respuesta rápida" a la UIF de destino.
- La solicitud debe contener los datos básicos acordados y la información necesaria para el intercambio de medidas coercitivas.
- Se solicita a la UIF de destino que adopte (cuando sea posible) medidas inmediatas para suspender y recuperar el producto ilícito, idealmente dentro de las 72 horas posteriores a la ocurrencia del delito.

El proyecto BEC aprovecha la plataforma segura de comunicaciones del Grupo Egmont para intercambiar las solicitudes de "respuesta rápida".

Fuente: Grupo Egmont

1 En la actualidad, los miembros del equipo del proyecto son: AUSTRAC (Australia), BFIU (Bangladesh), CTIF-CFI (Bélgica), TRACFIN (Francia), GHFIU (Ghana), HFIU (Hungría), IMPA (Israel), SIC (Líbano), FIU Luxemburgo, UPWBNM (Malasia), FinCEN (EE. UU.) y Europol.

5.2. Aplicación de la ley y enjuiciamiento

98. Más allá de la recuperación de activos, el carácter transnacional del FC también ha dado lugar a dificultades en todo el proceso de ejecución, desde la recopilación de información y la investigación hasta la recopilación de pruebas para el enjuiciamiento. La evolución de la tecnología ha aumentado la velocidad de las transacciones y ha facilitado la fragmentación de las operaciones transfronterizas. También ha aumentado el tiempo y el esfuerzo necesarios para que las LEAslos rastreen e identifiquen.

Recopilación de evidencias digitales

99. Si bien no está relacionada exclusivamente con el aprendizaje automático, la evidencia forense digital puede proporcionar pistas críticas para dirigir a las LEAs a avanzar en sus investigaciones de aprendizaje automático. La amplia

disponibilidad y facilidad de uso de los servicios de ocultación de identidad, como la VPN, complica aún más los esfuerzos para localizar a los autores finales de FC.

100. Desafortunadamente, actualmente no existe un régimen global único que rija la duración de la retención de datos digitales, incluso en relación con los proveedores de servicios técnicos. Varias jurisdicciones destacaron el importante riesgo de disipación de pruebas digitales. Los retrasos en los mecanismos formales de cooperación también supondrían un reto a la hora de asegurar rápidamente las pruebas digitales.

101. Hay varias buenas prácticas que pueden mitigar estos desafíos.

- **Aprovechar los canales informales** para recopilar y asegurar primero la inteligencia. A partir de entonces, se utilizan canales formales de cooperación para obtener las pruebas y declaraciones necesarias para la preparación de los procedimientos judiciales.
- **Las convenciones y las herramientas de investigación,** como la Convención sobre el Delito Cibernético, también conocida como Convención de Budapest, permiten la preservación rápida de los datos electrónicos y la transmisión de información espontánea, lo que ayuda a acelerar la identificación de los autores finales del FC. El Convenio de Budapest también establece una red 24/7 que garantiza la asistencia inmediata en materia de investigación para la prestación de asesoramiento técnico, la recopilación de pruebas, la conservación de datos, etc.
- **Cooperación directa** con proveedores de servicios extranjeros para obtener las pruebas forenses necesarias, como la información de los suscriptores, sin pasar por el proceso de ALM. Según una jurisdicción, la cooperación voluntaria directa de un proveedor de servicios extranjero es el mecanismo más eficaz para reunir pruebas digitales pertinentes[22].

[22] Véase también Consejo de Europa (julio de 2020) *El Convenio de Budapest sobre la Ciberdelincuencia: beneficios e impacto en la práctica* para obtener más información sobre la cooperación voluntaria con proveedores de servicios extranjeros.

Caso 40. El Convenio de Budapest

El Convenio de Budapest establece facultades procesales para: la conservación expedita de los datos almacenados, la conservación expedita y la divulgación parcial de los datos de tráfico, la orden de producción, el registro y la incautación de datos informáticos, la recopilación en tiempo real de datos de tráfico y la interceptación de datos de contenido. El Convenio también establece un régimen rápido y eficaz de cooperación internacional.

El Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia sobre el refuerzo de la cooperación y la divulgación de pruebas electrónicas también proporciona una base jurídica para la divulgación de la información sobre el registro de nombres de dominio y para la cooperación directa con los proveedores de servicios en materia de información de los abonados, medios eficaces para obtener información de los abonados y datos de tráfico, cooperación inmediata en situaciones de emergencia, instrumentos de asistencia mutua, así como salvaguardias para la protección de los datos personales.

Fuente: Consejo de Europa

Acción conjunta de ejecución

102. Los equipos conjuntos transfronterizos de investigación (JITs, por sus siglas en inglés) implican un acuerdo jurídico entre las autoridades competentes de dos o más jurisdicciones con el fin de llevar a cabo investigaciones penales. Esto puede facilitar el intercambio de información y el rastreo financiero transfronterizo. Por lo general, el intercambio de información se aprovecha a través de diversos marcos y acuerdos (por ejemplo, Eurojust, el Grupo de Trabajo Conjunto contra la Ciberdelincuencia con el apoyo de Europol).

103. Los JITs también constituyen un importante punto de coordinación para la adopción de medidas multilaterales de ejecución contra el FC, habida cuenta de sus operaciones transnacionales y descentralizadas. Con la reducción de las barreras de las operaciones delictivas, las organizaciones de FC pueden reubicarse fácilmente y establecer nuevos centros digitales de operaciones de forma remota. Por lo tanto, es necesaria una acción de coordinación para desarraigar simultáneamente los diversos subgrupos (que pueden estar trabajando en múltiples jurisdicciones).

Caso 41. Acción conjunta contra el fraude en las inversiones a gran escala[23]

Serbia, junto con Austria, Bulgaria y Alemania, y con el apoyo de Eurojust, participaron con éxito en operaciones contra dos grupos de delincuencia organizada sospechosos de fraude de inversión a gran escala en el comercio cibernético. Las autoridades serbias detuvieron a cinco sospechosos y registraron nueve lugares, incautando cinco apartamentos, tres automóviles, una cantidad considerable de dinero en efectivo y equipos informáticos. Más de 30 cuentas bancarias serbias también fueron puestas bajo vigilancia. Además, cuatro sospechosos fueron detenidos en Bulgaria, mientras que 2,5 millones de euros fueron congelados en la cuenta bancaria de una empresa implicada en la trama de fraude en Alemania.

Sobre la base de la información recopilada durante la operación, las autoridades emprendieron rápidamente otra operación contra una empresa en Belgrado 2 días después, arrestando a un sospechoso e incautando servidores, otros equipos informáticos y documentos.

En este caso, las autoridades serbias, entre otras cosas, utilizaron el artículo 26 del Convenio de Budapest (Información espontánea) para compartir información con otros interlocutores. Eurojust también prestó asistencia a las investigaciones financiando un equipo conjunto de investigación (JIT), así como organizando una reunión de coordinación en sus instalaciones de La Haya y una videoconferencia.

Fuente: Serbia; Consejo de Europa (julio de 2020) El Convenio de Budapest sobre la Ciberdelincuencia: beneficios e impacto en la práctica

104. Dicho esto, también existen desafíos asociados con la acción conjunta.

- **Las barreras legales** pueden restringir el intercambio informal de información incluso dentro de los equipos conjuntos de investigación. Una jurisdicción compartió la necesidad de seguir dependiendo de las solicitudes de ALM en el ámbito de acción para permitir el intercambio de información, lo que podría obstaculizar la eficacia y la participación. También puede haber límites a la información que se puede compartir, particularmente en relación con la dispersión de la información de transacciones financieras.
- **La desigualdad de capacidades y prioridades** también puede disuadir a las jurisdicciones de participar en acciones conjuntas. Como se ha señalado anteriormente, es posible que las prioridades internas nacionales no se ajusten a la acción conjunta y que las jurisdicciones se enfrenten a una decisión difícil a la hora de equilibrar estos intereses frente a las limitaciones de recursos, a pesar del aumento del FC.

[23] Para más información, véase también el comunicado de prensa de Eurojust (abril de 2020), disponible en: www.eurojust.europa.eu/news/action-against-large-scale-investment-fraud-several-countries

105. Además de los JITs, las operaciones conjuntas organizadas por organizaciones multilaterales como INTERPOL también constituyen un importante punto de coordinación para la adopción de medidas multilaterales de observancia contra el FC. Si bien estas operaciones pueden ser más informales que los JITs en ausencia de acuerdos jurídicos formales, pueden proporcionar una plataforma importante para que las jurisdicciones pertinentes luchen conjuntamente contra el FC.

Caso 42. Operación HAECHI de INTERPOL

Desde 2020, INTERPOL lleva a cabo una operación anual denominada HAECHI que se centra en los delitos financieros cibernéticos y el LA asociado, que contribuye al intercambio de información entre las jurisdicciones participantes. En el marco de la reciente HAECHI III (2022), en la que participaron 30 jurisdicciones, se detuvo a casi 1 000 sospechosos y se bloquearon 2 800 cuentas bancarias y de AV vinculadas a ingresos ilícitos por valor de 130 millones de dólares estadounidenses. A través de HAECHI III, INTEPROL ha coordinado numerosos casos entre los países miembros para combatir conjuntamente el FC.

La Operación HAECHI también sirvió de plataforma para el FINCAF, que recopila información de diferentes fuentes e identifica vínculos entre las investigaciones en curso en los diferentes países miembros. El FINCAF está estructurado para incluir datos y otros elementos de información relacionados con cualquier tipo de delito financiero y delitos con una dimensión transnacional. INTERPOL utiliza el FINCAF para trabajar con los países miembros con el fin de reforzar la respuesta táctica general a la delincuencia organizada internacional, como el FC. El FINCAF es una herramienta importante que proporciona una mejor comprensión de las actividades delictivas transfronterizas, las organizaciones delictivas, sus estructuras de grupo, las funciones individuales y las personas clave, los *modi operandi* y las transacciones financieras fraudulentas.

Fuente: INTERPOL

Colaboración público-privada

106. La colaboración público-privada puede extenderse más allá de las fronteras nacionales, lo que puede generar mejores resultados dado el alcance transnacional del FC. Al igual que las APP nacionales, esta colaboración puede abarcar tipologías o intercambio estratégico, así como la coordinación operativa. La composición de esas asociaciones también dependería de los objetivos y podría incluir a los sectores tradicionales pertinentes de ALA/CFT y no tradicionales.

Caso 43. Acción Europea de Mulas de Dinero

La Acción Europea de Mulas de Dinero es una operación internacional basada en el intercambio de información público-privada para luchar contra los complejos delitos modernos.

En 2022, con la coordinación continua de la Federación Bancaria Europea, alrededor de 1.800 bancos e IFs apoyaron a las LEAs en esta acción, junto con los servicios de transferencia de dinero en línea, los intercambios de criptomonedas, las empresas Fintech y KYC, y las corporaciones multinacionales de tecnología informática.

La operación consistió en la participación de las fuerzas del orden de 25 jurisdicciones[1] y contó además con el apoyo de Europol, Eurojust e INTERPOL. Se identificaron 8.755 mulas de dinero junto con 222 reclutadores de mulas de dinero. En total, se interceptaron 17,5 millones de euros de fondos y se detuvo a 2.469 mulas de dinero.

Fuente: Europol

1 Australia, Austria, Bulgaria, Chipre, Colombia, República Checa, Estonia, Grecia, Hungría, Singapur, Hong Kong (China), Irlanda, Italia, Moldavia, Países Bajos, Polonia, Portugal, República Checa, Rumanía, República Eslovaca, Eslovenia, Suecia, Suiza, España, Reino Unido y Estados Unidos.

6. Conclusión y áreas prioritarias

107. El FC es perpetrado por organizaciones transnacionales del crimen organizado. Se espera que la escala y la magnitud del FC crezcan con la tendencia creciente de la digitalización y los servicios virtuales en todo el mundo. Las jurisdicciones también deben ser conscientes de las vulnerabilidades adicionales en varios sectores, incluidas las IFs digitales y los sectores no tradicionales, que los delincuentes pueden explotar para mejorar las técnicas de FC y LA a través de la creciente digitalización.

108. Las jurisdicciones deben centrarse en romper las estructuras para acelerar y mejorar la colaboración entre diversos sectores y entidades, tanto a nivel nacional como internacional. Debido a la naturaleza descentralizada del FC y del LA conexo, la información y las pruebas financieras vitales suelen estar fragmentadas en diferentes lugares. Esto complica los esfuerzos para investigar y desmantelar las organizaciones de FC, y rastrear y recuperar los ingresos del FC.

109. El FC puede tener un impacto financiero significativo y paralizante en las víctimas. Pero el impacto no se limita a las pérdidas monetarias; puede tener consecuencias sociales y económicas devastadoras. Las conclusiones de este informe indican tres áreas prioritarias en las que las jurisdicciones deberían actuar para abordar el FC y el LA relacionado de manera más eficaz: fortalecer la coordinación nacional; apoyar la colaboración multilateral; y el fortalecimiento de la detección y la prevención.

Áreas prioritarias para contrarrestar eficazmente el FC y el LA relacionado

Fortalecer la coordinación nacional entre los sectores público y privado

- Las jurisdicciones deben desarrollar mecanismos de coordinación para reunir a las autoridades competentes pertinentes a fin de hacer frente al FC y al LA conexo de manera integral. Esto incluye a expertos técnicos en ciberdelincuencia, así como a sectores no tradicionales como las plataformas de redes sociales, el comercio electrónico, las telecomunicaciones y los proveedores de servicios de Internet. Las jurisdicciones también deben aprovechar las asociaciones público-privadas para mejorar la detección y las investigaciones, y acelerar las respuestas operativas de recuperación de activos.
- Una buena práctica consiste en la creación de una unidad centralizada específica que pueda aprovechar la información pertinente y coordinar las acciones en diversos sectores públicos y privados, incluidas las investigaciones, la recuperación de activos y la prevención del fraude.

Apoyo a la colaboración internacional multilateral

- A fin de mejorar los resultados de la recuperación de activos y evitar la disipación de los ingresos relacionados con el FC, las jurisdicciones deben colaborar para interceptar rápidamente los ingresos del FC. La experiencia operativa muestra que la intervención es generalmente más efectiva dentro de las 24 a 72 horas posteriores a un incidente de FC. Se requiere un enfoque global unificado para rastrear y recuperar de manera efectiva los ingresos del FC, que se lavan y distribuyen en múltiples jurisdicciones.
- Para ello, las jurisdicciones deben aprovechar y apoyar los mecanismos multilaterales existentes (y futuros) (como el programa I-GRIP de INTERPOL y el proyecto BEC del Grupo Egmont) para acelerar la cooperación internacional y el intercambio de información para combatir el FC. Estos mecanismos multilaterales también permiten a las jurisdicciones colaborar y desmantelar colectivamente las organizaciones transnacionales del FC.

Fortalecimiento de la detección y la prevención

- Para mejorar la detección, las jurisdicciones deben garantizar la facilidad de denuncia de las víctimas, por ejemplo, a través de plataformas específicas que permitan agilizar la denuncia. Las jurisdicciones también deberían colaborar con el sector privado para mejorar la notificación de transacciones sospechosas.
- Las jurisdicciones deben promover la concientización y la vigilancia contra el FC a través de la educación pública, lo que incluye compartir los signos reveladores del FC y mejorar la alfabetización cibernética. La prevención desempeña un papel clave en la reducción de la rentabilidad global de las organizaciones del FC. Las jurisdicciones también pueden colaborar con el sector privado para apoyar las estrategias de prevención de FC, como la protección del consumidor y la eliminación de los instrumentos penales.

Anexo A: Indicadores de riesgo del FC

Los siguientes indicadores de riesgo potencial se basan en la experiencia y los datos recibidos de las jurisdicciones de la Red Global del GAFI, el Grupo Egmont y el sector privado. Estos indicadores tienen por objeto mejorar la detección de transacciones sospechosas relacionadas con el FC. La lista se clasifica además en varias perspectivas, desde la apertura de cuentas hasta el monitoreo de transacciones. Los indicadores pueden ser relevantes para las entidades reguladas, incluidas las IFs, los PSAVs, las APNFDs y otras IFs y de pago.

La existencia de un único indicador en relación con un cliente o una transacción no puede justificar por sí sola la sospecha de un delito de FC, ni un único indicador proporcionará necesariamente una indicación clara de tal actividad. Sin embargo, podría dar lugar a un mayor seguimiento y examen, según proceda.

Patrones de transacción

- Transacciones rápidas o inmediatas, de alto o bajo valor después de la apertura de una cuenta, inconsistentes con el propósito de la cuenta.
- Retiros de efectivo rápidos o inmediatos o transferencias de grandes cantidades después de recibir una transferencia de fondos para vaciar la cuenta.
- Transacciones frecuentes y de gran envergadura, que no se ajusten al perfil económico del titular de la cuenta (por ejemplo, transferencias internacionales repentinas, retiradas de efectivo realizadas a través de tarjetas de pago en cajeros automáticos extranjeros, grandes compras de AV o de bienes para exportar al extranjero, o pagos a favor de Servicios de transferencia de dinero o valores extranjeros sin licencia).
- Transferencias de fondos hacia y desde jurisdicciones de alto riesgo de LA.
- Transacciones grandes y frecuentes con empresas de reciente creación y/o cuyas actividades principales no sean coherentes con las actividades realizadas por el beneficiario o tengan un propósito general.
- Un pago pequeño a un beneficiario, que una vez completado con éxito, es seguido rápidamente por pagos de mayor valor al mismo beneficiario.
- Compras de valor redondo que son frecuentes y/o en grandes cantidades, lo que puede indicar compras con tarjetas de regalo.

Instrucciones y observaciones sobre las transacciones de los clientes

- La transacción de un cliente requiere que se realicen pagos adicionales inmediatamente después de haberse efectuado un pago exitoso a una cuenta que el cliente no utilizó previamente para pagar a sus proveedores. Este comportamiento puede coincidir con el de un delincuente que intenta que se realicen pagos adicionales no autorizados al enterarse de que un primer pago fraudulento se ha realizado correctamente.
- Las instrucciones de transacción aparentemente legítimas de un cliente contienen un lenguaje vernáculo, un momento y unos importes diferentes a los de las instrucciones de transacción verificadas anteriormente.

- Las instrucciones de transacción incluyen marcas, afirmaciones o lenguaje que designan la solicitud de transacción como "Urgente", "Secreto" o "Confidencial".
- Un cliente presenta mensajes/correos electrónicos mal formateados (errores ortográficos y/o gramaticales) como justificación de una transacción.
- Instrucciones de transacción pago directo a un beneficiario conocido; sin embargo, la información de la cuenta del beneficiario es diferente de la que se utilizó anteriormente.
- El beneficiario previsto en la descripción de la transacción y el nombre del titular de la cuenta conocido por el banco beneficiario son inconsistentes.
- Transferencias ordenadas por personas físicas (presuntos inversores) sin experiencia ni conocimientos financieros, a favor de empresas (en muchos casos establecidas en jurisdicciones de alto riesgo) con motivos de pagos relacionados con inversiones y productos financieros.
- Las contrapartes que no guardan proporción con el nombre de la empresa/negocio de la cuenta pueden sugerir que pueden proporcionar cobertura para el movimiento de grandes cantidades de fondos a nivel internacional (por ejemplo, la empresa que se informa como una empresa de muebles realizó múltiples transferencias grandes a una empresa nombrada como empresa de comercio de petróleo).
- Transacciones realizadas con discrepancia de zona horaria del dispositivo.

Sospecha en el perfil del titular de la cuenta

- El titular de la cuenta no quiere o no puede pasar los controles de DDC.
- El titular de la cuenta no está familiarizado con el origen de los fondos que se mueven a través de su cuenta o afirma que está realizando transacciones para otra persona.
- Cambios frecuentes de nombres de personas morales o empresas unipersonales utilizando expresiones y terminología extranjeras.
- El cliente demuestra tener un conocimiento inadecuado sobre la naturaleza, el objeto, el importe o la finalidad de la/s transacción/es o de la relación/es o proporciona explicaciones poco realistas, confusas o incoherentes, que llevan a sospechar que el cliente está actuando como una mula.

Sospecha en la identidad del usuario de la cuenta

- El usuario intenta ocultar su identidad mediante el uso de una identificación compartida, falsificada, robada o alterada (dirección, número de teléfono, correo electrónico).
- Cambios frecuentes de datos de contacto, números de teléfono, direcciones de correo electrónico después de la apertura de la cuenta.
- Direcciones de correo electrónico que no parecen compatibles con el nombre del titular de la cuenta, o un patrón de direcciones de correo electrónico similares que se ven en varias cuentas.

- Irregularidades en los detalles del perfil del cliente, como credenciales compartidas (por ejemplo, compartidas por dos o más usuarios) con otras cuentas.
- Anomalías identificadas a través del comportamiento en línea, como vacilación en la introducción de datos, retrasos en la pulsación de teclas, signos de automatización, múltiples intentos fallidos de inicio de sesión, etc.
- Cuentas relacionadas con entidades de las que se podría esperar que ya no estén activas en la jurisdicción (por ejemplo, la cuenta de estudiantes extranjeros vendida al finalizar sus estudios).
- Direcciones IP o coordenadas GPS procedentes de jurisdicciones de alto riesgo de LA.
- Uso de VPN, dispositivos comprometidos (como dispositivos IOT) y empresas de alojamiento que pueden enmascarar la dirección IP de un usuario.
- Múltiples direcciones IP o dispositivos electrónicos asociados a una sola cuenta en línea.
- Una sola dirección IP estática o dispositivo electrónico asociado a varias cuentas de varios titulares de cuentas.
- Conexión de escritorio remoto, acceso a una cuenta a través de los puertos de la computadora utilizados por aplicaciones como TeamViewer, etc., lo que evita que se vea el dispositivo y la ubicación reales.
- Cuentas operadas con pulsaciones de teclas excesivamente rápidas o navegación que sugieren un posible control de bots.

Información adversa sobre el titular de la cuenta

- Presencia de noticias negativas relevantes y verificables sobre el cliente o las contrapartes, por ejemplo, la cuenta de una víctima anterior conocida o sospechada de estafa, mula o actividad de apropiación de identidad.
- Reporte de fraude o retiro de una institución de correspondencia u otras bases de datos de fraude de terceros.
- Presencia de solicitudes de retiro de transferencias bancarias.
- Presencia de información adversa proporcionada por las UIF o las LEAs sobre las personas involucradas en una transacción.

Transacciones de AVs

- Enviar/recibir grandes volúmenes o altas cantidades de AVs de alta frecuencia a direcciones de billetera no alojadas; o direcciones asociadas con mercados de la *darknet*, plataformas de material de abuso sexual infantil, mercados de explotación cibernética, grupos de *ransomware*, servicios de mezcla/*tumbling*, jurisdicciones de alto riesgo, sitios de apuestas y estafadores.
- Maximizar los límites de financiamiento diarios en los cajeros automáticos de Bitcoin.
- No hay documentos que acrediten el origen de AVs o del dinero convertido en criptoactivos.

- Transferencias de AVs a billeteras vinculadas a actividades ilegales en la *darkweb* (por ejemplo, terrorismo, pornografía infantil, narcóticos, etc.).
- Transacciones que involucran más de un tipo de AV, particularmente aquellas que proporcionan un mayor anonimato.
- Actividad anormal de las transacciones de los AVs desde billeteras asociadas a la plataforma *peer-to-peer* sin una explicación comercial lógica.

Otro

- Discrepancia entre el número de cuenta y el nombre del titular de la cuenta
- El usuario es visto por teléfono o acompañado por una persona a través de un circuito cerrado de televisión (CCTV) y siendo instruido o entrenado durante la transacción
- Las empresas beneficiarias gestionan sitios web de Internet que prestan servicios de negociación o inversión, en muchos casos no autorizados o enumerados por la autoridad de supervisión nacional

Anexo B: Aprovechamiento de las sinergias entre la lucha contra el fraude y los controles de combate contra el LA y el FT

En el presente anexo se recopilan algunos buenos ejemplos de cómo los reguladores financieros han adoptado requisitos de lucha contra el fraude junto con los controles de combate contra el LA y el FT, algunos de los cuales se centran en la capacidad de los delincuentes para registrar, acceder y controlar las cuentas mula a distancia. Entre ellas se incluyen diversas medidas relacionadas con la verificación de clientes y el control de transacciones.

Estos controles pueden ser útiles para las IFs, los PSAVs y otras IFs y de pago.

- Poner en marcha procesos rigurosos de Conozca a su Cliente (KYC, por sus siglas en inglés) o Conozca su Negocio, características biométricas durante el proceso de incorporación digital, etc., e identificación de un dispositivo móvil o seguro para autenticar las transacciones bancarias en línea (otros están bloqueados o sujetos a medidas mejoradas de mitigación de riesgos).
- Un período de espera para la inscripción por primera vez de servicios bancarios en línea o dispositivos seguros (es decir, el conjunto completo de servicios bancarios no está disponible inmediatamente en el momento de la apertura), lo que limita el número o el valor de las transacciones financieras del cliente.
- Desarrollar una definición de las transacciones esperadas (número de transacciones, importes, tipos de contrapartes, países involucrados) para ayudar a detectar transacciones sospechosas, así como el endurecimiento de las normas de detección de fraude y los desencadenantes para bloquear preventivamente las transacciones ilícitas.
- Utilizar los servicios de "verificación del beneficiario", que permiten al originador/ordenante/deudor de una orden de transferencia comprobar que el beneficiario/beneficiario/acreedor mencionado en los mensajes de pago coincide con el nombre del titular de la cuenta.
- Reducir cualquier comunicación a través de correo electrónico y redes sociales con los clientes a solo información general, indicando explícitamente que no se debe intercambiar ningún dato personal o de identificación con la IF/PSAV por correo electrónico.
- Añadiendo software de reconocimiento de voz y soporte de inteligencia artificial en la comunicación con los clientes para asegurar su verdadera identidad.
- Exigir mecanismos de autenticación multifactor para la verificación de clientes y para la realización de transacciones financieras, añadiendo o activando beneficiarios a través de diferentes canales.
- Para autenticar la identidad del usuario durante la configuración remota y evitar que los delincuentes obtengan acceso a múltiples cuentas utilizando la información de la cuenta de las mulas de dinero o de las víctimas mediante:

- Mejorar la confiabilidad del proceso de identificación del cliente a través de pruebas de vida (es decir, garantizar que un ser humano vivo y real), incluso si una persona está siendo sometida a ingeniería social durante las verificaciones de vida; o
- Monitoreo de direcciones IP utilizadas para conectarse a sitios web bancarios en línea, etc., incluida la detección del uso de herramientas de acceso remoto y ataques de "hombre en el navegador".

- Ampliar los tipos de datos que las entidades informantes recopilan y analizan sobre los clientes, incluidos, por ejemplo, números de teléfono móvil, direcciones IP, coordenadas GPS, ID de dispositivos, etc. con fines de prevención del fraude, las IF podrían repetir dicha identificación utilizando un enfoque basado en el riesgo (por ejemplo, realizar estas comprobaciones cuando se detecte un comportamiento anómalo).
- Implementar un sistema de monitoreo de transacciones en tiempo real basado en el riesgo para garantizar que cualquier actividad anormal pueda ser rápidamente detectada, investigada y, cuando corresponda, reportada a través de la presentación de un informe de transacciones sospechosas. El sofisma del sistema de supervisión debe ser proporcional al volumen y la naturaleza de las transacciones gestionadas por la IF.

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

INTERPOL

FATF

www.egmontgroup.org | www.interpol.int | www.fatf-gafi.org

Noviembre 2023

Flujos financieros ilícitos procedentes del fraude cibernético

Este informe analiza los métodos utilizados para el fraude cibernético, sus vínculos con otros delitos y el modo en que los delincuentes pueden explotar las vulnerabilidades de las nuevas tecnologías. Destaca ejemplos de respuestas y estrategias operativas nacionales que han demostrado su eficacia en la lucha contra el fraude cibernético. El informe también identifica indicadores de riesgo y requisitos y controles antifraude útiles que pueden ayudar a las entidades de los sectores público y privado a detectar y prevenir él.