Departamento del Tesoro

Evaluación Nacional del Riesgo de Blanqueo de Capitales 2026

Marzo de 2026

Departamento del Tesoro

Evaluación Nacional del Riesgo de Blanqueo de Capitales 2026

ÍNDICE

RESUMEN EJECUTIVO

Estados Unidos publicó por primera vez la Evaluación Nacional de Riesgo de Blanqueo de Dinero (NMLRA) hace más de 10 años. Esta quinta versión de la NMLRA concluye que las principales amenazas de blanqueo de capitales se han mantenido constantes: fraude, narcotráfico, ciberdelitos, trata de personas, tráfico de personas y corrupción generan los mayores volúmenes de ingresos ilícitos por actividad de lavado de capitales en Estados Unidos. El comercio ilícito, como la evasión arancelaria o el tráfico de bienes robados, ilícitos o regulados, también genera miles de millones de dólares cada año. Estas amenazas se ven potenciadas además por blanqueadores profesionales, como las redes chinas de blanqueo de capitales (CMLN), que hacen que el crimen sea más lucrativo al proporcionar experiencia y economías de escala.

Los avances tecnológicos en finanzas y comunicación han amplificado las amenazas que suponen todos estos crímenes y actores amenazantes. El rápido crecimiento de las tecnologías emergentes, que está mejorando el acceso y la experiencia del consumidor, también crea oportunidades que los actores ilícitos pueden explotar para ocultar el origen de los fondos ilícitos más rápido y a escala global. Los actores ilícitos dependen cada vez más de las redes sociales para colocar anuncios maliciosos y reclutar víctimas, aplicaciones de mensajería cifrada para comunicarse con víctimas y coconspiradores, activos digitales para recibir y blanquear fondos y, más recientemente, herramientas de inteligencia artificial (IA) para crear comunicaciones, identidades y sitios web fraudulentos.

Los blanqueadores de dinero buscan explotar todos los aspectos del sistema financiero estadounidense para ocultar la naturaleza y el origen de sus ingresos ilícitos. Ya sea a través de bancos o casinos, efectivo o activos digitales, el objetivo principal es disfrazar dinero sucio dentro de los billones de dólares de transacciones legítimas que ocurren cada año en Estados Unidos. En algunos casos, abusan de las entidades legales o dependen de guardianes financieros para frustrar a las instituciones financieras que buscan identificar a los actores subyacentes y reportar actividades sospechosas a las fuerzas del orden. Los sectores público y privado de EE. UU. deben seguir evolucionando nuestras capacidades para combatir la amenaza que supone la financiación ilícita, al tiempo que protegemos y fomentamos la financiación legítima sin una carga excesiva.

Los actores ilícitos que cometen delitos subyacentes de blanqueo de capitales no se preocupan por el bienestar de sus víctimas. Apuntan a Estados Unidos debido a la apertura de la economía estadounidense, el tamaño y sofisticación del sistema financiero estadounidense, y la relativa riqueza de los ciudadanos y empresas estadounidenses. Operan deliberadamente al margen de las leyes y regulaciones que se aplican a todos los individuos y empresas para obtener beneficios a costa directa de otros. Pero medir las pérdidas de estos crímenes en dólares y céntimos solo llega hasta cierto punto. La actividad financiera ilícita también desplaza a los actores legítimos, erosiona la confianza en el libre mercado y debilita la seguridad nacional de Estados Unidos.

Estafadores extranjeros están robando miles de millones de dólares en ahorros duramente ganados y desviando fondos públicos destinados a ayudar a los estadounidenses más necesitados a financiar estilos de vida lujosos. Los narcoterroristas están inundando las ciudades estadounidenses con drogas mortales y reinvirtiendo los beneficios ilícitos en sus conglomerados criminales que trafican con personas y aterrorizan comunidades. El gobierno estadounidense está abordando estas amenazas de frente, impulsando recursos mediante iniciativas como la Operación Recuperar América y los Grupos de Trabajo de Seguridad Nacional. A medida que evoluciona el panorama de amenazas, Estados Unidos seguirá trabajando para llevar ante la justicia a los actores amenazantes de todo el mundo, mientras fortalece el sistema financiero estadounidense frente a sus ataques.

INTRODUCCIÓN

La Evaluación Nacional de Riesgos de Blanqueo de Capitales (NMLRA) 2026 examina el entorno actual de blanqueo de capitales e identifica las formas en que los delincuentes y otros actores buscan blanquear fondos. Su objetivo es informar sobre el riesgo de financiación ilícita por parte de actores públicos y privados, fortalecer las estrategias de mitigación de riesgos de las instituciones financieras y reforzar las deliberaciones políticas del gobierno de EE. UU. Los actores ilícitos siempre buscarán desarrollar y adoptar nuevas formas de blanquear los ingresos ilícitos, lo que requiere la identificación continua de tendencias de blanqueo de capitales para desarrollar soluciones tácticas, regulatorias y políticas que detengan la actividad ilícita.

En los últimos cinco años, la pérdida mediana de casos de blanqueo de capitales condenados ha aumentado más de un 150 por ciento, pasando de 208.000 a 526.000 dólares. En 2019, solo el 17 por ciento de estos casos implicaban pérdidas superiores a 1,5 millones de dólares, y en 2024 esa proporción casi se ha duplicado hasta el 32 por ciento de los casos.[1] Esta tendencia se concuerda con el aumento del ataque a ciudadanos estadounidenses, empresas y programas gubernamentales por parte de narcoterroristas y organizaciones criminales transnacionales (TCOs) que participan en fraudes, trata de personas y contrabando, y corrupción, así como la explotación de tecnologías emergentes, como las comunicaciones cifradas y la inteligencia artificial (IA), que permiten a actores ilícitos aumentar su tamaño y alcance, y la rapidez de sus planes. Estas principales amenazas de blanqueo de capitales suponen una amenaza para la seguridad nacional de Estados Unidos y su sistema financiero.

Este informe fue elaborado conforme a las Secciones 261 y 262 de la Ley para Contrarrestar a los Adversarios de América a través de Sanciones (PL 115-44), modificada por la Sección 6506 de la Ley de Autorización de Defensa Nacional (NDAA) (P.L. 117-81) del año fiscal 2022. La NMLRA 2026 se basa principalmente en la información de fuentes abiertas del Departamento de Justicia (DOJ), el uso de documentos judiciales públicos y consultas con agencias de aplicación de la ley (LEA) y entidades reguladas. La NMLRA también utiliza información de informes de la Ley de Secreto Bancario (BSA), como el análisis estratégico de informes de actividades sospechosas (SAR) realizados por la Red de Aplicación de Delitos Financieros (FinCEN), así como diversos tipos de acciones de cumplimiento emprendidas por agencias reguladoras estadounidenses. El periodo de evaluación abarca del 1 de enero de 2024 al 31 de diciembre de 2025.

Los resultados de la NMLRA 2026, tomados junto con los resultados de la evaluación de riesgos de financiación de la proliferación y la evaluación del riesgo de financiación del terrorismo, informarán la próxima Estrategia Nacional de Financiación Ilícita de 2026, que establecerá la hoja de ruta para abordar las amenazas y vulnerabilidades al sistema financiero estadounidense y, en última instancia, fortalecerá la integridad del sistema financiero estadounidense.

1 Comisión de Sentencias de EE. UU. (USSC), "QuickFacts Año Fiscal 2024 sobre el Blanqueo de Capitales", https://www.ussc.gov/sites/default/files/pdf/ investigaciones y publicaciones/hechos rápidos/Money_Laundering_FY24.pdf; USSC, "QuickFacts Blanqueo de Capitales Año Fiscal 2019," https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Money_Laundering_FY19.pdf.

AMENAZAS

Las amenazas de blanqueo de capitales son los delitos subyacentes que generan ingresos ilícitos para el blanqueo en, desde o a través de Estados Unidos. Los actores amenazantes incluyen a quienes cometen delitos subyacentes o facilitan el proceso de blanqueo de capitales. Esta evaluación evalúa principalmente cómo las amenazas de blanqueo de capitales afectan a Estados Unidos, incluyendo el volumen de ingresos ilícitos generados, el alcance de la actividad ilícita y la actividad económica perdida debido a actores ilícitos que desplazan a los negocios legítimos. También considera las consecuencias para la seguridad nacional de las amenazas de blanqueo de capitales, financiación del narcoterrorismo y otras actividades de adversarios extranjeros. Por último, esta evaluación considera las consecuencias sociales de las amenazas de blanqueo de capitales, como los cientos de miles de estadounidenses que mueren cada año por drogas ilícitas introducidas en Estados Unidos o las víctimas de estafas estadounidenses que se ven llevadas a la ruina financiera o a autolesionarse por la devastadora pérdida de sus ahorros.

Las principales amenazas de blanqueo de capitales se han mantenido constantes: el fraude y el tráfico de drogas generan cientos de miles de millones de dólares en ingresos ilícitos cada año. El ciberdelito, la trata de personas, el tráfico de personas y la corrupción también generan miles de millones de dólares en ingresos ilícitos. Los blanqueadores profesionales de dinero, que van desde las complejas redes chinas de blanqueo de capitales (CMLNs) hasta mulas independientes que buscan ganar dinero rápidamente, amplifican las amenazas que suponen los delitos subyacentes al hacer que el crimen sea más lucrativo gracias a la experiencia en blanqueo de capitales y las economías de escala. Esta evaluación también examina el comercio ilícito como una amenaza de blanqueo de capitales. El blanqueo de capitales basado en el comercio (TBML) ha sido considerado durante mucho tiempo una vulnerabilidad para el lavado de capitales, pero el tráfico de bienes robados, el contrabando para evitar aranceles y otras tácticas ilícitas también generan miles de millones de dólares en ingresos ilícitos cada año.

I. Fraude

Los estadounidenses y el gobierno de Estados Unidos están bajo ataque por parte de defraudadores extranjeros y nacionales. Las pérdidas por fraude, tanto a consumidores como al gobierno, continúan aumentando año con año. En 2024, el Centro de Quejas de Delitos en Internet (IC3) del Buró Federal de Investigaciones (FBI) recibió 859,532 denuncias de víctimas por presuntos delitos en internet, con pérdidas que superaron los 16 mil millones de dólares, lo que representa un incremento del 33 % respecto de 2023. Esa cifra únicamente contempla las pérdidas reportadas y probablemente subestima las pérdidas reales por decenas de miles de millones de dólares. La Oficina de Responsabilidad del Gobierno de Estados Unidos (GAO) estima que el gobierno federal pierde entre 233 mil millones y 521 mil millones de dólares al año por fraude. El fraude a esta escala perjudica a los consumidores, distorsiona los mercados financieros y socava la confianza pública en los programas gubernamentales y en el sistema financiero, lo que debilita la seguridad económica y nacional de Estados Unidos.

El fraude puede ser perpetrado por estados nación, TCOs, organizaciones criminales nacionales o individuos. Los estafadores pueden avanzar en sus esquemas de fraude financiero cometiendo otros delitos como robo de identidad, robo de propiedad o acceso no autorizado a ordenadores. Cada vez dependen más de tecnologías para aumentar la escala, el alcance y la velocidad de sus esquemas de fraude.5 Esto incluye el uso de redes sociales para colocar anuncios maliciosos y reclutar víctimas, aplicaciones de mensajería cifrada para comunicarse con víctimas y cómplices, activos digitales para recibir y blanquear fondos y, más recientemente, herramientas de inteligencia artificial (IA) para crear comunicaciones, identidades y sitios web fraudulentos.

2 IC3, "Internet Crime Report 2024," (abril de 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf; *Véase también,* Comercio Federal Comisión (FTC), "Nuevos datos de la FTC muestran un gran aumento en las pérdidas reportadas por fraude hasta 12.500 millones de dólares en 2024," (10 de marzo de 2025) https://www. ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

3 En 2024, la FTC estimó pérdidas totales por fraude de hasta 195.900 millones de dólares frente a al menos 12.700 millones de dólares reportadas por fraude. *Consulta* FTC, "Protecting Older Consumers, 2024-2025" (diciembre de 2025), p. 28, https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.

4 GAO, "Los datos de 2018-2022 muestran que el gobierno federal pierde entre 233.000 y 521.000 millones de dólares anualmente por fraude, basándose en diversos entornos de riesgo," (abril de 2024) https://www.gao.gov/assets/gao-24-105833.pdf.

5 Grupo de Trabajo de Acción Financiera (GAFI), "Flujos financieros ilícitos derivados del fraude habilitado por cibernética", (noviembre de 2023) https://www.fatf-gafi.org/content/ presa/FATF-gafi/informes/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf.

6 IC3, "Los delincuentes utilizan inteligencia artificial generativa para facilitar el fraude financiero," (3 de diciembre de 2024) https://www.ic3.gov/PSA/2024/PSA241203.

Las pérdidas por fraude también están aumentando en parte debido a los TCOs extranjeros que se dirigen a consumidores, empresas y programas gubernamentales estadounidenses, debido a la apertura de la economía estadounidense, el tamaño y sofisticación del sistema financiero estadounidense, y la relativa riqueza de los ciudadanos y empresas estadounidenses. Los TCO pueden perpetrar fraude a escala industrial estando basados en jurisdicciones extranjeras donde los gobiernos no toman medidas suficientes contra las operaciones delictivas dentro de sus fronteras. Algunas TCOs han ampliado sus operaciones de fraude como otra fuente de ingresos ilícitos junto a sus operaciones de narcotráfico o tráfico de personas.[7] Los estafadores extranjeros, incluidos los TCOs, suelen depender de mulas de dinero con base en EE. UU. para blanquear los ingresos del fraude a través del sistema financiero estadounidense a jurisdicciones extranjeras donde se encuentran los perpetradores.

Esta evaluación analiza el fraude como motor de la actividad de blanqueo de capitales basándose en el volumen de ingresos ilícitos generados y el impacto general en el sector financiero estadounidense. El fraude puede categorizarse según la víctima, el método o la entidad explotada, y a menudo existe una superposición significativa en la forma en que se clasifican los esquemas. Por ejemplo, los esquemas de inversión en activos digitales son tanto una forma de fraude de inversión como una estafa de confianza, con los perpetradores utilizando tácticas similares para atrapar a las víctimas, incluyendo el contacto no solicitado, el desarrollo de relaciones románticas o cercanas entre el agresor y la víctima, y la recaudación de impuestos o tasas para resolver problemas inexistentes.

Fraude de inversiones

El fraude de inversión abarca cualquier esquema en el que las víctimas invierten fondos basándose en información falsa o engañosa. En 2024, el fraude de inversiones provocó las mayores pérdidas de víctimas reportadas a IC3, que totalizaron 6.570 millones de dólares, un aumento del 44 % respecto al año anterior en gran parte debido al aumento de las pérdidas relacionadas con esquemas de inversión en activos digitales descritos a continuación.8 El número total de informes de fraude de inversión y la pérdida media por informe de fraude de inversión han aumentado de forma constante en los últimos tres años (véase la Figura 1 más abajo). Además de robar a inversores inocentes, el fraude en inversiones también desvía capital de negocios legítimos, hace que los inversores sean escépticos respecto a las oportunidades de inversión legítimas y las tecnologías e industrias emergentes, y en última instancia perjudica la seguridad económica y nacional de EE. UU. al obstaculizar el desarrollo económico y tecnológico.

		2022	2023	2024
IC3	Pérdida total de $	$3.31 b	$4.57 b	$6.57 b
	# de informes	30,529	39,570	47,919
	Pérdida media de $.	108.478 $	115.498 $	137.119 $

Figura 1

Los esquemas de fraude en inversiones suelen comenzar con los perpetradores ofreciendo ofertas de inversión no solicitadas a las víctimas y anunciando altos rendimientos con riesgos mínimos. Estafadores afirman invertir fondos de víctimas en todo tipo de clases de activos, incluyendo activos financieros tradicionales como valores, derivados y divisas extranjeras; activos digitales; proyectos inmobiliarios y de construcción; y negocios físicos. Algunos agresores convencen a las víctimas para invertir en negocios que generan pocos o ningún retorno, mientras se enriquecen en el proceso. En otros casos, los estafadores no intentan invertir fondos de víctimas ni estructuran sus operaciones como esquemas Ponzi utilizando fondos de

7 *Véase, por ejemplo,* Red de Aplicación de Delitos Financieros (FinCEN), Oficina de Control de Activos Extranjeros (OFAC) y FBI, "Aviso conjunto sobre fraude de tiempo compartido asociado con organizaciones criminales transnacionales con sede en México," (16 de julio de 2024) https://www.fincen.gov/sites/default/files/shared/ FinCEN-Joint-Notice-Timeshare-Mexico-508C-FINAL.pdf.

8 IC3, "Informe sobre delitos en Internet 2024," (abril de 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

9 *Véase* el DOJ, "CEO tecnológico acusado en esquema de fraude de inversión en inteligencia artificial," (9 de abril de 2025)

https://www.justice.gov/usao-sdny/pr/ esquema de fraude de inversión acusado por un CEO tecnológico.

10 Oficina del Contralor de la Moneda (OCC), "Fraude financiero y de inversión," (consultado el 3 de julio de 2025) https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/financial-and-investment-fraud-.html.

11 *Ver, por ejemplo,* DOJ, "Estafador de inversiones condenado a 96 meses de prisión por defraudar inversores de influencia alfa por más de 20 millones de dólares," (7 de mayo de 2025) https://www.justice.gov/usao-ut/pr/investment-scammer-sentenced-96-months-imprisonment-defrauding-alpha- inversores de influencia.

nuevos inversores que pagan a los anteriores y dan la apariencia de rendimientos legítimos de inversión.[12] Estos esquemas implican cada vez más promesas de aprovechar tecnologías nuevas y emergentes, como la IA, para comerciar activos o alterar mercados existentes. [13]

Los estafadores de inversiones suelen dirigirse a grupos de identidad específicos, a menudo comunidades religiosas o étnicas. Estos esquemas de fraude basados en afinidades pueden ser más difíciles de interrumpir para las fuerzas del orden y los reguladores debido a las estructuras comunitarias muy cohesionadas que pueden animar a las víctimas a resolver disputas dentro del grupo.[14] Los autores suelen blanquear los ingresos del fraude de inversión intentando hacer pasar esos ingresos ilícitos como ganancias o comisiones legítimas cuando en realidad han malversado fondos de los inversores para gastos personales, a menudo de forma lujosa destinada a transmitir éxito de inversión que atraerá a más víctimas. Estas muestras abiertas de riqueza, como publicar capturas de pantalla de cuentas bancarias en redes sociales, pueden indicar fraude de inversión. [15]

El fraude de inversiones también incluye tipos de fraude en valores, como los esquemas de "ramp-and-dump", una variante de los esquemas de "pump-and-dump". En muchos de estos esquemas, individuos con sede en China hacen campañas fraudulentas para inflar el precio y el volumen de una acción para entidades de interés variable (VIEs), que son empresas afiliadas a China que cotizan en bolsas estadounidenses. Este esquema opera mediante estafadores que se hacen pasar por asesores financieros reales, entre otros, promocionan la acción en redes sociales y crean una falsa impresión de impulso comprador en todo el mercado. Una vez que el precio de la acción ha subido mucho, los estafadores "venden" sus propias participaciones, asegurando beneficios y haciendo que el precio de la acción se desplome en detrimento de los inversores minoristas estadounidenses y otros.[16] En solo la primera mitad de 2025, el IC3 reportó un aumento del 300 % en las quejas de víctimas de este tipo de esquemas de inversión respecto al año anterior.

12 *Véase, por ejemplo,* el DOJ, "Hombre de San Diego que dirigió un esquema de fraude de valores y ayuda COVID-Fraude de 35 millones de dólares condenado a casi 20 años," (28 de febrero de 2025) https://www.justice.gov/usao-sdca/pr/san-diego-man-who-ran-35-million-securities-fraud-and-covid-relief-fraud-scheme.

13 *Véase, por ejemplo,* DOJ, "CEO tecnológico acusado en esquema de fraude de inversión en inteligencia artificial," (9 de abril de 2025) https://www.justice.gov/usao-sdny/pr/ ceo tecnológico acusado-de-inteligencia-artificial-fraude-inversión-fraude-inversiones; SEC, "La SEC acusa a tres supuestas plataformas de negociación de criptoactivos y a cuatro clubes de inversión con un esquema dirigido a inversores minoristas en redes sociales" (22 de diciembre de 2025) https://www.sec.gov/newsroom/press-publicaciones/2025-144-sec-carga-tres-supuestas-plataformas-de negociación de criptoactivos-cuatro-clubes-inversionistas-schemes.

14 SEC, "Deteniendo el fraude de afinidad en tu comunidad," (julio de 2023) https://www.investor.gov/sites/investorgov/files/2023-09/Affinity-Fraud English.pdf

15 FTC, "¿Se puede detectar una estafa de inversión en redes sociales?" (28 de mayo de 2025) https://consumer.ftc.gov/consumer-alerts/2025/05/can-you- estafa-inversión spot-inversion-redes sociales.

16 *Ver, por ejemplo,* DOJ, "Co-CEO de empresa tecnológica china cotizada en bolsa y asesor financiero acusado de fraude de valores de más de 100 millones de dólares," (12 de septiembre de 2025) https://www.justice.gov/opa/pr/co-ceo-chinese-publicly-traded-technology-company-and- asesor financiero acusado por más de 100 millones; *véase también,* DOJ, "La Fiscalía de los Estados Unidos en Chicago obtiene la confiscación de 214 millones de dólares en ingresos de un supuesto esquema de fraude de inversiones "pump and dump" (28 de mayo de 2025) https://www.justice.gov/usao-ndil/pr/us-attorneys-office- Chicago-obtiene-dequista-214-millones-supuesto-ingresos-y; DOJ, "Empresario de Hong Kong acusado por su papel en la presentación de formularios falsos de asesor de inversiones de la SEC en nombre de entidades fraudulentas utilizadas en esquema de ramp-and-dump," (14 de noviembre de 2025) https://www.justice.gov/opa/pr/hong-kong-businessman-indicted-role-filing-false-sec-investment-adviser-forms-behalf-sham; SEC, "Liberación de suspensión de negociación: Smart Digital Group Limited" (26 de septiembre de 2025) https://www.sec.gov/enforcement-litigation/trading-suspensions/34-104112-ts; SEC, "Liberación de suspensión de negociación: Magnitude International Ltd" (4 de diciembre de 2025) https://www.sec.gov/files/litigation/suspensiones/2025/34-104317-ts.pdf 17 IC3, "Fraudadores atacan inversores en acciones estadounidenses a través de clubes de inversión accesibles en redes sociales y aplicaciones de mensajería," (3 de julio de 2025) https://www.ic3.gov/PSA/2025/PSA250703; *véase* también SEC, "Chats de grupo como puerta de entrada a estafas de inversión – Alerta de inversor" (22 de diciembre de 2025), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/ puerta de entrada a estafas de inversión; Autoridad Reguladora de la Industria Financiera (FINRA) "Alerta al inversor: Las estafas de impostores en redes sociales en redes sociales siguen aumentando" ("Alerta de Grupo de Inversión FINRA") (9 de diciembre de 2025) https://www.finra.org/investors/insights/ estafas de impostores de grupos de inversión. El 5 de septiembre de 2025, la SEC anunció la formación de un Grupo de Trabajo Transfronterizo para combatir el fraude como los esquemas de "pump-and-dump" y "ramp-and-dump" relacionados con empresas extranjeras. El grupo de trabajo también se centra en violaciones de la ley de valores "relacionadas con empresas de jurisdicciones extranjeras, como China." https://www.sec.gov/newsroom/press-lanzamientos/2025-113-sec-anuncia-formación-force-tarea-transfronteriza-fraude-fraude.

Estafas de inversión en activos digitales

Las estafas de inversión en activos digitales, algunas de las cuales se conocen comúnmente como estafas de "carnicería de cerdos", son una de las formas más dañinas de fraude en la inversión. Los TCOs realizan estas estafas operando centros de estafa a escala industrial en todo el sudeste asiático, principalmente en Camboya, Birmania y Laos, desde donde llevan a cabo una variedad de estafas dirigidas a estadounidenses.[18] informes recientes indican que las TCO están ampliando sus operaciones a África, Sudamérica y Asia del Sur.[19] El tamaño y la escala de estas operaciones fraudulentas han tenido consecuencias devastadoras. En 2024, las víctimas reportaron pérdidas de 5.800 millones de dólares relacionadas con estafas de inversión en activos digitales al IC3, un aumento del 47 % respecto al año anterior. Estas cifras probablemente representan un subestimado de las verdaderas pérdidas de las víctimas, ya que las revelaciones al IC3 son voluntarias y las víctimas a menudo no denuncian estas estafas por vergüenza por haber sido engañadas.

Los agresores suelen contactar con las víctimas en redes sociales, plataformas de citas o por SMS (texto) en dispositivos móviles y desarrollan relaciones con las víctimas durante semanas o meses antes de introducir gradualmente la idea de invertir en activos digitales.[20] La víctima entonces envía transferencias bancarias o activos digitales a lo que cree que son cuentas en una supuesta plataforma de inversión, pero que en realidad son cuentas bancarias o cuentas de intercambio de activos digitales controladas por el TCO. En algunos casos, las entidades falsas se registran fraudulentamente en FinCEN como empresas de servicios monetarios (MSB) y utilizan ese auto-registro para parecer legítimos o ganar credibilidad.[21] Las víctimas ven ganancias falsificadas en la aplicación o sitio web de la plataforma de inversión falsa, lo que les incita a invertir aún más. Cuando las víctimas finalmente intentan cobrar sus inversiones, los agresores les dicen que deben pagar impuestos o tasas para retirar fondos. Una vez que las víctimas pagan estas cantidades adicionales, los agresores dejan de comunicarse con ella. Muchas víctimas son contactadas por estafadores que se hacen pasar por bufetes de abogados ficticios o empresas de recuperación de activos, lo que puede aumentar aún más las pérdidas económicas para la víctima, agravando el daño al consumidor. [22]

Muchos de los individuos que perpetraron las estafas pueden ser víctimas de trata de personas y se ven obligados a manipular a las víctimas de la estafa. Los TCOs colocan anuncios falsos de empleo para empleos técnicos bien remunerados en redes sociales y sitios de empleo online para atraer a jóvenes trabajadores de todo el mundo. Una vez que las víctimas llegan para el trabajo, son retenidas en condiciones similares a prisiones en centros fraudulentos y obligadas a perpetrar estafas bajo amenaza de violencia. Los TCO castigan el bajo rendimiento y la desobediencia mediante abuso físico y tortura, abuso sexual, disminución salarial y esclavitud de deudas, y pueden "revender" a quienes no pueden cumplir cuotas de ventas o pagar deudas de reclutamiento a otras redes criminales por trabajo forzado en esquemas de fraude similares, servidumbre doméstica o trata sexual. [23]

Los autores utilizan activos digitales tanto para atraer a las víctimas al esquema como para blanquear los beneficios ilícitos. En un caso,

18 *Véase, por ejemplo,* Instituto de Paz de los Estados Unidos (USIP), "Crimen transnacional en el sudeste asiático: una amenaza creciente para la paz y la seguridad globales," (mayo de 2024), p. 26, https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf.

19 Oficina de las Naciones Unidas contra la Droga y el Crimen (UNODC), "Punto de inflexión: implicaciones globales de centros fraudulentos, banca clandestina y mercados ilícitos en línea en el sudeste asiático," (abril de 2025), pp. 9-10, https://www.unodc.org/roseap/uploads/documents/ Publications/2025/Inflection_Point_2025.pdf; Comisión Económica y Financiera de Nigeria (EFCC), "EFCC, NIS, NCoS Deportación Completa de 192 Extranjeros Condenados por Ciberterrorismo en Lagos," (18 de octubre de 2025) https://www.efcc.gov.ng/news/efcc-nis-ncos-deportación-completa-de-192-extranjeros-condenados-por-ciberterrorismo-en-Lagos.

20 FinCEN, "FinCEN recuerda a las instituciones financieras que permanezcan alertas ante posibles estafas de inversión en relaciones," (26 de febrero de 2025) https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-remain-vigilant-regarding-potential; FinCEN, "Alerta de FinCEN sobre la estafa prevalente de inversión en moneda virtual conocida comúnmente como 'carnicería de cerdos'", (8 de septiembre de 2023) https://www. fincen.gov/system/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf; *véase también la* SEC, "5 formas en que los estafadores pueden atraer víctimas a estafas que involucren valores de activos criptográficos" (29 de mayo de 2024) https://www.investor.gov/introduction-investing/general-resources/news- alertas/alertas-boletines/alertas_para_inversores/estafas cripto; SEC, "Chats grupales como puerta de entrada a estafas de inversión – Alerta de inversor," (22 de diciembre de 2025) https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/gateway-to estafas de inversión.

21 FinCEN, "Alerta de FinCEN sobre esquemas de fraude que abusan del nombre, insignia y autoridades de FinCEN para obtener beneficio económico," (18 de diciembre de 2024), p. 5, https://www.fincen.gov/system/files/2024-12/Alert-FinCEN-Scams-FINAL508.pdf.

22 IC3, "Despachos de abogados ficticios que apuntan a víctimas de estafas de criptomonedas combinan múltiples tácticas de explotación mientras ofrecen recuperar fondos," (13 de agosto de 2025) https://www.ic3.gov/PSA/2025/PSA250813; *véase también FINRA* Investment Group Alert (que alerta a los inversores de que las mismas estafas de grupos de inversión dirigidas a grupos de afinidad a través de WhatsApp y redes sociales también se están aplicando a esquemas de criptoactivos).

23 Departamento de Estado de EE. UU. (Estado), "Informe 2025 sobre la trata de personas: Camboya," (septiembre de 2025)

ciudadano con doble nacionalidad de China y de San Cristóbal y Nieves, se declaró culpable de su papel en el blanqueo de más de 73 millones de dólares en estafas de inversión en activos digitales. El hombre instruyó a los co-conspiradores para que abrieran cuentas bancarias estadounidenses establecidas en nombre de empresas pantalla y supervisarían la recepción y ejecución de transferencias bancarias interestatales e internacionales de fondos de las víctimas. El hombre y los cómplices recibirían fondos de las víctimas en cuentas financieras que controlaban y luego supervisaban la conversión de los fondos de las víctimas en activos digitales, específicamente stablecoins, y la posterior distribución a carteras controladas por los co-conspiradores. [24]

Los TCOs pueden blanquear un volumen tan grande de ingresos ilícitos de estas estafas en parte debido a instituciones financieras cómplices que operan en jurisdicciones con controles débiles o inexistentes contra el blanqueo de capital/contraataque de la financiación del terrorismo (AML/CFT), a menudo en la misma jurisdicción que los compuestos de estafas. Una de estas instituciones es Huione Group, con sede en Camboya, que ofrece servicios que van desde un mercado online que vende artículos útiles para llevar a cabo estafas cibernéticas, hasta servicios de pago de moneda fiduciaria y activos digitales utilizados frecuentemente para el blanqueo de capitales.[25] En octubre de 2025, FinCEN emitió una norma final conforme a la Sección 311 de la Ley USA PATRIOT que separó a Huione Group del sistema financiero estadounidense por blanquear al menos 4.000 millones de dólares en ingresos ilícitos entre agosto de 2021 y enero de 2025.[26] La norma final de FinCEN señaló que los riesgos derivados de la asociación del Grupo Huione con actores ilícitos y transacciones vinculadas a actividades ilícitas se agravan por la ausencia o ineficacia de políticas y procedimientos AML/Conoce a tu Cliente entre los componentes del Grupo Huione.

En octubre de 2025, se desveló una acusación contra el fundador y presidente del Prince Group, un conglomerado multinacional con sede en Camboya, por presunta conspiración de fraude electrónico y blanqueo de capitales por dirigir la operación de complejos de estafa de trabajo forzado por parte de Prince Group en todo Camboya. El DOJ también presentó una demanda civil por decomiso contra aproximadamente 127.271 Bitcoin, valorados en aproximadamente 15.000 millones de dólares en el momento de la incautación, que son los ingresos e instrumentos de los esquemas de fraude y blanqueo de capitales del acusado y que estaban almacenados en 27 monederos digitales auto alojados cuyas claves privadas poseía el demandado. La demanda es la mayor acción de decomiso en la historia del Departamento de Justicia.[28] La Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro de EE. UU., en una acción coordinada con el Reino Unido, también impuso sanciones amplias sobre 146 objetivos dentro del TCO del Grupo Prince, incluyendo a su líder Chen Zhi y empresas clave como Prince Holding Group y Prince Bank, así como multitud de vehículos de inversión en Asia y el Caribe.[29] En 2025, la OFAC también designó a otras 33 personas y entidades implicadas en centros fraudulentos. [30]

24 DOJ, "Ciudadano extranjero se declara culpable de blanquear millones en beneficios procedentes de estafas de inversión en criptomonedas," (12 de noviembre de 2024) https://www.justice.gov/archives/opa/pr/foreign-national-pleads-guilty-laundering-millions-proceeds-cryptocurrency-investment-Estafas.

25 FinCEN, "FinCEN considera que el grupo Huione, con sede en Camboya, es de principal preocupación por el blanqueo de capitales, propone una norma para combatir las estafas y robos cibernéticos," (1 de mayo de 2025) https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-preocupación por el blanqueo de capitales.

26 FinCEN, "FinCEN emite la norma final que separa a Huione Group del sistema financiero estadounidense," (14 de octubre de 2025) https://www.fincen.gov/ noticias/comunicados de prensa/fincen-issues-final-rule-severing-huione-group-us-financial-system.

27 También llamado "no custodio", "autocustodio" o "sin alojamiento". Véase The White House, "Fortaleciendo el liderazgo estadounidense en tecnología financiera digital" (julio de 2025), p. 33, https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.

28 DOJ, "Presidente de Prince Group acusado de operar complejos de estafa de trabajo forzado en Camboya y fraude con criptomonedas," (14 de octubre de 2025) https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor- estafas-compuestos-involucrados.

29 Tesorería, "EE. UU. y Reino Unido. Toma la mayor acción jamás dirigida a redes cibercriminales en el sudeste asiático," (14 de octubre de 2025) https://home. treasury.gov/news/press-releases/sb0278.

30 Véase Tesorería, "Hacienda sanciona a señor de la guerra y milicia de Birmania vinculados a operaciones de centros de estafas," (5 de mayo de 2025) https://home.treasury. gov/news/press releases/sb0129; Tesorería, "Tesorería toma medidas contra un importante facilitador de estafas cibernéticas," (29 de mayo de 2025) https://home. treasury.gov/news/press-releases/sb0149; Tesoro, "Hacienda sanciona redes del sudeste asiático que atacan a estadounidenses con estafas cibernéticas," (8 de septiembre de 2025) https://home.treasury.gov/news/press-releases/sb0237; Tesorería, "Hacienda sanciona a grupo armado y empresas de Birmania vinculados al crimen organizado que persigue a estadounidenses," (12 de noviembre de 2025) https://home.treasury.gov/news/press-releases/ sb0312.

Fraude en la sanidad

En 2023, los Centros de Medicare y Medicaid informaron que el gasto sanitario en Estados Unidos superó los 4,9 billones de dólares, representando el 17,6 por ciento del PIB del país.[31] La cantidad de fondos disponibles para la explotación la convierte en un objetivo atractivo tanto para criminales nacionales como internacionales. El fraude sanitario cuesta a los contribuyentes entre el tres y el diez por ciento del gasto total en sanidad, estimado entre 147.000 y 490.000 millones de dólares.

Los delincuentes participan en varios tipos de esquemas de fraude sanitario, incluyendo fraude de sobornos y derivaciones, fraude en telemedicina, upcoding, desagregación, facturación duplicada, diagnósticos falsos y fraude relacionado con servicios y equipos innecesarios.[33] Clínicos y administradores cómplices a menudo trabajan dentro de las mismas redes para ocultar el esquema y enmascarar la recepción de fondos mal habidos. Los propietarios de negocios también son infractores frecuentes, ya sea a través de sus entidades legales o como individuos solitarios que se aprovechan de compañías de seguros y programas gubernamentales. Estas personas pueden hacerse pasar por profesionales sanitarios o asumir la identidad de otra persona para utilizar su seguro. También se pueden presentar [34] reclamaciones falsas para pacientes que no existen. El fraude sanitario también se cruza directamente con el fraude en beneficios gubernamentales, principalmente porque los programas más afectados —como Medicare, Medicaid y TRICARE—están financiados con fondos públicos y administrados por agencias gubernamentales.

En junio de 2025, el DOJ anunció los resultados de su Retirada Nacional de Fraude en Atención Sanitaria de 2025 (Takedown), que resultó en cargos penales contra 324 acusados, incluidos 96 médicos, enfermeros especialistas, farmacéuticos y otros profesionales médicos titulados, en 50 distritos federales y 12 oficinas de fiscales generales estatales en todo Estados Unidos, por su presunta participación en diversos planes de fraude sanitario que implicaron más de 14.600 millones de dólares en pérdidas previstas. La retirada involucró a agencias federales y estatales de aplicación de la ley en todo el país y representa un esfuerzo sin precedentes para combatir esquemas de fraude sanitario que explotan a pacientes y contribuyentes. [35]

Como parte de la retirada, Estados Unidos imputó a 11 acusados en un esquema de fraude sanitario multimillonario que representa el mayor importe caso por pérdida jamás imputado por el Departamento de Justicia. En el caso, apodado "Operación Fiebre del Oro" por las fuerzas del orden, 11 acusados, incluidos miembros de una TCO con sede en Rusia y otros lugares, supuestamente orquestaron un esquema multimillonario de fraude sanitario y blanqueo de capitales para robar al programa Medicare y a las compañías privadas de seguros de salud. El TCO adquirió decenas de empresas de equipos médicos duraderos (DME) que ya tenían la capacidad de presentar reclamaciones a Medicare y a aseguradoras suplementarias de Medicare. El TCO ejecutaba estas compras pagando a ciudadanos extranjeros y otros para que actuaran como propietarios nominales de las empresas DME. La TCO creó entonces registros corporativos ficticios que indicaban falsamente que los propietarios nominados controlaban las empresas DME cuando, en realidad, estaban controladas por la dirección extranjera de la TCO. Tras obtener el control de las empresas de DME, rápidamente presentó miles de millones de dólares en reclamaciones falsas y fraudulentas de sanidad a Medicare. El TCO lo hizo robando las identidades e información personal identificativa de más de un millón de estadounidenses en total 50 estados, incluyendo ancianos y estadounidenses con discapacidad. El TCO presentó más de 10.600 millones de dólares en reclamaciones fraudulentas de Medicare por DME.

31 Centros de Servicios de Medicare y Medicaid "Datos Nacionales de Gastos Sanitarios – Históricos" (18 de diciembre de 2024) https://www.cms.gov/ datos-investigación/estadísticas-tendencias-y-reportes/datos-nacional-de gastos en salud/históricos.

32 Según la GAO, en 2023 se realizaron más de 100.000 millones de dólares en pagos indebidos relacionados con Medicare y Medicaid. Esto incluye pagos que fueron por una cantidad incorrecta o que no deberían haberse realizado en absoluto. Este total no incluye posibles pagos por fraude realizados en relación con seguros privados u otros programas sanitarios gubernamentales. GAO, "Medicare y Medicaid: Acciones adicionales necesarias para mejorar la integridad del programa y ahorrar miles de millones," (16 de abril de 2024) https://www.gao.gov/assets/gao-24-107487.PDF.

33 Upcoding es un esquema en el que los profesionales presentan múltiples reclamaciones por el mismo servicio, ya sea a la misma aseguradora o a varias aseguradoras. El desagregado se refiere a la presentación de múltiples facturas por servicios que se supone deben facturarse juntos a una tarifa reducida. Esto incrementa el reembolso de forma injusta.

34 FBI, "Fraude en la atención sanitaria," (consultado en julio de 2025) https://www.fbi.gov/investigate/white-collar-crime/health-care-fraud.

35 DOJ, "Desmantelamiento por fraude nacional en la atención sanitaria resulta en 324 acusados en relación con más de 14.600 millones de dólares en presunto fraude," (30 de junio de 2025) https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection- más de 146 años.

En otro caso, dos residentes de California se declararon culpables en relación con su participación en un esquema de fraude de Medicare de casi 16 millones de dólares que involucraba a empresas falsas de hospicio que facturaban por servicios innecesarios o inexistentes. Los conspiradores crearon cuatro empresas falsas de hospicio— tres supuestamente propiedad de extranjeros pero controladas por los acusados— y usaron sistemáticamente la información personal de extranjeros para abrir cuentas bancarias, presentar reclamaciones de Medicare y firmar contratos de arrendamiento para ocultar su fraude. Como parte de la operación de blanqueo de capitales, mantuvieron documentos bancarios fraudulentos e identificaciones a nombre de estos supuestos propietarios extranjeros, con uno de los responsables moviendo aproximadamente 3,2 millones de dólares a través de diversas cuentas vinculadas a extranjeros y a empresas falsas. [36]

Fraude en los beneficios gubernamentales

Al igual que ocurre con el fraude sanitario, otros programas gubernamentales, incluidos los programas tradicionales de ayuda por COVID-19, son objetivo de defraudadores extranjeros y nacionales debido a la cantidad de fondos públicos disponibles.[37] El fraude sin control en los mercados y programas gubernamentales de EE. UU. roba a los estadounidenses trabajadores y perjudica al sector público. Las fuerzas del orden continúan descubriendo esquemas de fraude que duraron años y que hicieron grandes esfuerzos para blanquear dinero robado de los contribuyentes de programas de ayuda por COVID-19, incluyendo los Préstamos por Desastres por Lesiones Económicas (EIDL), el Programa de Protección de Nóminas (PPP) y varios programas de desempleo asociados a la pandemia. En un caso, un preparador de impuestos fue declarado culpable por un jurado de su esquema que buscaba más de 170 millones de dólares en devoluciones fraudulentas de impuestos al Servicio de Impuestos Internos (IRS), provocando la presentación de más de 1.900 declaraciones falsas ante el IRS reclamando créditos fiscales laborales relacionados con la COVID-19. Según los documentos de este caso y las pruebas en el juicio, el hombre logró que el gobierno pagara más de 55 millones de dólares en reembolsos. Durante todo el programa, también cobraba a los clientes un porcentaje de los cheques de reembolso como honorarios y solicitaba pagos en efectivo. No declaró el dinero que recibió de sus clientes, evadiendo así sus propios impuestos. [38]

La Seguridad Social, las prestaciones para veteranos, los programas de nutrición y otros programas financiados por el gobierno también suelen ser objetivo de estafadores. Por ejemplo, en noviembre de 2025, el Departamento de Justicia anunció cargos contra el 78º acusado en el esquema de fraude Feeding Our Future, un esquema de fraude de 300 millones de dólares que explotó un programa federal de nutrición infantil durante la pandemia de COVID-19. Según se establece en la acusación, entre marzo de 2021 y febrero de 2022, la organización sin ánimo de lucro y su presidente recibieron 1,1 millones de dólares en fondos del Programa Federal de Nutrición Infantil de Feeding Our Future. Sin embargo, poco de ese dinero fue utilizado por el hombre para comprar comida. En cambio, el individuo y un co-conspirador blanquearon la mayor parte del dinero de los contribuyentes para sus familias y para sí mismos. La persona utilizó su parte de los beneficios del fraude para viajar y comprar bienes raíces en Minnesota.[41] Estados Unidos continúa combatiendo el fraude en beneficios gubernamentales, en particular, el fraude rampante y generalizado en estos programas en Minnesota.[42] El gobierno de EE. UU. está actualmente llevando a cabo múltiples investigaciones activas, en curso y exhaustivas sobre la actividad fraudulenta que ha ocurrido en varios programas gubernamentales en Minnesota, incluyendo los programas estatales Feeding Our Future, Housing Stabilization Services y Early Intensive Development and Behavioral Intervention.
[43]

36 DOJ, "Dos residentes de California declaran culpables en relación con un esquema de fraude en hospicios de 16 millones de dólares y esquema de blanqueo de capitales," (8 de julio de 2025) https://www.justice.gov/opa/pr/two-california-residents-plead-guilty-connection-16m-hospice-fraud-scheme-and-money.

37 La Casa Blanca, "Protegiendo la cuenta bancaria de Estados Unidos contra el fraude, el desperdicio y el abuso," (25 de marzo de 2025) https://www.whitehouse.gov/ presidentes-actions/2025/03/protecting-americas-bank-account contra-fraude-desperdicio-y-abuso/.

38 DOJ, "Preparador de impuestos de Nueva Jersey condenado por un esquema de crédito fiscal COVID-19 de 170 millones de dólares," (19 de noviembre de 2025) https://www.justice.gov/ usao-nj/pr/new-jersey-tax-preparer-convicted-170-million-covid-19-tax-credit-tax-scheme.

39 *Véase, por ejemplo,* DOJ, "Empleado de la Seguridad Social se declara culpable de esquema de fraude multimillonario," (5 de junio de 2025) https://www.justice.gov/ usao-sdtx/pr/social-security-employee-pleads-guilty-multimillion-dollar-fraud-scheme; DOJ, "Mujer de Austin condenada por estafa de 25 años de la Seguridad Social," (21 de agosto de 2025) https://www.justice.gov/usao-mn/pr/austin-woman-sentenced-25-year-social-security-scam.

40 *Véase, por ejemplo,* el DOJ, "Tres personas acusadas en un esquema para defraudar al Departamento de Asuntos de Veteranos por más de 9,1 millones de dólares," (2 de mayo de 2025) https:// www.justice.gov/opa/pr/three-individuals-charged-scheme-defraud-department-veterans-affairs-over-91m.

41 DOJ, "78º acusado de alimentar nuestro futuro esquema de fraude," (24 de noviembre de 2025) https://www.justice.gov/usao-mn/pr/78th acusado-acusado-alimentar-nuestro-futuro-fraude-scheme.

42 FinCEN, "Alerta FinCEN sobre redes de fraude y su explotación de programas federales de nutrición infantil en Minnesota," (9 de enero de 2026) https:// www.fincen.gov/system/files/2026-01/FinCEN-Alert-Federal-Child-Nutrition-Programs.pdf.

43 Véase Tesorería, "El Secretario Bessent anuncia iniciativas para combatir el fraude rampante en Minnesota," (9 de enero de 2026) https://home. treasury.gov/news/press-releases/sb0354; DOJ, "Seis acusados adicionales acusados, un acusado se declara culpable de esquemas de fraude en curso," (18 de diciembre de 2025) https://www.justice.gov/usao-mn/pr/six-additional-defendants-charged-one-defendant-pleads-guilty-esquemas de fraude en curso.

En respuesta a la ola continua de fraudes dirigida a programas y beneficios del gobierno federal, la Administración Trump anunció la próxima creación de una nueva división del DOJ centrada en la aplicación nacional del fraude.[44] La nueva división hará cumplir las leyes penales y civiles federales contra el fraude dirigido a programas del gobierno federal, prestaciones financiadas federalmente, empresas, organizaciones sin ánimo de lucro y ciudadanos privados en todo el país. Estos esfuerzos de aplicación, junto con las iniciativas existentes en todo el gobierno federal, servirán para combatir los esfuerzos de explotación de los programas gubernamentales mediante el desperdicio, el fraude y el abuso.

Estafas de confianza

Las estafas de confianza abarcan una amplia variedad de planes en los que los agresores engañan o manipulan a las víctimas para que realicen pagos autorizados o proporcionen información que permita a los delincuentes hacer pagos en nombre de la víctima. Durante una estafa de confianza, la víctima cree que está realizando una transacción legítima, ya sea para realizar un negocio normal, resolver un problema técnico o legal, o ayudar a alguien necesitado. En 2024, las víctimas reportaron pérdidas al IC3 por un total de más de 5.500 millones de dólares debido a diversos tipos de estafas de confianza.46 Como ocurre con otras cantidades de pérdidas reportadas por las víctimas, este total probablemente subestima las pérdidas reales en miles de millones de dólares.

Las estafas de confianza suelen ser perpetradas por estafadores con base en el extranjero, incluidos TCOs, bandas o individuos, y pueden llevar a cabo varios esquemas diferentes utilizando distintos métodos.[47] empresas y consumidores están siendo inundados con mensajes de estafa en casi todas las plataformas de comunicación. Según la FTC, las víctimas son contactadas por correo electrónico, llamada telefónica, mensaje de texto, redes sociales y páginas web/aplicaciones, todas las cuales permiten perpetrar estas estafas desde cualquier parte del mundo. Las estafas originadas en redes sociales por las mayores pérdidas reportadas por víctimas, que sumaron casi 1.900 millones de dólares en 2024, pero las estafas derivadas de llamadas telefónicas provocan la mayor pérdida mediana reportada por víctima, con 1.500 dólares. Esto. se debe en parte a que los estafadores pueden falsificar números de teléfono e información de identificador de llamadas, facilitando convencer a las víctimas de que están hablando con actores legítimos.[49]

Cuatro de las estafas de confianza más comunes incluyen el compromiso de correo electrónico empresarial (BEC), las estafas de suplantación, las estafas románticas y las estafas con adelantos de honorarios.

Compromiso de correo electrónico empresarial

Los perpetradores de compromiso de correo electrónico empresarial (BEC) se apoderan de direcciones de correo legítimas o crean sus propias direcciones que parecen similares a una dirección de correo electrónico empresarial legítima para comunicarse con las víctimas.[50] perpetradores envían entonces instrucciones de transferencia bancaria falsas para transacciones comerciales normales que dirigen los fondos a cuentas bancarias controladas por los perpetradores o sus cómplices. Las quejas y pérdidas de BEC reportadas al IC3 han sido relativamente

44 La Casa Blanca, "Hoja informativa: El presidente Donald J. Trump establece nueva División del Departamento de Justicia para la Aplicación Nacional del Fraude," (8 de enero de 2026) https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-establishes-nueva división del Departamento de Justicia para la aplicación nacional del fraude.

45 Véase la sección de Ciberdelitos para esquemas en los que las víctimas son extorsionadas o coaccionadas para realizar pagos o situaciones en las que se realizan pagos no autorizados contra las cuentas de la víctima usando credenciales robadas.

46 IC3, "Internet Crime Report 2024," (abril de 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. Este total incluye las pérdidas reportadas por Compromiso de Correo Empresarial, Soporte Técnico, Confianza/Romance, Suplantación Gubernamental, Lotería/Sorteo/Herencia y estafas de adelanto de comisión.

47 *Véase, por ejemplo,* el Departamento de Justicia, "Hombre nigeriano se declara culpable tras extradición por participar en estafas románticas y otros esquemas de fraude dirigidos a víctimas mayores," (24 de septiembre de 2024) https://www.justice.gov/usao-sdny/pr/nigerian-man-pleads-guilty-after-extradition-participating-estafas románticas y otros.

48 FTC, "Todos los informes de fraude por método de contacto," (6 de mayo de 2025) https://public.tableau.com/app/profile/federal.trade.commission/viz/ FraudReports/PaymentContactMethods.

49 Comisión Federal de Comunicaciones (FCC), "Suplantación del identificador de llamadas" (actualizado el 13 de noviembre de 2024) https://www.fcc.gov/consumers/guides/spoofing.

50 *Véase, por ejemplo,* el Departamento de Justicia, "Un ciudadano nigeriano se declara culpable de blanquear millones en beneficios criminales vinculados a estafas románticas y esquemas de compromiso de correos electrónicos empresariales," (28 de marzo de 2025) https://www.justice.gov/usao-ndtx/pr/nigerian-national-pleads-guilty-laundering-millones de beneficios criminales vinculados-romance; DOJ, "Nacionalidad nigeriana extraditada sentenciada a ocho años de prisión por esquema de

compromiso de correo electrónico empresarial," (5 de diciembre de 2024) https://www.justice.gov/usao-ct/pr/extradited-nigerian-national-sentenced-eight-years-prisión-empresa-correo electrónico comprometido

estable en los últimos tres años. En 2024, el IC3 recibió 21.422 quejas asociadas a más de 2.700 millones de dólares en pérdidas, lo que lo convierte en la segunda categoría de pérdida total más alta después del fraude de inversión. [51]

Estafas de suplantación

Las estafas de suplantación abarcan varios esquemas diferentes en los que los perpetradores se hacen pasar por soporte técnico, empleados gubernamentales o empleados bancarios [52] para convencer a las víctimas de pagar para resolver asuntos técnicos, legales o financieros inexistentes o entregar sus bienes a supuestos agentes gubernamentales para su custodia durante investigaciones policiales inexistentes. Las estafas de suplantación provienen principalmente de centros de llamadas con sede en India, pero a menudo dependen de mulas de dinero con base en EE. UU. para recibir y blanquear los fondos. Las estafas de soporte técnico [53] suelen comenzar con correos electrónicos, mensajes de texto, llamadas telefónicas o anuncios maliciosos que indican que hay un problema con el ordenador de la víctima que debe resolverse llamando al soporte técnico.[54] Cuando las víctimas llaman al número proporcionado, los estafadores se presentan como soporte técnico legítimo para empresas conocidas y a menudo permanecen horas al teléfono para guiar a la víctima en la compra y activación de tarjetas regalo para resolver el problema inexistente.

Las estafas de suplantación gubernamental suelen comenzar con llamadas de estafadores con números falsificados que parecen ser de un gobierno o de una agencia policial.[55] Los estafadores usan un tono urgente o agresivo para convencer a las víctimas de que deben actuar rápidamente para resolver un problema, como pagar una multa por no asistir al servicio de jurado o dejar sus bienes en manos del gobierno para su custodia porque su identidad se utilizó para facilitar un delito. A continuación, se les indica que compren tarjetas regalo o depositen dinero en efectivo en un quiosco de activos digitales[56] para pagar rápidamente la supuesta multa.[57] En algunos casos, se indica a las víctimas que liquiden cuentas bancarias y de jubilación y conviertan sus activos en efectivo o lingotes de oro para que los supuestos agentes gubernamentales los recojan.[58] Los perpetradores suelen dirigirse a personas mayores en estos esquemas. Aproximadamente el 98 por ciento de estas pérdidas fueron reportadas por personas mayores de 60 años. Estafas donde las víctimas convierten sus bienes a los lingotes de oro, que recogen las mulas de dinero puede ser especialmente devastador.60 En 2024, las víctimas denunciaron 525 incidentes de este tipo al IC3, lo que resultó en pérdidas totales superiores a 219.000.000 de dólares, una media de más de 417.000 dólares por víctima. [61]

---

51 IC3, "Internet Crime Report 2024," (abril de 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

52 Véase IC3, "Fraude en la toma de control de cuentas mediante suplantación de apoyo a instituciones financieras," (25 de noviembre de 2025) https://www.ic3.gov/PSA/2025/PSA251125.

53 IC3, "Internet Crime Report 2022," (23 de abril de 2025) p.14, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf; *véase, por ejemplo,* DOJ, "Ciudadanos indios condenados por conspiración de blanqueo de dinero que arrebató ahorros de toda la vida a víctimas en Ohio, Michigan, Illinois e Indiana," (4 de febrero de 2025) https://www.justice.gov/usao-ndoh/pr/indian-nationals-convicted-money-laundering-conspiracy-took-life- víctimas de ahorros-Ohio

54 FTC, "Cómo detectar, evitar e informar estafas de soporte técnico," (actualizado septiembre de 2022) https://consumer.ftc.gov/articles/how-spot-evitar y reportar estafas de soporte técnico.

55 agencias gubernamentales estadounidenses han advertido sobre estas estafas. *Véase, por ejemplo,* FinCEN, "Alerta sobre esquemas de fraude que abusan del nombre, insignia y autoridades de FinCEN para obtener beneficio económico," (18 de diciembre de 2024) https://www.fincen.gov/system/files/2024-12/Alert-FinCEN-Scams- FINAL508.pdf; DEA, "Alerta de estafa", https://www.dea.gov/scam-alert; FTC, "No, ese no es un comisionado de la FTC al teléfono," (19 de septiembre de 2025) https://consumer.ftc.gov/consumer-alerts/2025/09/no-that's-not-ftc-commissioner-phone. Los estafadores también pueden hacerse pasar por agentes de la ley extranjeros. Véase IC3, "Delincuentes se hacen pasar por proveedores de seguros de salud estadounidenses y fuerzas del orden chinas para atacar a hablantes de chino residentes en Estados Unidos," (13 de noviembre de 2025) https://www.ic3.gov/PSA/2025/PSA251113.

56 Véase la sección de Activos Digitales para un debate más detallado sobre el uso de quioscos de activos digitales en la financiación ilícita.

57 FinCEN, "Aviso sobre el uso de quioscos de moneda virtual convertibles para pagos fraudulentos y otras actividades ilícitas," (4 de agosto de 2025), pp. 6– 7, https://www.fincen.gov/sites/default/files/shared/FinCEN-Notice-CVCKIOSK.pdf.

58 FTC, "Falsa alarma, estafa real: cómo los estafadores están robando los ahorros de toda la vida de los adultos mayores," (7 de agosto de 2025) https://www.ftc.gov/news-events/ visualizaciones de datos/foco de datos/2025/08/falsa alarma-estafa-real-estafa-cómo-estafadores-están-robando-ahorros-de toda una vida.

59 FBI, "FBI Boston advierte sobre aumento de estafas de mensajería con lingotes de oro y efectivo a granel," (22 de septiembre de 2025) https://www.fbi.gov/contact-us/field- oficinas/Boston/noticias/FBI-Boston advierte sobre un aumento en estafas de mensajería en lingotes de oro y efectivo a granel.

60 FBI, "Estafadores utilizan mensajeros para recuperar dinero y metales preciosos de víctimas de estafas de soporte

técnico y suplantación gubernamental," (29 de enero de 2024) https://www.ic3.gov/PSA/2024/PSA240129.

61 IC3, "Internet Crime Report 2024," (abril de 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

Estafas románticas

Los estafadores románticos crean personajes falsos para mantener relaciones online con las víctimas, ganarse la confianza de las víctimas y solicitar fondos por diversas razones, como una factura médica, un billete de avión para visitar a la víctima o incluso conceder un préstamo al supuesto negocio de su pareja.[62] Agresores solicitarán a sus víctimas en redes sociales, aplicaciones de citas, mensajes de texto u otras aplicaciones de mensajería. Los perpetradores, a menudo radicados en Nigeria o Ghana, operan en grupos poco conectados, siguen guiones similares para llevar a cabo sus planes y dependen de mulas de dinero con base en EE.UU. para blanquear beneficios ilícitos. Black Axe, una TCO con sede en Nigeria que opera en varios países, es un grupo criminal destacado que organiza estafas románticas y otras cosas.[63] A veces los agresores utilizan víctimas de estafas románticas para blanquear los beneficios ilícitos de otras estafas. [64]

Estafas con adelantos de pago

En las estafas de pago anticipado, las víctimas reciben un aviso no solicitado, por correo electrónico, redes sociales, mensaje de texto, aplicación de mensajería o correo físico, alegando que tienen derecho a una gran cantidad de dinero, ya sea de una herencia, un premio de lotería o sorteo, o una oportunidad exclusiva de negocio. Los estafadores inducen a las víctimas a pagar por adelantado para cubrir supuestos impuestos o tasas administrativas y acceder a fondos inexistentes, a veces solicitando varias rondas de pagos antes de que las víctimas se den cuenta de que han sido estafadas.[65] En otra variante, los estafadores anuncian empleos falsos en redes sociales o foros de empleo online y dicen a los candidatos que deben pagar tasas anticipadas para conseguir el puesto.66 En 2024, las víctimas reportaron más de 204 millones de dólares en pérdidas al IC3 debido a diversas estafas de adelantos. [67]

Las TCO con sede en México también han atacado a propietarios estadounidenses de multipropiedades en México mediante estafas de adelanto de tarifas que operan desde centros de llamadas. Según el FBI, el Cartel terrorista Jalisco Nueva Generación (CJNG), el Cartel de Golfo y el Cartel de Sinaloa llevan más de 10 años llevando a cabo esquemas de fraude en multipropiedad para ayudar a financiar sus esfuerzos ilícitos, y CJNG es el cártel dominante que realiza fraudes en México basado en la notificación de denuncias y el rastreo financiero.[68] Entre 2019 y 2024, aproximadamente 6.000 víctimas estadounidenses han reportado pérdidas de aproximadamente 350 millones de dólares atribuibles a esquemas de fraude en tiempos compartidos en México.[69] Los TCOs generalmente obtienen información sobre propietarios estadounidenses de multipropiedades en México de insiders cómplices en resorts de multipropiedad y luego contactan con las víctimas alegando representar compradores, inquilinos o inversores dispuestos como parte de estafas de salida, re-alquiler y inversión de multipropiedad. Los responsables solicitan entonces impuestos o tasas por adelantado para, aparentemente, acelerar la venta. En algunos casos, las víctimas son objeto de estafas posteriores en las que los responsables afirman ser bufetes de abogados con sede en EE. UU. o autoridades gubernamentales de EE. UU. o México que pueden ayudar a recuperar los ingresos perdidos del fraude inicial de multipropiedad. [70]

---

62 FBI, "Romance Scams," (consultado el 11 de julio de 2025) https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and- estafas/romance-scams.

63 *Véase, por ejemplo,* DOJ, "Líder destacado de Black Axe extraditado a Estados Unidos por conspirar para participar en estafas en Internet y blanqueo de dinero," (16 de diciembre de 2024) https://www.justice.gov/usao-nj/pr/prominent-leader-black-axe-extradited-united-states-conspiring-involucrarse-estafas-y; INTERPOL, "La operación INTERPOL asesta un duro golpe contra la delincuencia financiera en África Occidental," (16 de julio de 2024) https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-operation-strikes-major-blow-against-West-African-financial-delito.

64 *Véase, por ejemplo,* DOJ, "Mujer de Pensilvania condenada a prisión federal por su papel en fraude y esquema de blanqueo de capitales," (10 de junio de 2025) https://www.justice.gov/usao-ndia/pr/pennsylvania-woman-sentenced-federal-prison-role-fraud-and-money-laundering-scheme.

65 DOJ, "Hombre sentenciado por estafa de sorteo que ataca a ancianos," (7 de febrero de 2025) https://www.justice.gov/usao-sdca/pr/man estafa de sorteo sentenciada que ataca a ancianos.

66 FTC, "Explicación de estafas laborales" (actualizado agosto de 2024) https://consumer.gov/scams-identity-theft/job-scams-explained.

67 IC3, "Internet Crime Report 2024," (abril de 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. Este total incluye las categorías de "Tarifa Avanzada" y "Lotería/Sorteo".

68 FBI, "Cárteles mexicanos apuntan a estadounidenses en estafas de fraude de tiempo compartido, FBI advierte," (7 de junio de 2024) https://www.fbi.gov/news/stories/mexican-cárteles que atacan estadounidenses en estafas de fraude en tiempo compartido advierte al FBI.

69 DOJ, "Miembro senior de la CJNG acusado de fraude electrónico, blanqueo de dinero y terrorismo por operar un esquema masivo de fraude de tiempo compartido," (22 de septiembre de 2025) https://www.justice.gov/opa/pr/senior-cjng-member-indicted-wire-fraud-money-laundering-and- cargos de terrorismo-operando.

70 FinCEN, OFAC & FBI, "Aviso conjunto sobre fraude de tiempo compartido asociado con organizaciones criminales

transnacionales con sede en México," (16 de julio de 2024) https://www.fincen.gov/sites/default/files/shared/FinCEN-Joint-Notice-Timeshare-Mexico-508C-FINAL.pdf.

Explotación financiera de ancianos

La explotación financiera de personas mayores (EFE), una forma de abuso a personas mayores, implica el uso o explotación indebido del dinero, bienes o información personal de una persona mayor con fines económicos.[El 71] EFE puede ser perpetrado por familiares y amigos, profesionales de confianza o completos desconocidos.[72] Los adultos mayores suelen ser objetivo de diversos tipos de robos y estafas de confianza porque los perpetradores creen que tienen mayores ahorros acumulados, capacidades cognitivas o físicas en declive, menos contactos sociales que podrían impedir el esquema y menos familiaridad con la tecnología utilizada para llevar a cabo el esquema.[73] En 2024, adultos mayores de 60 años reportaron pérdidas totales de casi 4.900 millones de dólares en el IC3 en todos los tipos de fraude y estafa habilitados por internet, un aumento del 44 % respecto al año anterior.[74] instituciones financieras presentaron más de 155.000 informes de actividad sospechosa (SARs) asociados a más de 27.000 millones de dólares en actividades sospechosas reportadas en el año posterior a la publicación de un Aviso EFE por FinCEN en junio de 2022.[75]

Además de los otros esquemas de fraude descritos anteriormente, los adultos mayores también son objetivo de estafas específicas para personas mayores, como las estafas de Medicare o de abuelos. En las estafas de abuelos, los estafadores contactan por teléfono con las víctimas y dicen que un familiar cercano, generalmente un nieto, ha sido arrestado tras un accidente de coche u otro incidente y necesita dinero para la fianza o la representación legal. En un caso reciente, 25 ciudadanos canadienses fueron acusados de presuntamente operar una estafa de abuelos desde centros de llamadas en Montreal y sus alrededores. Se convenció a las víctimas para que entregaran dinero bajo fianza a supuestos "fiadores" que acudirían a la casa de la víctima para cobrar el dinero. Los fondos se transmitían luego a Canadá tras entregas de efectivo y transacciones financieras, a veces involucrando activos digitales.[76]

Enfoque especial: Uso de la IA en fraudes y estafas

Desde 2022, la disponibilidad comercial de grandes modelos de lenguaje (LLMs) ha provocado una explosión en el uso de herramientas avanzadas de IA. Estas herramientas de IA tienen varias aplicaciones útiles, como redactar textos, explicar temas complejos, escribir código y generar contenido multimedia, incluyendo imágenes, audio y vídeo. Sin embargo, estas mismas capacidades están siendo aprovechadas por los estafadores para robar a ciudadanos y empresas estadounidenses. Según el FBI, los delincuentes utilizan texto, imágenes, audio y vídeo generados por IA para cometer fraude a mayor escala y aumentar la credibilidad de sus planes.[77] En los primeros siete meses de 2025, IA representó más de 9.000 quejas a IC3, y esas quejas abarcaron todo tipo de estafas.[78]

---

71 Gobierno de EE. UU., "Declaración Interinstitucional sobre la Explotación Financiera de Personas Mayores," (4 de diciembre de 2024) https://www.occ.gov/news-issuances/ comunicados de prensa/2024/nr-ia-2024-130a.pdf.

72 DOJ, "Iniciativa de Justicia para Mayores – Explotación Financiera," (consultado el 14 de julio de 2025) https://www.justice.gov/elderjustice/financial- explotación-0. *Véase también,* DOJ, "El Departamento de Justicia publica el informe anual 2025 al Congreso sobre los esfuerzos para combatir el fraude y abuso de personas mayores" (17 de noviembre de 2025) https://www.justice.gov/opa/pr/department-justice-releases-2025-annual-report-congress-efforts-combat- fraude y abuso de ancianos.

73 Ver Alerta de Inversor de la SEC "Detectando y reportando estafas de inversión dirigidas a inversores mayores," (5 de febrero de 2024), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/spotting-and-reporting-investment-scams- targeting investors-older-investors.

74 IC3, "Internet Crime Report 2024," (abril de 2025) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

75 FinCEN, "Explotación financiera de ancianos: Patrón de amenazas e información sobre tendencias, junio de 2022 a junio de 2023," (abril de 2024), p. 1, https:// www.fincen.gov/sites/default/files/shared/FTA_Elder_Financial_Exploitation_508Final.pdf; FinCEN, "Advisory on Aged Financial Exploitation" (15 de junio de 2022) https://www.fincen.gov/system/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20 Exploitation%20FINAL%20508.pdf.

76 DOJ, "25 ciudadanos canadienses acusados en Vermont en relación con una 'estafa de abuelos' multimillonaria a nivel nacional", (4 de marzo de 2025) https://www.justice.gov/usao-vt/pr/25-canadian-nationals-charged-vermont-connection-nationwide-multimillion-dollar.

77 *Véase, por ejemplo,* IC3, "Los delincuentes utilizan inteligencia artificial generativa para facilitar el fraude financiero," (3 de diciembre de 2024) https://www.ic3.gov/ PSA/2024/PSA241203; IC3, "Altos funcionarios estadounidenses siguen siendo suplantados en campaña de mensajes maliciosos," (19 de diciembre de 2025) https://www.ic3.gov/PSA/2025/PSA251219; Asociación Americana de Banqueros y FBI, "La Fundación ABA y el FBI lanzan nueva infografía para ayudar a los estadounidenses a detectar y evitar estafas de deepfake," (3 de septiembre de 2025) https://www.aba.com/about-us/press-room/press-releases/ABA- Infografía conjunta de la Fundación y el FBI sobre estafas de deepfake.

78 IC3, "No dejes que los estafadores arruinen tu temporada navideña," (8 de diciembre de 2025)

https://www.fbi.gov/news/press-releases/dont-let-scammers- arruina tu temporada navideña.

Los estafadores utilizan IA y otras tecnologías para crear perfiles falsos en redes sociales, clones de voz, documentos de identificación y vídeos con representaciones creíbles de figuras públicas o incluso seres queridos, lo que acelera los riesgos existentes de phishing (basado en correo electrónico), smishing (basado en texto por SMS), vishing (basado en voz y vídeo) e ingeniería social mediante la creación de mensajes altamente convincentes que son difíciles de detectar para los consumidores.[79] Esto incluye a defraudadores extranjeros que utilizan herramientas de IA para ayudar en traducciones de idiomas y evitar errores gramaticales o ortográficos al atacar a víctimas estadounidenses, permitiéndoles enviar contenido creíble a más víctimas más rápidamente. [80]

Las fuerzas del orden y los reguladores también advierten que los delincuentes pueden utilizar contenido mediático "deepfake", como imágenes, vídeos y documentos generados por IA, para ayudar en sus intentos de perpetrar fraudes y eludir las comprobaciones de identificación de clientes en instituciones financieras estadounidenses.[81] Criminales crean estas imágenes deepfake modificando una imagen fuente auténtica o creando una imagen sintética, y también han combinado imágenes generadas por IA con información personal identificable (PII) robada u obtenida fraudulentamente o completamente falsa para crear identidades sintéticas. El análisis de FinCEN de los datos de la BSA también muestra que actores maliciosos han abierto con éxito cuentas usando identidades fraudulentas sospechosas de haber sido producidas con IA generativa y han utilizado esas cuentas para recibir y blanquear los beneficios de otros esquemas de fraude. [82]

Actualización: Fraude de cheques

El fraude de cheques es el uso ilícito de cheques en papel o digitales para obtener acceso no autorizado a fondos. El uso de cheques sigue disminuyendo,83 pero el fraude con cheques sigue siendo un problema persistente para consumidores, empresas y el gobierno.[84] Estafadores se dirigen a los cheques porque pueden ser adquiridos y explotados mediante métodos de baja tecnología como el lavado de cheques y la falsificación. Según las fuerzas del orden estadounidenses, un volumen significativo de fraude con cheques se ve facilitado por el robo de correo.[85] Según informes de la BSA, las técnicas utilizadas para adquirir y modificar cheques robados varían mucho en sofisticación. [86]

Los delincuentes suelen atacar cheques gubernamentales o empresariales creyendo que las cuentas subyacentes están bien financiadas y les permitirán robar cantidades mayores.[87] Reconociendo la amenaza que supone el fraude de cheques gubernamentales, comenzando

79 IC3, "Altos funcionarios estadounidenses suplantados en campaña de mensajes maliciosos," (15 de mayo de 2025) https://www.ic3.gov/PSA/2025/PSA250515. *Véase también SEC*, "Alerta al inversor: Inteligencia artificial y fraude en inversiones" (25 de enero de 2024), https://www.investor.gov/introduction- inversiones/recursos generales/alertas de noticias/alertas-boletines/alertas-inversores/fraude por inteligencia artificial.

80 Departamento de Servicios Financieros del Estado de Nueva York, "Riesgos de ciberseguridad derivados de la inteligencia artificial y estrategias para combatir riesgos relacionados," (16 de octubre de 2024) https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies- riesgos relacionados con el combate.

81 FinCEN, "Alerta sobre esquemas de fraude que involucran medios deepfake dirigidos a instituciones financieras," (13 de noviembre de 2024), pp. 1– 2, https://www. fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.

82 *Id.* en p. 3.

83 En 2024, los cheques representaron solo el tres por ciento de todos los pagos al consumidor, frente al siete por ciento de 2016. Durante ese mismo periodo, el volumen de cheques comerciales recaudados y de cheques gubernamentales procesados por la Reserva Federal también disminuyó un 43 por ciento y un 38 por ciento, respectivamente. Servicios Financieros de la Reserva Federal, "Hallazgos de 2025 del diario de la elección de pagos al consumidor," (mayo de 2025) https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2025-diary-of-consumer-payment-choice. pdf; Junta de la Reserva Federal (FRB), "Cheques comerciales recogidos a través de la Reserva Federal--Datos anuales" (actualizado el 4 de septiembre de 2025) https://www.federalreserve.gov/paymentsystems/check_commcheckcolannual.htm; FRB, "Cheques gubernamentales procesados por la Reserva Federal--Datos anuales," (actualizado el 4 de septiembre de 2025) https://www.federalreserve.gov/paymentsystems/check govcheckprocannual.htm/.

84 Federal Reserve Financial Services, "El fraude por cheques sigue siendo la principal amenaza — descubre cómo puede ayudar la Reserva Federal Financial Services," (3 de junio de 2025) https://www.frbservices.org/news/fed360/issues/060325/check-fraud-remains-top-threat.

85 FBI y Servicio Postal de Inspección de EE. UU. (USPIS), "El fraude de cheques relacionado con el robo de correo está en aumento," (27 de enero de 2025) https://www.ic3. gov/PSA/2025/PSA250127; *véase también en general* FinCEN, "Alerta de FinCEN sobre el aumento nacional de esquemas de fraude de cheques relacionados con robo de correo dirigidos al correo postal dirigido al correo de EE. UU." (27 de febrero de 2023) https://www.fincen.gov/system/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20 Check%20Fraud%20FINAL%20508.pdf.

86 FinCEN, "Análisis de tendencias financieras: fraude de cheques relacionado con el robo de correo: patrón de amenazas e información sobre tendencias, febrero a agosto de 2023," (septiembre de 2024), p. 5, https://www.fincen.gov/sites/default/files/shared/FTA-Check-Fraud-FINAL508.pdf.

87 *Véase, por ejemplo,* el Departamento de Justicia, "Hombre de Nevada que robó más de 7 millones de dólares en cheques del tesoro, condenado a seis años de prisión," (29 de mayo de 2025) https://www.justice.gov/usao-ut/pr/nevada-man-who-stole-over-7m-treasury-checks-sentenced-six-years-prison.

El 30 de septiembre de 2025, el gobierno federal dejó de emitir cheques en papel para la mayoría de los pagos federales, lo que debería reducir considerablemente una fuente de fraude con cheques.[88] Treasury también pudo recuperar más de 1.000 millones de dólares en el año fiscal 2024 implementando un proceso mejorado mediante IA para mitigar el fraude de cheques casi en tiempo real, fortaleciendo y acelerando procesos para recuperar pagos potencialmente fraudulentos. [89]

Narcotráfico

Los TCOs, incluidos los cárteles internacionales de drogas, producen y trafican ilegalmente drogas que suponen una gran amenaza para la salud pública y la seguridad nacional de EE. UU. Entre 1999 y 2023, más de 800.000 personas en Estados Unidos murieron por sobredosis de opioides, enriqueciendo a los cárteles extranjeros a costa de vidas estadounidenses.[90] muertes por sobredosis de drogas en Estados Unidos disminuyeron casi un 24 por ciento entre 2023 y 2024, pero el fentanilo fabricado ilícitamente sigue siendo el principal causante de muertes por sobredosis y una prioridad máxima para el gobierno estadounidense en la lucha contra el narcotráfico. [91]

Las TCOs con sede en el hemisferio occidental, incluyendo el Cártel de Sinaloa y la CJNG en México, siguen siendo los principales productores y proveedores ilícitos de drogas ilícitas, incluido el fentanilo.[92] TCOs pueden utilizar diversos métodos para blanquear sus ingresos del tráfico de drogas a través del sistema financiero estadounidense, lo que supone riesgos para bancos y MSB, así como para negocios y profesiones no financieras (como abogados y profesionales inmobiliarios). En los últimos años, estos TCOs han utilizado cada vez más CMLNs, que trasladan valor a través de fronteras mediante sistemas informales de transferencia de valor (IVTS), esquemas TBML y activos digitales. [93]

El tráfico de drogas está impulsado por los ingresos ilícitos que los TCO buscan obtener. Esta sección se centra en la financiación relacionada con la producción ilícita de drogas, como empresas químicas extranjeras que suministran precursores de fentanilo y metanfetamina destinados a Estados Unidos, y el posterior blanqueo de capitales de los ingresos ilegales procedentes de la venta de todos los tipos de drogas por parte de actores amenazantes de TCO y blanqueadores profesionales de dinero. [94]

Tipos de fármacos

Según se describe en la Evaluación Nacional de Amenazas de Drogas (NDTA) de 2025 de la Administración para el Control de Drogas (DEA), el fentanilo fabricado por cárteles de drogas con sede en México es el principal motor de las muertes por sobredosis de drogas en Estados Unidos. El 95 Fentanilo se produce ilícitamente utilizando precursores de productos químicos que provienen principalmente de proveedores de productos químicos con sede en China, así como de proveedores de productos químicos con sede en India.[96] Fentanilo, que puede ser 50 veces más fuerte que la heroína, tiene

88 La Casa Blanca, Orden Ejecutiva Nº 14247 – Modernización de los Pagos hacia y Desde la Cuenta Bancaria de Estados Unidos (25 de marzo de 2025) https://www. federalregister.gov/documents/2025/03/28/2025-05522/modernizing-payments-to-and-from-americas-bank-account; Tesorería, "El Tesoro anuncia que el gobierno federal eliminará los cheques en papel el 30 de septiembre ," (14 de agosto de 2025) https://fiscal.treasury.gov/news/paper-checks-going-away.html.

89 Tesoro, "El Tesoro anuncia procesos mejorados de detección de fraude, incluyendo IA por aprendizaje automático, prevenido y recuperado más de 4.000 millones de dólares en el año fiscal 2024," (17 de octubre de 2024) https://home.treasury.gov/news/press-releases/jy2650.

90 Centros para el Control y la Prevención de Enfermedades (CDC), "Comprendiendo la epidemia de sobredosis de opioides" (9 de junio de 2025) https://www.cdc.gov/ overdose-prevention/about/understanding-the-opioid-overdose-epidemic.html.

91 CDC, "CDC informa de casi un 24% de disminución en las muertes por sobredosis de drogas en EE. UU." (25 de febrero de 2025) https://www.cdc.gov/media/ releases/2025/2025-cdc-reports-decline-in-us-drug-overdose-deaths.html.

92 Oficina del Director de Inteligencia Nacional (ODNI), "Evaluación Anual de Amenazas de la Comunidad de Inteligencia de EE. UU.", (marzo de 2025), p. 5, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

93 Véase la sección sobre redes chinas de blanqueo de capitales. *Véase también,* FinCEN, "Aviso FinCEN sobre el uso de redes chinas de blanqueo de dinero por organizaciones criminales transnacionales con sede en México para blanquear ingresos ilícitos," (28 de agosto de 2025) https://www.fincen.gov/ system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

94 Según el Informe del Año 2024 de FinCEN, el mayor porcentaje de investigaciones activas (40 por ciento) estuvo vinculado a los SARs/CTRs del Programa de Control de Drogas contra el Crimen Organizado. Para más información, véase p.2: https://www.fincen.gov/system/files/2025-08/FinCEN- Infographic-Public-2025-508.pdf.

95 DEA, "Evaluación Nacional de la Amenaza de Drogas (NDTA) 2025," (mayo de 2025), https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugTh reatAssessment.pdf.

96 FinCEN, "Financiación ilícita relacionada con el fentanilo: Patrón de amenazas e información de tendencias 2024," (abril de 2025), p. 12, https://www.fincen.gov/system/ archivos/compartidos/FinCEN-FTA-Fentanyl.pdf; DEA, NDTA 2025, p. 8, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatA ssessment.pdf.

o bien sustituyó la heroína o se combina regularmente con heroína y otras drogas en muchos mercados de drogas de EE. UU.[97] Entre 2020 y 2024, el volumen de incautaciones de heroína en Estados Unidos disminuyó más del 77 por ciento, mientras que el volumen de incautaciones de fentanilo se disparó casi un 250 por ciento. El 98 Fentanilo también puede combinarse con otros fármacos, como nitazenos (un opioide sintético) y xilazina (un sedante no opioide), o comprimirse en pastillas falsas, aumentando considerablemente el riesgo de intoxicación y sobredosis. Otras drogas, como la metanfetamina y la cocaína, también son producidas por TCOs fuera de Estados Unidos, introducidas de contrabando en el país y distribuidas y vendidas por organizaciones locales de tráfico de drogas (DTOs) que colaboran con las TCOs. La marihuana, que sigue estrictamente controlada por la ley federal, también puede ser introducida de contrabando en Estados Unidos por TCOs o producida internamente por TCOs o grupos criminales no afiliados. Siete tipos de drogas representan más del 98 por ciento de los delitos de tráfico de drogas, siendo los tres principales relacionados con metanfetamina (46 por ciento), fentanilo y análogos (22 por ciento) y cocaína en polvo (20 por ciento).[99]

Actores de amenaza

Los principales actores amenazantes del TCO incluyen el Cártel de Sinaloa, CJNG, Cartel del Noreste, La Nueva Familia Michoacana, Cartel del Golfo y Carteles Unidos, todos ellos designados como Organizaciones Terroristas Extranjeras (FTOs) y Terroristas Globales Especialmente Designados (SDGTs) en 2025.[100] Estados Unidos está comprometido a utilizar todas las herramientas disponibles para contrarrestar estos TCOs, que están llevando a cabo campañas de violencia y terror contra Estados Unidos y otros países del hemisferio occidental.[101] Dado que los principales actores de la amenaza del TCO son grupos terroristas designados, Estados Unidos puede presentar cargos como narcoterrorismo y apoyo material al terrorismo, que conllevan largas penas de prisión y fuertes multas.[102] Las designaciones FTO también permiten soluciones pragmáticas a la enorme escala del problema de las drogas. Por ejemplo, en septiembre de 2025, las fuerzas del orden estadounidenses incautaron 300.000 kilogramos de precursores de metanfetamina enviados desde China con destino al Cártel de Sinaloa en México bajo la disposición de confiscación terrorista. Entre las autoridades de decomiso, la disposición sobre decomisos por terrorismo se aplica al rango más amplio de bienes e incluye todos los activos extranjeros o nacionales relacionados con un delito federal de terrorismo.[103] Esta fue la mayor incautación de precursores de metanfetamina en la historia de EE. UU. y suficiente para producir aproximadamente 190.000 kilogramos de metanfetamina, con un valor de mercado de hasta 569 millones de dólares. [104]

Sinaloa y CJNG

Los dos mayores actores amenazantes del TCO siguen siendo el Cártel de Sinaloa y CJNG, y siguen desempeñando un papel desproporcionado en la crisis de las drogas, que está matando a decenas de miles de estadounidenses cada año.[105] El Cártel de Sinaloa, uno de los más

97 La Casa Blanca, "Designando el fentanilo como arma de destrucción masiva," (15 de diciembre de 2025) https://www.whitehouse.gov/ acciones presidenciales/2025/12/designando-fentanilo como arma de destrucción masiva/.

98 DEA, 2025 NDTA, p. 21, 33, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

99 USSC, "QuickFacts: Delitos de Tráfico de Drogas FY2024," (mayo de 2025) https://www.ussc.gov/sites/default/files/pdf/research-and- publicaciones/datos rápidos/Drug_Trafficking_FY24.pdf

100 State, "Designación de Cárteles Internacionales", (20 de febrero de 2025) https://www.state.gov/designation-of-international-cartels. Los otros dos TCOs designados como parte de esta orden, Tren de Aragua (TdA) y Mara Salvatrucha (MS-13), se dedican principalmente a actividades de tráfico de drogas a pequeña escala o de nivel minorista, como trabajar como mensajeros de drogas, guardas de casas y distribuidores de drogas en la calle, como parte de sus operaciones criminales más amplias. Véase NDTA 2025, pp. 18-19, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreat Assessment.pdf.

101 Operación Take Back America exige que los Grupos de Trabajo contra el Crimen Organizado contra las Drogas (OCDETF) aumenten los recursos existentes para abordar las prioridades fundamentales de aplicación del Departamento de Justicia: detener la inmigración ilegal, eliminar cárteles y TCOs, y acabar con el tráfico ilegal de drogas y seres humanos peligrosos. La Operación Take Back America también incluirá todos los esfuerzos para atacar a TdA, MS-13, el Cártel de Sinaloa, CJNG, Cartel del Noreste, La Nueva Familia Michoacana, Cartel del Golfo, Carteles Unidos y cualquier otro Cártel o TCO designado conforme al proceso establecido en la Orden Ejecutiva 14157. https://www.justice.gov/dag/media/1393746/dl?inline 102 *Ver, por ejemplo,* DOJ, "Líderes del cártel de Sinaloa acusados de narcoterrorismo, apoyo material al terrorismo y tráfico de drogas," (13 de mayo de 2025) https://www.justice.gov/opa/pr/sinaloa-cartel-leaders-charged-narco-terrorism-material-support-terrorism-and-drug.

103 18 U.S.C. § 981(a)(1)(G) 104 DOJ, "EE.UU. INCAUTA 300.000 KILOS DE QUÍMICOS PRECURSORES DE METANFETAMINA ENVIADOS DESDE CHINA CON DESTINO AL CÁRTEL MEXICANO DE Sinaloa," (3 de septiembre de 2025)

https://www.justice.gov/usao-dc/pr/us-seizes-300000-kilos-meth-precursor-chemicals-sent-china-destined-mexicos-sinaloa- droga.

105 CDC, "Conteos provisionales de muertes por sobredosis de drogas," (actualizado el 13 de agosto de 2025) https://www.cdc.gov/nchs/nvss/vsrr/drug-overdose-data.htm.

poderosos y omnipresentes TCOs en el mundo, es responsable de una parte significativa del fentanilo y otras drogas mortales traficadas hacia Estados Unidos. De manera similar, la CJNG es un cártel brutalmente violento responsable de una parte notable de fentanilo y otras drogas que entran ilícitamente en Estados Unidos. El Cártel de Sinaloa y la CJNG inician el proceso de producción de fentanilo y metanfetamina importando precursores de China y de India.Operan laboratorios clandestinos en México para producir fentanilo, metanfetamina, cocaína y otras drogas ilícitas que luego se trafican hacia Estados Unidos a través de múltiples puertos de entrada. [106]

Gráfico 1: Etapas clave de la cadena de suministro del fentanilo
Precursor Chemicals: China sigue siendo la principal fuente de sustancias utilizadas para producir fentanilo, pero los cárteles parecen estar diversificando su fuente de suministro para incluir proveedores con base en India. Las operaciones comerciales aparentemente legítimas pueden ser abusadas por redes criminales para traficar productos químicos esenciales para el fentanilo y otras drogas. [107]
Producción y fabricación: El Cártel de Sinaloa y CJNG son los principales productores ilícitos de fentanilo destinado a Estados Unidos. Las prensas de pastillas, a menudo importadas de China, pueden usarse para introducir fentanilo en pastillas que se asemejan a medicamentos con receta como la oxicodona.El [108] Fentanilo también se mezcla con otras drogas, incluyendo metanfetamina y cocaína.
Trata y distribución: La mayoría del fentanilo ilícito cruza la frontera entre Estados Unidos y México en vehículos de pasajeros. Debido a la potencia del fentanilo, los cárteles pueden contrabandear cantidades relativamente pequeñas en peso, lo que dificulta su detectación. Una vez en Estados Unidos, las filiales de los cárteles mexicanos facilitan la distribución para ventas a nivel de calle.
Venta y blanqueo de capitales: Para repatriar los ingresos de la droga a México, los cárteles utilizan diversos métodos como el contrabando de efectivo al por mayor, TBML y blanqueadores profesionales de dinero, incluidos los CMLN.

El Cártel de Sinaloa y la CJNG emplean una variedad de métodos de blanqueo de capitales. Es más probable que los TCO más pequeños que dependan de servicios profesionales de blanqueo de capitales, incluidas las CMLN, que mueven grandes sumas de efectivo con empresas pantalla y múltiples cuentas bancarias que ocultan el origen de los fondos. A cambio de una tarifa, es habitual que blanqueadores profesionales actúen como MSB no autorizados que:1) depositan efectivo en instituciones financieras de todo Estados Unidos; 2) transferir fondos por transferencias bancarias, cheques y transferencias interbancarias; y 3) transferir dinero a México en nombre de terceros.[109] Además, se sabe que el Cártel de Sinaloa utiliza sus propias filiales para blanquear dinero de Estados Unidos hacia México. [110]

106 Véase FinCEN, "Aviso suplementario sobre la adquisición de productos químicos precursores y equipos de fabricación utilizados para la síntesis de fentanilo ilícito y otros opioides sintéticos" (20 de junio de 2024), p. 3, https://www.fincen.gov/system/files/advisory/2024-06-20/FinCEN-Supplemental-Advisory-on-Fentanyl-508C.pdf; y FinCEN, "Financiación ilícita relacionada con el fentanilo: información sobre patrones y tendencias de amenazas 2024" (abril de 2025) https://www.fincen.gov/system/files/shared/FinCEN-FTA-Fentanyl.pdf.

107 En septiembre de 2025, OFAC designó Guangzhou Tengyue Chemical Co., Ltd., una empresa química dedicada a la fabricación y venta de opioides sintéticos. Guangzhou Tengyue explotó canales comerciales legítimos para traficar drogas ilícitas hacia Estados Unidos. Tesorería, "Hacienda sanciona a una empresa química con sede en China para combatir el tráfico de opioides sintéticos," (3 de septiembre de 2025) https:// home.treasury.gov/news/press-releases/sb0235.

108 *véase, por ejemplo,* DOJ, "Empresa china y tres ciudadanos chinos acusados de importar ilegalmente equipo para fabricar pastillas utilizado para fabricar sustancias controladas," (12 de mayo de 2025) https://www.justice.gov/opa/pr/chinese-company-and-three-chinese-nationals- acusados-importar-fabricar-pastillas.

109 *Ver, por ejemplo,* DOJ, "Ohio Siblings Sentenceed for Laundering $784,045 in Drug Proceedes" (21 de agosto de 2025) https://www.justice.gov/opa/pr/ ohio-siblings-sentenceed-laundering-784045-drug-proceeds.

110 En marzo de 2025, la OFAC designó a seis individuos y siete entidades implicados en una de las redes de blanqueo de capitales del Cártel de Sinaloa. Las actividades de la red incluían el uso de esquemas de arbitraje de divisas, la creación de negocios y representantes empresariales, y la coordinación de recogidas de efectivo en nombre de la organización. Tesorería, "Hacienda sanciona a operadores criminales y blanqueadores de dinero para el notorio cártel de Sinaloa," (31 de marzo de 2025) https://home.treasury.gov/news/press-releases/sb0064.

Tanto Sinaloa como CJNG son conocidos por utilizar activos digitales para comprar productos químicos precursores, blanquear y repatriar fondos, y para otros fines.[111] Como se describe en la NDTA de 2025, el uso de activos digitales acelera el blanqueo de ingresos por drogas, porque los blanqueadores profesionales están dispuestos a liberar inmediatamente una cantidad equivalente de activos digitales tan pronto como reciben efectivo en gran cantidad de los TCOs. En la evaluación, la DEA también destaca específicamente el uso por parte de CJNG de intercambios de activos digitales para blanquear los ingresos de la droga. [112]

Además de explotar a las instituciones financieras estadounidenses, los cárteles también explotan a las instituciones financieras mexicanas para repatriar y blanquear sus fondos. En junio de 2025, FinCEN identificó tres instituciones financieras con sede en México como de principal preocupación por el blanqueo de capitales en relación con el tráfico ilícito de opioides y facilitando pagos por la adquisición de químicos precursores para producir fentanilo, así como actividades de lavado que benefician al Cártel de Sinaloa, CJNG y otros TCOs. [113]

Otros TCOs y actores de amenazas

En comparación con el Cártel de Sinaloa y CJNG, otros TCOs, como Cartel del Noreste (CDN), La Nueva Familia Michoacana (LNFM), Cartel de Golfo (CDG), Carteles Unidos (CU), Tren de Aragua (TdA) y Mara Salvatrucha (MS-13) desempeñan un papel menor conocido en la producción, tráfico y venta ilícita de drogas en Estados Unidos, pero también participan en una amplia variedad de delitos. Estados Unidos está comprometido a garantizar que cada uno de estos FTOs no se convierta en el próximo gran actor en el mercado interno de drogas ilícitas. [114]

La facción Los Mayos del Cártel de Sinaloa proporciona a CDN fentanilo, metanfetamina y cocaína ilícitos, que se introduce de contrabando en Estados Unidos y luego se distribuye y vende a través de rutas bajo control del Cártel de Sinaloa. El CDN está involucrado en una amplia variedad de actividades criminales, incluyendo secuestro, extorsión, robo de vehículos, tráfico de personas, blanqueo de capitales, prostitución y robos a mano armada.

LNFM y CU son importantes TCOs con sede en el estado mexicano de Michoacán. CU opera como un conglomerado de varias facciones poderosas que trafican con fentanilo, metanfetamina, cocaína y heroína. LNFM también trafica drogas a Estados Unidos y blanquea los beneficios de la droga mediante diversos métodos, incluyendo MSB afiliados a cárteles y negocios legítimos desprevenidos.

A fecha de 2025, el CDG se dividió en varias facciones, incluyendo Los Metros y Los Escorpiones, que luchan entre sí por el control de rutas de tráfico, territorio y autoridad organizativa. CDG genera ingresos significativos de sus actividades de tráfico de migrantes. Mientras que los beneficios del tráfico de drogas y personas se introducen en México a gran escala, el CDG también blanquea dinero a través de empresas de intercambio de dinero.

La TdA facilita el tráfico de migrantes venezolanos hacia Estados Unidos y luego extorsiona a los migrantes, obligándolos a la prostitución u otras actividades delictivas para saldar "deudas". Los miembros de la TdA son sospechosos y/o acusados de diversos delitos, incluyendo tráfico de drogas, asesinato, secuestro, extorsión, tráfico de migrantes, trata de personas, prostitución, crimen minorista organizado, robos y fraude documental.
[115]

111 *Véase, por ejemplo,* el Departamento de Justicia, "El Departamento de Justicia destaca las incautaciones de drogas de la DEA en la primera mitad de 2025, operaciones exitosas en las últimas semanas," (15 de julio de 2025) https://www.justice.gov/opa/pr/justice-department-highlights-dea-drug-seizures-first-half-2025-successful- operaciones terminadas; DOJ, "Acusación federal alega alianza entre el cártel de Sinaloa y blanqueadores de dinero vinculados a la banca clandestina china," (junio de 2024) https://www.justice.gov/archives/opa/pr/federal-indictment-alleges-alliance-between-sinaloa- vinculados a cártel y lavadores de dinero; DOJ, "Dos ejecutivos de empresas químicas chinas condenados y múltiples sitios web y cuentas de criptomonedas incautados en relación con la importación de precursores de fentanilo y esquemas de blanqueo de capitales," (3 de febrero de 2025) https://www.justice.gov/usao-sdny/pr/two-chinese-chemical-company-executives-convicted-and-multiple-websites-and-0. 112 DEA, 2025 NDTA, p.64, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

113 Las órdenes de FinCEN se emitieron conforme a 21 U.S.C. 2313a. Para más información, véase: https://www.fincen.gov/news/news-releases/ tesorería-emite-órdenes-sin precedentes bajo una poderosa nueva autoridad.

114 Todas las descripciones encontradas en el NDTA de 2025 de la DEA, pp. 11-19,

https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAsse ssment.pdf.

115 Véase DOJ, "El Departamento de Justicia destaca la represión nacional contra el Tren de Aragua," (18 de diciembre de 2025) https://www.justice.gov/ opa/pr/departamento de justicia-destaca-represión nacional-tren-de-aragua.

MS-13 es una banda criminal internacional extremadamente violenta, con un estimado de miles de miembros ubicados en casi los 50 estados de EE. UU. La brutalidad de sus crímenes violentos ha atraído una atención significativa por parte de las fuerzas del orden y los medios. Los miembros de MS-13 también participan en el tráfico minorista de drogas, robos, prostitución, extorsión, delitos relacionados con armas de fuego y otros delitos.

También hay muchas otras TCOs, negocios (incluidos MSBs sin licencia y con licencia) y particulares que adquieren precursores químicos o drogas refinadas de origen extranjero, que introducen las drogas de contrabando en Estados Unidos para su venta por todo el país y blanquean los beneficios ilícitos tras la distribución y venta de las sustancias. Por ejemplo, en septiembre de 2025, OFAC sancionó a una empresa química con sede en China y a dos personas por su papel en la fabricación y envío de opioides sintéticos y agentes de corte directamente a Estados Unidos. [116]

Tendencias adicionales

Mercados de la Darknet

Los mercados de la darknet permiten a los usuarios comprar y vender drogas de forma anónima en todo el mundo utilizando activos digitales. La naturaleza dispersa y opaca de esta red de distribución de la dark web dificulta su detección e interdicción. Durante el periodo de evaluación, hubo un número creciente de casos relevantes en los que las personas aprovecharon la facilidad para hacer negocios y la falta de supervisión regulatoria y aplicación de estas plataformas en línea. Por ejemplo, en abril de 2025 un hombre fue condenado a 15 años de prisión por su participación en una conspiración de drogas que distribuía una amplia variedad de drogas. Según documentos judiciales, el hombre fabricó y obtuvo pastillas falsificadas de Oxycodona, Adderall y Xanax para su compra. Publicó anuncios de las sustancias controladas en Tor2Door y otros cuatro marketplaces, y aceptó pagos en activos digitales. Durante la conspiración, el hombre envió pastillas de oxicodona falsificadas al Distrito de Columbia al menos seis veces. Estas pastillas contenían fentanilo, una sustancia controlada de la Lista II, y metonazeno, una sustancia controlada de la Lista I. El hombre y un cómplice también enviaron pastillas falsas de Xanax y Adderall al Distrito en varias ocasiones. [117]

Estos mercados también permiten transacciones transfronterizas de drogas. En marzo de 2025, la OFAC designó a Behrouz Parsarad, con sede en Irán, como único administrador de Nemesis, un mercado en línea de la darknet que fue objeto de una operación internacional de aplicación de la ley y que fue retirado en 2024. Antes de su retirada por parte de las fuerzas del orden, narcotraficantes y ciberdelincuentes comerciaban abiertamente con drogas controladas y servicios en Nemesis, que estaba diseñado con funciones integradas de blanqueo de capitales. Nemesis contaba con más de 30.000 usuarios activos y 1.000 vendedores, y facilitó la venta de casi 30 millones de dólares en medicamentos en todo el mundo entre 2021 y 2024incluyendo a Estados Unidos. Además de proporcionar a los delincuentes una plataforma para realizar transacciones, Parsarad blanqueó activos digitales para narcotraficantes y ciberdelincuentes activos en Nemesis. [118]

Operaciones de cultivo de marihuana

Aunque la marihuana sigue estrictamente controlada bajo la ley federal, es la droga más comúnmente mal utilizada en Estados Unidos. Según las fuerzas del orden, las operaciones de cultivo de marihuana suelen llevarse a cabo en estados donde supuestamente el cultivo es legal según la ley estatal para fines medicinales o recreativos, como California, Oklahoma y Maine. A pesar de las medidas de legalización, el mercado ilícito de la marihuana se ha expandido significativamente en las últimas dos décadas debido al papel cada vez más dominante de los TCOs chinos y otros asiáticos.[119] Estos TCOs, así como los cárteles de droga con sede en México, están obteniendo beneficios como resultado. [120]

116 Tesorería, "Hacienda sanciona a una empresa química con sede en China para combatir el tráfico de opioides sintéticos," (3 de septiembre de 2025) https:// home.treasury.gov/news/press-releases/sb0235.

117 DOJ, "Narcotraficante de la Darknet del oeste de Pensilvania condenado en D.C. por vender grandes cantidades de fentanilo en línea," (23 de abril de 2025) https://www.justice.gov/usao-wdpa/pr/darknet-drug-trafficker-western-pennsylvania-sentenced-dc-selling-mass-quantities. 118 Tesorería, "El Tesoro sanciona a la cabeza del mercado online de darknet vinculado a la venta de fentanilo," (4 de marzo de 2025) https://home.treasury.gov/ noticias/comunicados de prensa/sb0040.

119 Véase Área de Tráfico de Drogas de Alta Intensidad del Medio Oeste (HIDTA), "Legalización de la marihuana en el Medio Oeste HIDTA: Los impactos actualizados," Volumen 5 (julio de 2025), pp. 13-20, https://img1.wsimg.com/blobby/go/893a8d74-0308-463e-b5f2-5dc56ff67d71/downloads/b326f5df-cd99-4327-b0fb-f9734237bcea/Midwest%20HIDTA%202025%20Marijuana%20Impact%20Report.pdf?ver=1766163078317. 120 DEA, NDTA 2025, pp. 48-54, https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf.

Por ejemplo, en julio de 2025, siete ciudadanos chinos fueron acusados en relación con una conspiración multimillonaria para cultivar y distribuir marihuana en la región noreste de Estados Unidos. Según los documentos de acusación, los acusados supuestamente poseían, operaban o se asociaban con una red de cultivos interconectados en Massachusetts y Maine para cultivar y distribuir cantidades de marihuana del tamaño de un kilogramo al por mayor. Datos extraídos del teléfono móvil de un acusado supuestamente revelaron que ayudó a introducir clandestinamente ciudadanos chinos en Estados Unidos, poniéndolos a trabajar en una de las casas de cultivo que controlaba, mientras mantenía la posesión de sus pasaportes hasta que le devolvieron el coste asociado a su contrabando en el país. Además, se alega que los beneficios de la venta de marihuana, que sumaron millones de dólares, se utilizaron para comprar casas de lujo, automóviles, joyas y otros artículos en Massachusetts, incluyendo para expandir el negocio mediante la compra de bienes inmuebles. La empresa criminal supuestamente realizaba transacciones al por mayor en efectivo con operadores ubicados en Nueva York.[121] Según las fuerzas del orden, los grupos chinos también repatrian los ingresos de la marihuana intercambiando dinero en efectivo por transferencias intra-China o transferencias de activos digitales. Los ingresos de la marihuana que se blanquean y no solo se repatrian a China pasan por el mismo proceso, sino que utilizan el valor transferido a China para comprar bienes que se exportan desde China para su venta. Las CMLN están asociadas con el blanqueo de ingresos para el tráfico de marihuana. [122]

III. Ciberdelincuencia

El cibercrimen abarca una variedad de amenazas diferentes que suponen graves riesgos para los ciudadanos estadounidenses, las instituciones, las infraestructuras críticas y el sistema financiero estadounidense. Los criminales y los estados-nación apuntan a Estados Unidos para comprometer sus redes tecnológicas, robar propiedad financiera e intelectual, y generar beneficios ilícitos de estas actividades, ya sea directamente mediante fondos extorsionados o rescatados, o robando información personal identificable (PII) para usarla en otros fraudes y esquemas.

Esta sección se centra en los principales tipos de ciberdelitos perpetrados por criminales y adversarios extranjeros para generar y blanquear ingresos ilícitos. Estas actividades varían en tamaño y complejidad desde el simple robo de identidad hasta la generación avanzada de código de malware. Los autores de estas actividades varían de forma similar desde ladrones solitarios hasta sofisticadas organizaciones criminales que ofrecen cibercrimen como servicio. De estas actividades maliciosas, el fraude y las estafas relacionadas con la identidad representan la mayor amenaza para los ciudadanos estadounidenses y las instituciones financieras estadounidenses. Sin embargo, el cibercrimen suele consistir en amenazas complejas y superpuestas a diversas partes críticas del sistema financiero estadounidense.

Robo de identidad

El robo de identidad es una grave amenaza para el público estadounidense y un riesgo serio para las instituciones financieras estadounidenses, que genera grandes volúmenes de ingresos ilícitos para actividades de blanqueo de capitales. En 2024, la Comisión Federal de Comercio informó de más de un millón de incidentes de robo de identidad, lo que representa el 18 por ciento de todas las quejas de los consumidores, basándose en la denuncia directa de víctimas.[123] En enero de 2024, FinCEN publicó su análisis de Actividad Sospechosa Relacionada con la Identidad, que examinaba actividades relacionadas con la explotación de procesos de identidad durante la creación de cuentas, el acceso a cuentas y el procesamiento de transacciones. El análisis de FinCEN encontró que aproximadamente 1,6 millones de informes, o el 42 por ciento de los informes presentados por instituciones informantes, estaban relacionados con la identidad, que representan 212.000 millones de dólares en actividad sospechosa. [124]

El robo de identidad permite a los delincuentes aprovechar diversas formas de adquirir y blanquear los ingresos criminales. Las identidades obtenidas ilegalmente permiten a los delincuentes maximizar los montantes de los préstamos u obtener fondos mediante la apertura o adquisición ilegal

121 DOJ, "Siete ciudadanos chinos acusados de presuntas implicaciones en blanqueo de dinero, tráfico de extranjeros y tráfico de drogas multimillonarios," (8 de julio de 2025) https://www.justice.gov/usao-ma/pr/seven-chinese-nationals-charged-alleged-roles-multi_blanqueo_de_dinero_millonario.

122 FinCEN, "Aviso de FinCEN sobre el uso de redes chinas de blanqueo de dinero por organizaciones criminales transnacionales con sede en México para blanquear ingresos ilícitos," (28 de agosto de 2025), p. 3,

https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf. 123 FTC, "Consumer Sentinel Network Data Book 2024," (marzo de 2025) https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data- book-2024.pdf.

124 FinCEN, "Actividad sospechosa relacionada con la identidad: amenazas y tendencias en 2021," (enero de 2024), p. 1, https://www.fincen.gov/sites/default/ archivos/compartidos/FTA_Identity_Final508.pdf.

cuentas bancarias, MSB o de crédito; desviar fondos de desempleo u otras prestaciones gubernamentales; o presentar declaraciones de impuestos falsas. [125]

En abril de 2024, FinCEN publicó un Aviso sobre el aumento del uso de tarjetas de pasaporte estadounidenses falsificadas por parte de particulares y redes de fraude para acceder a cuentas de víctimas en instituciones financieras de todo el país.[126] Los ladrones de identidad también están aprovechando nuevas tecnologías, como herramientas de inteligencia artificial, para explotar grandes cantidades de información y documentos públicos en la búsqueda de la operación altamente técnica y sofisticada del robo de identidad.

Una vez que se han abierto cuentas fraudulentas y se han adquirido fondos, los delincuentes pueden depositar los beneficios de sus delitos en cuentas bancarias o de servicios monetarios recién abiertas, como plataformas de pago peer-to-peer (P2P), o financiar otros instrumentos de pago, como tarjetas prepago. Luego pueden superponer y blanquear estos fondos mediante transferencias rápidas de cámara de compensación automatizada (ACH) o depósitos en cuentas de activos digitales, redes de mulas de dinero o la compra de artículos y bienes de alto valor.

El Análisis de Tendencias Financieras de FinCEN describe dos arquetipos de técnicas de blanqueo de capitales de terceros relacionadas con el robo de identidad: 1) mulas de dinero: individuos que a menudo son reclutados en línea y reciben y reenvían fondos robados mediante transferencias ACH, pagos por transferencia, cuentas de activos digitales y depósitos en efectivo, en nombre de redes de fraude; y 2) compradores y prestatarios ficticios: personas que usan sus nombres, números de la seguridad social o archivos de crédito para abrir una cuenta bancaria, de tarjeta de crédito, préstamo de automóvil, hipoteca o servicio monetario para otra persona. En el primer caso, las mulas de dinero ayudan a ocultar la pista de auditoría y el flujo de fondos derivados de delitos de robo de identidad, al situarse entre el delito subyacente y el destino final de estos fondos. En el segundo caso, las credenciales legítimas permiten a los delincuentes saltarse los procesos de verificación de identidad de clientes de un banco y colocar ingresos ilícitos en cuentas y canales aparentemente normales de consumidores o empresas. [127]

En un caso representativo, seis personas, incluidos cuatro ciudadanos chinos que entraron en Estados Unidos bajo falsas pretensiones, fueron condenadas a prisión federal por su participación en un complejo esquema de robo de identidad y fraude financiero que defraudó a varios minoristas nacionales por valor de al menos 1,2 millones de dólares.[128] Como parte del esquema, estos seis acusados robaron las identidades de las víctimas — incluyendo sus números de la Seguridad Social, fechas de nacimiento y direcciones domiciliaria— y usaron esa información para fabricar permisos de conducir falsos que se usaron para acceder a créditos a nombre de las víctimas en grandes minoristas nacionales.

Ransomware

El ransomware se refiere a un tipo de software malicioso (malware) diseñado para bloquear el acceso a un sistema informático o cifrar datos hasta que se pague un rescate.[129] Normalmente es utilizado por ciberdelincuentes para extorsionar dinero a particulares, empresas o entidades gubernamentales. El ransomware suele transmitirse mediante correos electrónicos de phishing o explotando vulnerabilidades del sistema. Una vez activado, el programa de ransomware cifra archivos o bloquea el sistema, haciendo que los datos sean inaccesibles para el usuario, y se muestra una nota de rescate que exige el pago — a menudo en activos digitales descentralizados o con anonimato mejorado—a cambio de la clave de descifrado. Los actores de ransomware también pueden usar la "doble extorsión", es decir, la amenaza de filtrar datos sensibles al público o de eliminarlos o manipularlos si las víctimas se niegan a pagar rescates.

Los actores y grupos criminales de ransomware continúan perpetrando crímenes contra infraestructuras críticas y en todos los sectores de la economía estadounidense, lo que resulta en el robo de miles de millones de dólares a personas y empresas estadounidenses cada vez

125 *Ver, por ejemplo,* IRS, "Informe Anual 2024 sobre el Fraude por Robo de Identidad y Devolución de Impuestos ISAC," (noviembre de 2024) https://www.irs.gov/pub/ redacción/2024-isac-annual-report.pdf.

126 Véase en general, FinCEN, "Aviso sobre el uso de tarjetas de pasaporte estadounidenses falsificadas para perpetrar robo de identidad y fraude en instituciones financieras" (15 de abril de 2024) https://www.fincen.gov/system/files/shared/FinCEN_Notice_Counterfeit_US_Passport_FINAL508.pdf.

127 FinCEN, "Actividad sospechosa relacionada con la identidad: amenazas y tendencias en 2021," (enero de 2024) https://www.fincen.gov/sites/default/files/ compartido/FTA_Identity_Final508.pdf.

128 DOJ, "Cuatro ciudadanos chinos condenados a prisión federal en esquema dirigido a cientos de consumidores estadounidenses y múltiples minoristas estadounidenses", (17 de marzo de 2025) https://www.justice.gov/usao-cdca/pr/four-chinese-nationals-sentenced-federal-prison-scheme-targeting-hundreds- consumidores estadounidenses..

129 DHS Agencia de Ciberseguridad e Seguridad de Infraestructuras (CISA), "Detener ransomware," (consultado en agosto de 2025) https://www.cisa.gov/ detener ransomware.

año. Según FinCEN, entre 2022 y 2024, las instituciones financieras presentaron cerca de 7.400 informes relacionados con casi 4.200 incidentes de ransomware, que sumaron un total de casi 2.100 millones de dólares en pagos de ransomware.[130] El número total de ataques de ransomware en todo el mundo, por año, ha ido aumentando cada año; la Oficina del Director de Inteligencia Nacional registró 4.591 ataques en 2023 y 5.289 ataques en 2024. Los ataques en Estados Unidos representaron aproximadamente la mitad de ese total global, en parte debido a la amplia gama de objetivos rentables. [131]

Los actores criminales de ransomware continúan innovando y ampliando su alcance, incluso utilizando modelos de "ransomware como servicio". El ransomware como servicio (RaaS) es un modelo basado en suscripción en el que los administradores crean una interfaz fácil de usar y luego ofrecen su software a afiliados para desplegar ataques. Los afiliados de estos grupos identifican objetivos y despliegan software malicioso, para luego compartir un porcentaje de cada pago de rescate. A menudo utilizan equipos especializados para varios pasos del proceso de ransomware, incluido el proceso de blanqueo.

Uno de los actores más prolíficos de RaaS es el grupo ruso LockBit, que ha atacado instituciones financieras estadounidenses e infraestructuras críticas, incluidos hospitales y escuelas. LockBit funciona mediante un modelo de afiliados, emplea doble extorsión y ha sido desplegada contra más de 2.500 víctimas, que han pagado más de 500 millones de dólares en pagos de rescate.[132] En febrero de 2024, OFAC sancionó a afiliados del LockBit Ransomware Group, en relación con el ataque de LockBit a una institución financiera que afectó la liquidación de activos por valor de más de 9.000 millones de dólares respaldados por valores del Tesoro de EE. UU.[133] El DOJ procesó con éxito casos contra dos afiliados criminales de LockBit, que desplegaron LockBit contra 12 víctimas. El DOJ también logró obtener con éxito la extradición de un desarrollador de LockBit desde Israel al Distrito de Nueva Jersey, donde fue acusado mediante una denuncia, y acusó al desarrollador principal de LockBit, así como a otras afiliadas." [134]

Para blanquear los beneficios de sus delitos, los delincuentes de ransomware suelen recurrir a activos digitales y proveedores de servicios relacionados para ocultar y enviar pagos que enriquecen a ellos y a sus afiliados.[135] En un caso, un ciudadano iraní y sus cómplices —todos ellos en el extranjero—causaron decenas de millones de dólares en pérdidas y interrumpieron servicios públicos esenciales al desplegar el ransomware Robbinhood contra ciudades estadounidenses, organizaciones sanitarias y empresas. Intentaron blanquear los pagos del rescate mediante servicios de mezcla de activos digitales y moviendo activos entre diferentes tipos de activos digitales, una práctica conocida como chain-hopping. También ocultaban sus identidades y actividades mediante varios métodos técnicos, incluyendo el uso de redes privadas virtuales y servidores que operaban. [136]

130 FinCEN, "Tendencias de ransomware en los datos de la Ley de Secreto Bancario entre 2022 y 2024," (diciembre de 2025), p. 1, https://www.fincen.gov/ system/files/2025-12/FTA-Ransomware.pdf.

131 Oficina del Director de Inteligencia Nacional (ODNI), "Ransomware mundial, 2024: Aumento de la tasa de ataques atenuada por interrupciones en las fuerzas del orden," (febrero de 2025) https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf. 132 DOJ, "Lockbit", (actualizado el 22 de julio de 2024) https://www.justice.gov/usao-nj/lockbit. Los actores de ransomware suelen atacar a entidades que consideran más propensas a pagar un rescate, centrando el ataque en los datos más sensibles de la víctima. Los atacantes también pueden emplear múltiples formas de extorsión. Los actores de ransomware pueden presionar a las víctimas para que paguen un rescate, por ejemplo, robando datos confidenciales y amenazando con publicarlos.

133 OFAC, "Estados Unidos sanciona a afiliados del grupo ruso LockBit Ransomware Group," (20 de febrero de 2024) https://home.treasury.gov/ noticias/comunicados de prensa/jy2114.

134 DOJ, "Dos ciudadanos extranjeros se declaran culpables de participar en el grupo de ransomware LockBit," (18 de julio de 2024) https://www.justice.gov/ archives/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group; DOJ, "Doble nacionalidad rusa e israelí extraditada a Estados Unidos por su papel en la conspiración del ransomware LockBit," (13 de marzo de 2025) https://www.justice.gov/usao- nj/pr/nacionalidad dual rusa e israelí extraditada-unidos-estados-su-rol-lockbit-ransomware; DOJ, "EE.UU. y Reino Unido interrumpen la variante de ransomware LockBit," (20 de febrero de 2024) https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant. 135 GAFI, "Contrarrestando la financiación de ransomware," (marzo de 2023) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf

136 DOJ, "Hombre iraní se declaró culpable de su papel en el ransomware Robbinhood," (27 de mayo de 2025) https://www.justice.gov/opa/pr/iranian-man se declaró culpable de robo-robar-ransomware.

Enfoque especial: Sextorsión financiera

La extorsión sexual motivada económicamente (sextorsión financiera) ocurre cuando individuos, cada vez más niños y adolescentes, son coaccionados para enviar imágenes explícitas en línea y posteriormente son extorsionados por dinero.[137] El FBI y el Departamento de Seguridad Nacional (DHS) han identificado un aumento exponencial en los delitos de sextorsión financiera dirigidos a menores desde 2022, especialmente a niños entre 14 y 17 años. Entre octubre de 2021 y marzo de 2023, recibieron más de 13.000 informes de sextorsión financiera en línea de menores. La sextorsión involucró al menos a 12.600 víctimas y provocó al menos 20 suicidios.[138] En septiembre de 2025, FinCEN publicó un Aviso sobre sextorsión financiera con indicadores de alerta para ayudar a las instituciones financieras a identificar e informar de actividades sospechosas. [139]

Los perpetradores de sextorsión financiera son organizados y deliberados, a menudo robando o tomando imágenes, como fotos de perfil de otra persona de edad similar a la de la posible víctima y de género diferente, para comunicarse con la víctima mediante cuentas falsas. También pueden enviar imágenes explícitas a la víctima para ganarse su confianza y usar la amenaza de divulgar el contenido explícito de la víctima para apoderarse forzosamente de la cuenta de la víctima y así seguir extorsionando sexualmente a sus amigos en línea. Según el FBI, la sextorsión financiera suele ser un delito transnacional, con perpetradores que operan en África Occidental y el Sudeste Asiático atacando a víctimas estadounidenses.[140] Una vez que el agresor obtiene un vídeo o foto explícito, amenaza con publicar el material comprometedor a menos que la víctima envíe dinero o tarjetas regalo. Con frecuencia, los perpetradores exigen pagos con activos digitales y plataformas de pago P2P. Estos pagos pueden ser recibidos por una mula de dinero desprevenida, que también puede ser víctima de cierta actividad delictiva y remitidos a través de MSB. [141]

En un caso, cinco acusados afincados en Estados Unidos se declararon culpables de conspirar para blanquear los beneficios de los sextorsionistas nigerianos. Según la acusación, los conspiradores utilizaron sistemas de pago en línea para recaudar los ingresos de la sextorsión y enviarlos a un individuo nigeriano al que llamaban "El Enchufe". Los sextorsionistas hicieron que niños y jóvenes crearan imágenes desnudas.Después de que los sextorsionistas recibieran esas imágenes, supuestamente hicieron que las víctimas enviaran fondos a los blanqueadores de dinero con sede en EE. UU. a través de sistemas de pago en línea como Apple Pay, Cash App y Zelle. Los blanqueadores de dinero se quedaban con alrededor del 20 por ciento del dinero, convertían el resto en Bitcoin y enviaban el Bitcoin a The Plug en Nigeria, que se quedaba con una parte y luego enviaba el resto a los sextorsionistas.[142] En otro caso, dos acusados y otros intentaron extorsionar aproximadamente 6 millones de dólares a miles de posibles víctimas y lograron extorsionar aproximadamente 1,7 millones de dólares a esas víctimas, utilizando únicamente cuentas de Cash App y Apple Pay. [143]

---

137 FBI, "Sextorsión," https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion; FBI, "FBI y Socios emiten una alerta nacional de seguridad pública sobre esquemas de sextorsión financiera," (19 de diciembre de 2022) https://www.fbi.gov/news/press- publica/FBI-y-partners-emiten-alerta-nacional-de seguridad pública sobre esquemas de sextorsión financiera; ICE, "Sextorsión: Es más común de lo que crees" (actualizado el 18 de septiembre de 2025); https://www.ice.gov/features/sextortion; FBI, "El FBI emite una advertencia sobre el aumento de esquemas de sextorsión financiera dirigidos a menores," (27 de octubre de 2023) https://www.fbi.gov/contact-us/field-offices/losangeles/news/fbi advierte sobre el aumento de esquemas de sextorsión financiera que apuntan a menores.

138 FBI, "Sextorsión: Una amenaza creciente que apunta a menores" (23 de enero de 2024), https://www.fbi.gov/contact-us/field-offices/nashville/news/ la sextassión de una amenaza creciente que apunta a menores.

139 FinCEN, "Aviso sobre la sextorsión motivada económicamente" (8 de septiembre de 2025) https://www.fincen.gov/system/files/2025-09/FinCEN-Notice- FMS-508C.pdf 140 FBI, "Sextorsión: una amenaza creciente dirigida a menores" (23 de enero de 2024), https://www.fbi.gov/contact-us/field-offices/nashville/news/ la sextasión, una amenaza creciente que apunta a menores.

141 Ibid.

142 DOJ, "Todos los blanqueadores de dinero acusados vinculados al esquema de sextorsión nigeriano se declaran culpables," (3 de abril de 2025) https://www.justice.gov/usao- wdmi/pr/2025_0403_Nigerian_Sextortion_Scheme_Plea.

143 DOJ, "Mujer de Delaware arrestada por esquema internacional de sextorsión y blanqueo de capitales" (12 de abril de 2024), https://www.justice.gov/ archivos/opa/pr/delaware-woman-arrested-international-sextortion-and-money-laundering-cash-branding.

IV. Blanqueo profesional de capitales

Las redes profesionales de blanqueo de capitales (PML) permiten a otros actores mariscos blanqueando ingresos ilícitos a cambio de una tarifa. Los corredores que gestionan redes PML pueden tener una historia de cobertura o profesión, pero su principal actividad generadora de ingresos es coordinar el proceso de blanqueo de capitales. Las redes PML generalmente no están involucradas en los delitos básicos que generan ingresos ilícitos, pero a menudo cometen otros delitos para facilitar el blanqueo de capitales, como el robo de identidad, el fraude con dispositivos de acceso y la evasión fiscal. La PML hace que la delincuencia sea más lucrativa porque proporciona experiencia y economías de escala, así como la repatriación de fondos para esquemas transnacionales. También hace que las redes criminales sean más complejas y difíciles de desentrañar.

Los intermediarios de PML negocian contratos con organizaciones criminales que cubren cómo se recogerán, blanquearán y entregarán los beneficios ilícitos. Los corredores pueden cobrar una amplia gama de comisiones, dependiendo de la dificultad de cada uno de esos pasos, así como de lo difícil que pueda ser para el corredor deshacerse del dinero "sucio". Los métodos de blanqueo de capitales utilizados dependen de la forma en que se recaudan los ingresos ilícitos, la experiencia o la historia de cobertura del corredor, y el método de entrega preferido por la organización criminal.

Las redes PML blanquearán los beneficios ilícitos de cualquier tipo de delito, pero la mayoría de las veces trabajan para TCOs dedicados al tráfico de drogas, trata de personas, tráfico de personas o fraude. Las redes PML suelen participar en esquemas de blanqueo más sofisticados. En abril de 2025, tres hombres fueron acusados de conspirar presuntamente para blanquear millones de dólares en ingresos procedentes del tráfico de drogas. Según documentos judiciales, los hombres supuestamente trabajaban para una organización de blanqueo de capitales que blanqueaba al menos 30 millones de dólares en ingresos relacionados con la distribución de drogas ilegales, incluyendo cocaína y fentanilo, que se importaban ilegalmente a Estados Unidos, normalmente a través de México. Los hombres y sus cómplices supuestamente viajaron por todo Estados Unidos para recaudar los beneficios de la droga. Se comunicaron con co-conspiradores en China para organizar el blanqueo de estos productos mediante transacciones destinadas a ocultar el origen ilegal de los mismos, incluyendo el disfrazamiento del origen mediante el envío de bienes electrónicos a China y Oriente Medio. [144]

Mulas de Dinero

Las mulas de dinero son personas que recogen o reciben ingresos ilícitos y luego transportan, transfieren o convierten los fondos en nombre de otra persona u organización. Los autores de todo tipo de delitos generadores de ingresos pueden usar mulas de dinero, aunque, como otras formas de PML, suelen estar implicados en fraude, tráfico de drogas, trata de personas y tráfico de personas. Los delincuentes utilizan mulas de dinero para crear distancia entre ellos y la actividad delictiva, dificultando que las fuerzas del orden sigan el dinero de vuelta a quienes se benefician del delito. También son frecuentemente utilizados por los TCOs para repatriar ingresos ilícitos de Estados Unidos a las jurisdicciones extranjeras donde se encuentran los perpetradores.

Los delincuentes reclutan mulas de dinero a través de redes sociales, foros de empleo, aplicaciones de mensajería y el boca a boca. Las mulas de dinero pueden ser inconscientes, astutos o cómplices, y la sofisticación de sus métodos de blanqueo de dinero generalmente depende de su nivel de conocimiento. [145]

Las mulas de dinero sin saberlo desconocen que forman parte de una red criminal y pueden creer que están ayudando a una pareja, asistiendo a una persona sin bancarización o realizando las tareas habituales de un nuevo trabajo. Es probable que usen su propia identidad y cuentas bancarias, y pueden quedarse con una parte de los ingresos porque creen que están realizando un trabajo o servicio legítimo.

144 DOJ, "Tres miembros de una organización internacional de blanqueo de dinero acusados de blanquear millones de dólares en ingresos por drogas," (24 de abril de 2025)
https://www.justice.gov/opa/pr/three-members-international-money-laundering-organization-charged-blanqueo_de_millones.

145 FBI, "Money Mules" (consultado el 15 de julio de 2025)
https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ mulas de dinero.

Las mulas del dinero conscientes ignoran señales de alerta evidentes y pueden haber sido alertadas por instituciones financieras o fuerzas del orden de que sus actividades son ilegales. Puede que no hubieran sido conscientes de empezar, pero seguir trabajando como mulas de dinero tras darse cuenta de la ilegalidad debido a la perspectiva de obtener beneficios económicos.

Las mulas cómplices entienden que forman parte de una red de blanqueo de capitales. Pueden anunciar sus servicios a múltiples grupos criminales, negociar sus propias tarifas o reclutar y entrenar a otras mulas de dinero. Sus métodos de blanqueo de capitales son más complejos, a menudo involucrando identidades falsas o robadas y utilizando cuentas bancarias a nombre de empresas pantalla.

Muchas mulas de dinero forman parte de comunidades de la diáspora en Estados Unidos con conexiones con los países extranjeros donde se basan las TCOs o redes PML. Pueden ser ciudadanos estadounidenses, inmigrantes autorizados o inmigrantes ilegales. Según las fuerzas del orden, los migrantes recientes con circunstancias financieras precarias, como aquellos con visados de estudiante que no permiten autorización de trabajo, son especialmente vulnerables a ser reclutados como mulas de dinero. [146]

La actividad de mulas de dinero varía según cómo el delito subyacente genere ingresos ilícitos. Para el tráfico de drogas y la trata de personas, las mulas de dinero se utilizan frecuentemente para recaudar grandes cantidades de dinero en efectivo. Tras la cobranza, pueden depositar el efectivo en cuentas embudo, transportar el efectivo a puntos de consolidación para que los co-conspiradores lo blanqueen o contrabandear el efectivo fuera de Estados Unidos, la mayoría de las veces a México. En un caso, nueve mulas de dinero fueron acusadas de conspirar presuntamente para blanquear dinero al granel en activos digitales en nombre de cárteles de la droga en México y Colombia. Según la acusación de sustitución, los acusados y los co-conspiradores trabajaron juntos para conseguir grandes cantidades de dinero provenientes de la venta de drogas en Estados Unidos y cambiar ese dinero por activos digitales mediante blanqueadores de activos digitales del mercado negro. Los activos digitales luego se convertían de nuevo en efectivo en México o Colombia y se entregaban a los líderes de los cárteles. [147]

Para fraude y ciberdelitos, los money mules pueden recibir transferencias bancarias de víctimas en cuentas bancarias que controlan; depositar efectivo, cheques o giros postales que reciben por correo de víctimas en las mismas cuentas; o recoger dinero en efectivo o lingotes de oro de las víctimas en persona. Desde allí, pueden transmitir los beneficios a los responsables mediante transferencia bancaria o activos digitales y enviar cualquier dinero en efectivo y lingotes de oro a los intermediarios PML que coordinan la operación. En un caso, un hombre de Maryland fue condenado a 42 meses de prisión por servir como transmisor de dinero sin licencia en relación con diversas relaciones amorosas, compromisos de correos electrónicos comerciales y esquemas de inversión. Su tarifa por recibir y transmitir fondos de las víctimas solía ser del 20 por ciento o más. Tras recibir fondos de las víctimas en cuentas bancarias personales y empresariales que controlaba, transfería esos fondos a los participantes del esquema en el extranjero. [148]

Redes Chinas de Blanqueo de Capitales (CMLNs)

En la última década, las redes chinas de blanqueo de capitales (CMLN) se han convertido en las PML dominantes para los DTOs y otros TCOs en todo el mundo. El auge de las CMLN fue impulsado originalmente, en parte, por la creciente demanda de moneda extranjera necesaria para eludir los controles monetarios chinos por parte de los ciudadanos chinos.[149] Esta demanda global sostenida permite a los corredores de CMLN cobrar altas comisiones a los ciudadanos chinos por comprar moneda, mientras que cobran a los delincuentes que suministran el dinero ilícito tarifas más bajas que otros blanqueadores de dinero. Según FinCEN, durante el periodo de cinco años comprendido entre el 1 de enero de 2020 y el 31 de diciembre de 2024, las instituciones financieras presentaron más de
137.000 denuncias relacionadas con 312.000 millones de dólares en actividades sospechosas asociadas a sospechas de actividad CMLN. [150]

146 *Véase también,* FinCEN, "Asesor de FinCEN sobre el uso de redes chinas de blanqueo de dinero por organizaciones criminales transnacionales con sede en México para blanquear ingresos ilícitos," (28 de agosto de 2025), pp. 2-3,

https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

147 DOJ, "Quince acusados acusados en una operación que busca convertir ingresos en efectivo estadounidenses a granel procedentes de ventas de drogas en criptomonedas para cárteles mexicanos," (20 de noviembre de 2024) https://www.justice.gov/usao-sdfl/pr/fifteen-defendants-charged-operation-targeting- conversión-granel-us-efectivo-dinero-droga.

148 DOJ, "Hombre del condado de Baltimore sentenciado a prisión federal por su papel en esquemas de fraude contra ancianos," (4 de marzo de 2025) https://www.justice.gov/ esquemas de fraude de usao-md/pr/baltimore-county-man-sented-federal-prison-role-elder-fraud.

149 FinCEN, "Asesoría FinCEN sobre el uso de redes chinas de blanqueo de dinero por organizaciones criminales transnacionales con sede en México para blanquear ingresos ilícitos," (28 de agosto de 2025), p. 5, https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf. 150 FinCEN, "Redes chinas de blanqueo de capitales: 2020 - 2024 Patrón de amenazas e información sobre tendencias," (agosto de 2025), p. 1, https://www.fincen.gov/sites/default/files/shared/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf.

Para el tráfico de drogas y otros delitos generadores de dinero, los corredores de CMLN utilizan redes de mulas de dinero en todo Estados Unidos para recaudar los ingresos ilícitos en dólares estadounidenses (USD) y ofrecerlos a la venta a compradores chinos en WeChat u otras aplicaciones de mensajería. Los compradores chinos generalmente compran el USD transfiriendo una cantidad equivalente de renminbi, más comisiones, a la cuenta bancaria del corredor CMLN en China. El corredor CMLN luego proporciona los USD al comprador en Estados Unidos mediante efectivo, cheques o transferencias bancarias desde cuentas bancarias estadounidenses financiadas con depósitos en efectivo realizados por mulas de dinero.[151] Estas cuentas bancarias estadounidenses controladas por CMLN pueden abrirse utilizando pasaportes chinos fraudulentos y estar a nombre de empresas pantalla.[152] Según las fuerzas del orden, las CMLN también están intercambiando cada vez más USD por activos digitales, especialmente stablecoins, en parte para evitar grandes transferencias bancarias intrachinas que puedan levantar sospechas de fuga de capitales.

En junio de 2024, Estados Unidos desclasificó una acusación de sustitución que acusa a asociados con base en Los Ángeles del cártel de drogas de Sinaloa en México de conspirar con grupos de blanqueo de dinero para blanquear los ingresos del tráfico de drogas. Según la acusación, los miembros de la CMLN supuestamente blanquearon los ingresos ilícitos de las drogas entregando directamente USD a sus clientes de la casa de cambio o comprando bienes inmuebles o personales, incluidos bienes de lujo y coches para ser enviados a China. También supuestamente utilizaron diversos métodos tradicionales para depositar los fondos en el sistema bancario tradicional, como comprar cheques de caja o estructurar pequeñas cantidades a la vez en cuentas bancarias embudo abiertas para este propósito, para evitar que los bancos reportaran grandes depósitos en efectivo al gobierno de EE. UU. [153]

Según las fuerzas del orden, los CMLN continúan adaptando sus técnicas. Los corredores CMLN utilizan varias plataformas de mensajería cifrada para anunciar sus servicios y comunicarse con mulas de dinero, compradores de USD y clientes de TCO. Sellarán diferentes conversaciones en ciertas plataformas de mensajería cifrada para aumentar la seguridad operativa. Algunas mulas de dinero de CMLN ahora recogen efectivo de los DTOs en los aparcamientos de los bancos y depositan inmediatamente los fondos para limitar las oportunidades de interdicción de las fuerzas del orden. Cuando algunos mules de dinero de CMLN son alertados por bancos de que sus cuentas pueden cerrarse debido a actividades sospechosas, ingresan ingresos ilícitos en efectivo en la cuenta sabiendo que, cuando el banco cierre la cuenta, recibirán el saldo mediante cheque, blanqueando efectivamente los fondos. Las mulas de dinero de CMLN pueden operar decenas de cuentas en varios bancos diferentes bajo distintas identidades falsas y puede que no intenten activamente evitar el cierre de cuentas o los umbrales de notificación de la BSA.

Las CMLN están lavando cada vez más los beneficios de diversos esquemas de fraude utilizando transferencias bancarias y activos digitales para mover ingresos ilícitos para defraudadores extranjeros.[154] En febrero de 2025, tres personas, incluidos dos ciudadanos chinos que entraron en EE. UU. con visados de estudiante, fueron arrestadas por presuntamente crear empresas pantalla que blanquearon más de 13 millones de dólares robados a víctimas de estafas de inversión en activos digitales. Tras recibir los fondos de las víctimas mediante transferencia bancaria, los acusados supuestamente transfirieron esos fondos a cuentas bancarias en el extranjero y otros negocios nacionales y utilizaron las ganancias habidas para gastos personales. [155]

Las CMLN continúan blanqueando fondos de tarjetas regalo obtenidos mediante fraude para comprar bienes de alto valor, como se destacó en la NMLRA de 2024. En abril de 2025, tres ciudadanos chinos fueron condenados por blanquear los beneficios de diversos esquemas de fraude con tarjetas regalo. Según documentos judiciales, las TCOs con sede en China adquirieron más de 100 millones de dólares en tarjetas regalo hackeando empresas estadounidenses, manipulando tarjetas regalo físicas y atacando a ciudadanos estadounidenses mediante fraudes amorosos y de personas mayores. Luego enviaron los datos de las tarjetas regalo a varias células de ciudadanos chinos que operaban en Estados Unidos

151 FinCEN, "Aviso FinCEN sobre el uso de redes chinas de blanqueo de capitales por organizaciones criminales transnacionales con sede en México para blanquear ingresos ilícitos," (28 de agosto de 2025) https://www.fincen.gov/sites/default/files/advisory/2025-08-28/FinCEN-Advisory-CMLN-508. pdf.

152 HSI Cornerstone, "Organizaciones chinas de blanqueo de dinero (CMLOs) - Uso de pasaportes chinos falsificados," (enero de 2024) https:// content.govdelivery.com/bulletins/gd/USDHSICE-37fff16?wgt_ref=USDHSICE_WIDGET_217 153 DOJ, "Acusación federal alega alianza entre el cártel de Sinaloa y blanqueadores de dinero vinculados a la banca clandestina china," (18 de junio de 2024) https://www.justice.gov/archives/opa/pr/federal-indictment-alleges-alliance-between-sinaloa-cartel-and-money_Vinculados_a

los lavanderos.

154 Consulta la sección "Estafas de inversión en activos digitales" para un ejemplo de caso de activos digitales.

155 DOJ, "Tres acusados arrestados por denuncias federales que alegan haber recibido conscientemente más de 13 millones de dólares en dinero de víctimas de estafa," (25 de febrero de 2025) https://www.justice.gov/usao-cdca/pr/three-defendants-arrested-federal-complaints-alleging-they-recibieron-más-conscientemente 13.

Estados Unidos a través de una plataforma de mensajería con sede en China a cambio de activos digitales. Una vez que las células estadounidenses recibieron los datos de las tarjetas regalo, utilizaron las tarjetas regalo para comprar electrónica de alto valor, principalmente productos de Apple. Tras comprar los productos Apple, los miembros de la célula consolidaron la electrónica en almacenes para su envío a China, Hong Kong o países del sudeste asiático. Las células operaban principalmente en estados sin impuesto sobre las ventas, como New Hampshire, para maximizar sus beneficios. [156]

V. Trata de personas y tráfico de personas

La trata de personas y el tráfico de personas son industrias ilícitas de miles de millones de dólares para los TCOs que valoran el beneficio por encima de la seguridad humana y que a menudo se aprovechan de personas vulnerables. La trata de personas y las redes de tráfico de personas suponen una grave amenaza criminal con consecuencias devastadoras. La inmigración ilegal es un factor central que facilita tanto el tráfico de personas como para muchas formas de trata de personas, generando sustanciales ingresos ilícitos para las TCOs y redes asociadas, y generando un riesgo significativo de blanqueo de capitales a través del sistema financiero estadounidense. Aunque la trata y el tráfico de personas son delitos distintos, las personas que son traficadas son especialmente vulnerables a la trata de personas y otros delitos graves. La trata de personas implica la explotación de una persona para fines laborales, de servicios o de sexo comercial, mientras que el tráfico de personas implica traer extranjeros a Estados Unidos evadiendo deliberadamente las leyes migratorias y transportando y albergando ilegalmente a extranjeros que ya están presentes ilegalmente en el país.[157] Ambos delitos generan grandes beneficios, algunos de los cuales se blanquean a través del sistema financiero estadounidense por diversos medios, incluyendo compras de bienes raíces y de lujo, transferencias bancarias, tarjetas de crédito, aplicaciones de pago P2P, activos digitales y transferencias de efectivo al por mayor. El lavado exitoso de los beneficios ilícitos proporciona incentivos adicionales para perpetrar la explotación humana.

Trata de personas

La trata de personas es un delito que implica obligar o coaccionar a una persona a proporcionar trabajo, servicios o sexo comercial. La coacción puede ser sutil o abierta, física o psicológica. La explotación de un menor para fines sexuales comerciales es trata de personas, independientemente de si se ha utilizado cualquier forma de fuerza, fraude o coacción.[158] A diferencia del tráfico de personas, la trata de personas no requiere transporte ni movimiento a través de una frontera y puede ocurrir dentro de un solo país, estado, ciudad o comunidad.[159] Las víctimas en Estados Unidos incluyen ciudadanos estadounidenses, extranjeros con estatus migratorio legal y personas que están presentes ilegalmente, especialmente aquellas que entraron en Estados Unidos por rutas ilegales de contrabando y que posteriormente son explotadas por redes criminales. Las víctimas provienen de todos los orígenes socioeconómicos. La migración reciente, el consumo de sustancias, los problemas de salud mental, la implicación en el sistema de bienestar infantil y la falta de hogar juvenil son factores de riesgo significativos para la trata de personas. [160]

La trata de personas es un delito rentable, y los delitos de trata sirven como base para los delitos de blanqueo de capitales.[161] En 2024, la Línea Nacional de Trata de Personas de EE. UU. recibió notificaciones de 11.999 situaciones de posible trata de personas que involucraban a 21.865 víctimas, incrementos del 25 y 29 por ciento respectivamente en comparación con

156 DOJ, "Ciudadanos chinos condenados a prisión federal por participar en una conspiración fraudulenta de tarjetas regalo que implica la compra y exportación de productos Apple a China," (22 de abril de 2025) https://www.justice.gov/usao-nh/pr/chinese-nationals-sentenced-federal-prison_conspiración_de_tarjetas_regalo_fraudulentas_participantes.

157 Véase, DOJ, "Definición de la trata de personas", https://www.justice.gov/humantrafficking; ICE, "Tráfico de personas," (actualizado el 20 de agosto de 2025) https://www.ice.gov/about-ice/hsi/investigate/human-smuggling.

158 DOJ, "¿Qué es la trata de personas?" (actualizado el 26 de junio de 2023) https://www.justice.gov/humantrafficking/what-is-human-trafficking; Estado, "Informe sobre la trata de personas 2024," (junio de 2024) https://www.state.gov/wp-content/uploads/2025/02/TIP-Report-2024_Introduction_V10_508-accessible_2.13.2025.pdf.

159 DHS, "Campaña Azul, mitos y conceptos erróneos," (actualizado el 25 de agosto de 2022) https://www.dhs.gov/blue-campaign/myths-and- conceptos erróneos.

160 National Trafficking Hotline, "Trata de personas: ¿Quién es vulnerable?" (consultado el 15 de diciembre de 2025) https://humantraffickinghotline.org/en/human-trafficking#:~:text=Who%20is%20Vulnerable%3F,a%20runaway%20or%20homeless%20youth;

DHS, "Datos rápidos sobre la trata de personas" (actualizado el 22 de mayo de 2025) https://www.dhs.gov/human-trafficking-quick-facts.

161 Estado y Tesoro, "Informe al Congreso sobre un análisis de los esfuerzos contra el blanqueo de capitales relacionados con la trata de personas" (7 de octubre de 2020) https://home.treasury.gov/system/files/136/Report-Money-Laundering-Human-Trafficking.pdf.

el año anterior.[162] Una agencia federal de seguridad de EE. UU. inició más de 1.500 casos relacionados con posible trata de personas entre octubre de 2023 y septiembre de 2024.[163] Estas investigaciones policiales y los informes gubernamentales indican que la trata de personas es una industria criminal multimillonaria en Estados Unidos.

Los datos y estimaciones exactas de los ingresos criminales siguen siendo difíciles de determinar debido a la naturaleza ilícita de la actividad delictiva. En marzo de 2024, la Organización Internacional del Trabajo (OIT) de las Naciones Unidas (ONU) estimó que el trabajo forzado generaba más de 236.000 millones de dólares en beneficios ilícitos globales anualmente, con 52.000 millones en América, y que la explotación sexual comercial forzada constituye más de dos tercios (73 por ciento) de los beneficios ilegales totales a nivel mundial, mientras que solo representa el 27 por ciento de las víctimas. [164]

La actividad financiera derivada de la trata de personas se cruza con el sistema financiero regulado durante las etapas de reclutamiento, transporte y explotación. Las transacciones relacionadas con la trata de personas incluyen pagos relacionados con el transporte y alojamiento de víctimas; la recaudación de los ingresos generados por la explotación de víctimas; y el movimiento de los beneficios.[165] FTOs y TCOs designados también financian actividades relacionadas con la trata de personas para generar ingresos ilícitos para sus organizaciones y blanquear fondos. Los TCO invierten en empresas de transporte, distribuidores de alimentos y empresas de importación/exportación para operar y ocultar sus actividades relacionadas con la trata. Empresas que de otro modo parecen legítimas pueden estar blanqueando dinero para facilitar la trata de personas. [166]
Los ingresos ilícitos de la trata de personas pueden pagarse en efectivo, en sistemas de transferencias electrónicas de fondos/remesas, transacciones con tarjeta de crédito, aplicaciones de pago o activos digitales. En los últimos años, las plataformas de redes sociales han surgido como facilitadoras de la trata sexual.[167] En Estados Unidos, la trata de personas se produce en una amplia variedad de industrias, incluyendo hostelería, agricultura, sanidad (como auxiliares de salud doméstica o residencias de ancianos), silvicultura y tala, manufactura, servicios de limpieza comercial, construcción, servicios de salud y belleza, venta ambulante y mendicidad, industrias de servicios de alimentación, servicios de salones de salud, trabajo doméstico, ferias y carnavales, masajes ilícitos y servicios de acompañamiento, y tráfico y distribución de drogas. [168]

En abril de 2025, Estados Unidos acusó a 27 personas actualmente o anteriormente asociadas con Tren de Aragua, una organización de operaciones de comercio designada por el Departamento de Estado de EE. UU. en febrero de 2025, de múltiples delitos, incluyendo conspiración para la trata de personas sexuales.[169] Según las acusaciones contenidas en las acusaciones, las mujeres introducidas de contrabando en Estados Unidos pagarían las "deudas" contraídas con el Tren de Aragua mediante actos sexuales comerciales en el país. Los miembros de la organización criminal hacían cumplir la situación amenazando con matar a las mujeres y sus familias;

162 National Human Trafficking Hotline, "Estadísticas Nacionales, Casos Identificados en 2024," (consultado el 15 de diciembre de 2025) https:// humantraffickinghotline.org/en/statistics.

163 DHS, "Combatiendo la trata de personas: Año fiscal 2024 en revisión," (julio de 2025), https://www.dhs.gov/sites/default/ archivos/2025-08/25_00809_ccht_fy24-year-in-review-annual-report_508.pdf.

164 Organización Internacional del Trabajo, Naciones Unidas, "Beneficios y pobreza: la economía del trabajo forzado," (19 de marzo de 2024) https:// www.ilo.org/resource/news/annual-profits-forced-labour-amount-us-236-billion-ilo-report-finds. La OIT descubrió que traficantes y criminales generan cerca de 10.000 dólares por víctima.

165 FinCEN, "Asesoramiento suplementario sobre la identificación y reporte de la trata de personas y actividades relacionadas," (15 de octubre de 2020) https://www. fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf; *Véase también,* FinCEN, "Alerta sobre el Tráfico de Personas a lo largo de la Frontera Suroeste de Estados Unidos" (13 de enero de 2023) https://www.fincen.gov/sites/default/files/ compartido/FinCEN%20Alert%20Human%20Smuggling%20FINAL_508.pdf

166 GAO, "Trata y blanqueo de dinero: estrategias utilizadas por grupos criminales y terroristas y esfuerzos federales para combatirlos," (diciembre de 2021), p. 10, https://www.gao.gov/assets/gao-22-104807.pdf.

167 *Véase, por ejemplo,* DOJ, "Traficante sexual reincidente es condenado a 27 años de prisión," (7 de julio de 2025) https://www.justice.gov/usao-wdnc/pr/repeat- tratante sexual condenado a 27 años de prisión.; DOJ, "Hombre del condado de St. Louis condenado a 125 meses de prisión por trata sexual de adolescente fugada," (11 de diciembre de 2025) https://www.justice.gov/usao-edmo/pr/st-louis-county-man-sentenced-125-months-prison-sex-trafficking- adolescente fugada.

168 DHS, "Combatiendo la trata de personas: un año en revisión," (febrero de 2024) https://www.dhs.gov/sites/default/files/2024-03/24_0223_ ccht_year-in-review-annual-report_508.pdf; Polaris, "La tipología de la esclavitud moderna," (30 de agosto de 2023) https://polarisproject.org/ la tipología de la esclavitud moderna/.

169 DOJ, "27 miembros o asociados de Tren de Aragua acusados de extorsión, narcóticos, trata de personas, robo y delitos con armas de fuego," (21 de abril de 2025)
https://www.justice.gov/opa/pr/27-members-or-associates-tren-de-aragua-charged-racketeering-narcotics- trata sexual.

agredirlos, dispararles o matarles; la incautación de documentos de inmigración estadounidenses pertenecientes a las mujeres y sus familias; y rastrear y secuestrar a mujeres que intentaron huir.

En marzo de 2025, una madre y un hijo fueron condenados por sus roles en la gestión de salones de masajes que funcionaban como tapaderas para operaciones comerciales de sexo. Los documentos judiciales revelaron que, en al menos 10 ocasiones entre junio de 2023 y febrero de 2024, agentes encubiertos compraron masajes por diferentes cantidades en los salones de Texas y Nuevo México. Los agentes también observaron el vehículo de la acusada transportando a mujeres asiáticas directamente desde el aeropuerto hasta sus salones de masajes. Los vecinos dijeron que las mujeres nunca salieron del edificio. Los registros de las instalaciones revelaron camas colocadas en el suelo, lo que sugiere que las mujeres vivían en los salones de masajes. Los registros del casino revelaron que la demandada viajaba frecuentemente a California para blanquear los beneficios de sus negocios ilícitos de salones de masajes. Entre enero de 2018 y agosto de 2023, retiró aproximadamente 1.771.360 dólares en fichas del casino. [170]

Tráfico de personas

Los traficantes de personas cometen el delito de facilitar la entrada ilegal de individuos a través de fronteras internacionales mediante la evasión deliberada de las leyes migratorias, generando a menudo importantes beneficios ilícitos que se blanquean a través de sistemas financieros nacionales e internacionales. El tráfico de personas es un delito inherentemente transnacional, con traficantes que explotan rutas legítimas de comercio y viaje para traer personas a Estados Unidos a pie y mediante diversos medios de transporte, como aviones, barcos, tráileres y automóviles. Las redes de contrabando pueden estar vinculadas a otras formas de crimen organizado, como el narcotráfico, el contrabando de armas y el terrorismo.[171] Aunque los siguientes ejemplos se centran en la frontera sur, también operan traficantes de personas a lo largo de la frontera norte y otros puntos de entrada. [172]

Las redes de tráfico de personas son lucrativas. En solo un caso, los investigadores federales descubrieron pruebas que sugieren que una TCO con sede en Guatemala generó entre 104 y 416 millones de dólares en ingresos ilícitos procedentes de sus actividades de tráfico de personas entre septiembre de 2020 y abril de 2023.[173] La OIT estima que traficantes y criminales generan cerca de 10.000 dólares por víctima o más, según los casos estadounidenses. En uno de los programas de contrabando y trata de mano de obra entre 2022 y 2023, los traficantes en México y Estados Unidos cobraron a las personas entre 15.000 y
20.000 dólares por cruzar la frontera hacia Estados Unidos.[174] Los contrabandistas también exigieron que muchas víctimas entregaran propiedades como garantía antes de abandonar México. Dado que este delito genera beneficios significativos, los contrabandistas pueden seguir rutas peligrosas, exponiendo a los migrantes a deshidratación, asfixia u otros daños. Los migrantes sufren frecuentemente agresiones, violaciones y extorsiones cometidas por traficantes de personas, motivados por ganancias económicas.

En otro caso presentado en septiembre de 2025, 12 acusados operaron una prolífica operación de tráfico de extranjeros que facilitó la entrada ilegal de ciudadanos cubanos en Estados Unidos mediante la preparación de supuestas solicitudes de visado, el blanqueo de millones de dólares en pagos y la explotación del proceso migratorio. Según la acusación de sustitución, desde enero de 2021 hasta junio de 2025, los acusados promovieron servicios de visados falsos en línea, alegando que ciudadanos cubanos podían asegurar la entrada estadounidense mediante falsas afirmaciones de ciudadanía europea. Presentaron cientos de solicitudes fraudulentas del Sistema Electrónico de Autorización de Viaje (ESTA) ante la Oficina de Aduanas y Protección Fronteriza de EE. UU. (CBP), utilizando direcciones falsas y documentos falsificados. Los demandados cobraron a los clientes entre 1.500 y
40.000 dólares, a veces incluso fletando aviones privados para mover grupos de extranjeros. Los registros muestran que gastaron más de 2,5 millones de dólares solo en vuelos y canalizaron más de 7 millones a través de aplicaciones de pago como Zelle. Basado en un análisis financiero realizado de 27 cuentas conocidas asociadas con el

170 DOJ, "Operadores ilícitos de salones de masaje sentenciados," (19 de marzo de 2025) https://www.justice.gov/usao-ndtx/pr/illicit-massage-parlor- operadores-sentenciados.

171 DHS, "Entendiendo el tráfico de personas", https://www.ice.gov/about-ice/hsi/investigate/human-smuggling.

172 DOJ, "Hombre canadiense arrestado y detenido por su participación en la conspiración mortal de tráfico de extranjeros en la frontera norte de EE. UU.", (1 de julio de 2025)

https://www.justice.gov/opa/pr/canadian-man-arrested-and-detained-role-deadly-alien-smuggling-conspiracy-uss-northern. 173 DOJ, "Ocho miembros de la Organización de Tráfico de Personas López que operan en Guatemala, México y Estados Unidos acusados y dos arrestados" (25 de julio de 2024) https://www.justice.gov/usao-nm/pr/eight-members-lopez-human-smuggling-organization-operating- Guatemala-México-y-United.; DOJ, "Nueve miembros de la organización de tráfico de personas López se declaran culpables de cargos federales" (16 de junio de 2025) https://www.justice.gov/usao-nm/pr/nine-members-lopez-human-smuggling-organization-plead-guilty-federal-charges 174 DOJ, "Un nacional mexicano admite su papel en el esquema de contrabando y trata laboral," (24 de octubre de 2024) https://www.justice.gov/usao-ct/ pr/mexicano-nacional-admite-papel-contrabando-y-tráfico-laboral-esquema.

acusados y sus cómplices, la organización de contrabando de extranjeros recaudó más de 18 millones de dólares durante la conspiración. [175]

Los cárteles se han diversificado cada vez más hacia el tráfico de personas como parte de sus operaciones ilícitas para ganar dinero. En noviembre de 2024, dos altos cargos miembros del cártel fueron condenados a prisión por su implicación en una extensa conspiración de tráfico de personas que involucraba a CDN, uno de los TCOs más violentos de México y una FTO designada por Estados Unidos. El CDN ejerce una influencia significativa sobre toda la actividad económica cerca de Nuevo Laredo[176] y utiliza las redes sociales para anunciar sus servicios de transporte para personas que intentan entrar ilegalmente en Estados Unidos.[177] TCOs y FTOs que mantienen el control sobre el territorio de tráfico de drogas también se benefician de esta actividad ilegal cobrando a las organizaciones de contrabando una tasa o impuesto por pasar por sus territorios. [178]

En marzo de 2025, el Tesoro tomó medidas contra la Organización de Tráfico de Personas López (HSO), una organización de tráfico de personas con sede en Guatemala responsable de traficar a miles de inmigrantes ilegales desde Guatemala, pasando por México y hacia Estados Unidos. Las designaciones del Tesoro se realizaron en coordinación con acciones policiales estadounidenses contra la HSO López y un miembro del cártel La Línea que ayudó en las operaciones de tráfico de personas de la organización en México y hacia Estados Unidos.[179] La Línea está alineada con CJNG, una TCO designada por la FTO, con CJNG sirviendo como fuente de suministro de cocaína, metanfetamina y fentanilo de La Linea.[180] Como se ha descrito anteriormente, las pruebas descubiertas por investigadores federales sugieren que la HSO de López generó entre 104 y 416 millones de dólares en ingresos ilícitos de sus actividades de tráfico de personas entre septiembre de 2020 y abril de 2023.[181] La HSO de López empleaba una red de contrabandistas de nivel medio para llevar a cabo las operaciones diarias y abrir cuentas bancarias en EE. UU. Además, la organización utilizó aplicaciones de transferencia de dinero P2P y efectivo masivo para facilitar los pagos entre co-conspiradores. Los miembros de la organización también compraron bienes inmuebles y utilizaron MSB para transferir dinero a los miembros de la HSO López en Guatemala. [182]

En conjunto, estos casos demuestran que la inmigración ilegal se ha convertido en una fuente significativa de ingresos para los TCO y los FTOs, con los ingresos del tráfico de personas que cada vez se cruzan más con instituciones financieras formales, plataformas de pago y activos con sede en EE. UU.

VI. Corrupción

La corrupción sigue generando cantidades significativas de ingresos ilícitos que tanto actores corruptos nacionales como extranjeros buscan blanquear a través de Estados Unidos. Las actividades corruptas pueden incluir sobornos, malversación, extorsión, recepción de sobornos, manipulación o manipulación de contratos gubernamentales, diversos tipos de fraude y una serie de otras actividades y delitos relacionados con abusos de poder público, posición y confianza. En casos nacionales y extranjeros, las tipologías relacionadas con la corrupción suelen implicar el uso indebido de entidades legales, el blanqueo de fondos corruptos mediante compras inmobiliarias, la sobrefacturación o insuficiente de bienes o servicios prestados como parte de contratos gubernamentales, y pagos de sobornos que

involucran efectivo o cuentas bancarias offshore. Estados Unidos

175 DOJ, "Doce personas acusadas por su papel en conspiraciones de tráfico internacional de extranjeros, fraude de asilo y blanqueo de capitales," (4 de septiembre de 2025) https://www.justice.gov/opa/pr/twelve-people-charged-their-roles-international-alien-smuggling-asylum-fraud-and-money. 176 Hacienda, "Hacienda sanciona a altos cargos de la organización terrorista extranjera Cartel del Noreste," (21 de mayo de 2025) https://home.treasury.gov/news/press-releases/sb0146.

177 ICE, "Miembros del Cartel del Noreste enviados a prisión por roles en un esquema de tráfico de personas vinculado a cárteles," (4 de noviembre de 2024) https:// www.ice.gov/news/releases/cartel-del-noreste-members-sent-prison-roles-cartel-linked-human-smuggling-scheme.

178 ICE, "El tráfico de personas equivale a grave peligro, mucho dinero," (actualizado el 29 de enero de 2025) https://www.ice.gov/features/human-smuggling- peligro.

179 Tesorería, "El Tesoro apunta a líder mexicano de organización criminal transnacional responsable de el tráfico de miles de migrantes a través de la frontera sur de EE. UU.", (18 de marzo de 2025) https://home.treasury.gov/news/press-releases/sb0051.

180 Tesoro, "Hacienda sanciona a miembros clave de La Linea, un grupo implicado en el tráfico de fentanilo hacia Estados Unidos," (31 de octubre de 2024) https://home.treasury.gov/news/press-releases/jy2704.

181 DOJ, "Ocho miembros de la Organización de Tráfico de Personas López que operan en Guatemala, México y Estados Unidos

acusados y dos arrestados" (25 de julio de 2024) https://www.justice.gov/usao-nm/pr/eight-members-lopez-human-smuggling-organization-operating- Guatemala-México-y-Unidos.

182 DOJ, "Nueve miembros de la organización de tráfico de personas López se declaran culpables de cargos federales" (16 de junio de 2025) https://www.justice.gov/usao-nm/pr/nine-members-lopez-human-smuggling-organization-plead-culpy-federal-charges.

investiga y procesa presuntas conductas indebidas que presentan fuertes indicios de intención corrupta, como pagos sustanciales de sobornos, intentos probados y sofisticados de ocultar pagos, conductas fraudulentas en el apoyo a esquemas de soborno y esfuerzos para obstruir la justicia, independientemente de la nacionalidad de las personas o entidades implicadas. [183]

Corrupción interna

La corrupción dentro de Estados Unidos ocurre en todos los niveles de gobierno, desde las autoridades locales hasta los funcionarios federales. En estos casos, los casos de corrupción implican cada vez más no solo los intentos de los funcionarios de enriquecerse a través de sus cargos públicos, sino también actores ilícitos— incluidos TCOs y gobiernos extranjeros— que llevan a cabo prácticas corruptas para promover sus intereses estratégicos. Los casos de corrupción nacional varían mucho en su sofisticación, con algunas de estas actividades realizadas mediante simples pagos en efectivo, y otras ocultas mediante el uso indebido de empresas pantalla, honorarios de consultoría y cuentas bancarias a nombre de asociados de funcionarios públicos, entre otros métodos.

En un caso, cuatro hombres, incluido un funcionario de contratación gubernamental de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID), se declararon culpables de sus roles en un esquema de soborno de una década que involucraba al menos 14 contratos de primera línea por un valor superior a 550 millones de dólares de los contribuyentes estadounidenses. Según documentos judiciales, el oficial de contratación de USAID accedió a recibir sobornos a cambio de influir en la adjudicación de los contratos. Durante todo el plan, recibió dinero en efectivo, portátiles, miles de dólares en entradas para una suite en un partido de la NBA, una boda en un club de campo, entradas de dos hipotecas residenciales, teléfonos móviles y trabajos para familiares. Los sobornos también se ocultaban a menudo mediante transferencias bancarias electrónicas que lo listaban falsamente en la nómina, empresas pantalla constituidas y facturas falsas. Se le alega que recibió sobornos valorados en más de aproximadamente un millón de dólares como parte del esquema. [184]

Los TCO y los gobiernos extranjeros también intentan involucrarse con las fuerzas de seguridad estadounidenses u otros funcionarios públicos actuales o anteriores para buscar una ventaja estratégica. Estos esquemas suelen implicar pagos en efectivo a personal de las fuerzas del orden, el mal uso de empresas pantalla o pagos en capas a asociados de funcionarios públicos. En julio de 2025, dos agentes de la CBP se declararon culpables de conspirar con miembros de una DTO con sede en México para permitir la entrada de vehículos cargados de drogas a Estados Unidos sin inspección. Como parte del programa, los dos hombres, que trabajan en los puertos de entrada de California, informarían a los miembros de la DTO qué hora y carril se les asignó utilizando un código secreto basado en emojis. El DTO enviaría entonces los coches cargados de drogas por los carriles de los agentes, sabiendo que los dos hombres inspeccionarían esos vehículos. Estados Unidos ha alegado que ambos demandados obtuvieron beneficios generosos, financiando tanto viajes nacionales como internacionales, así como la compra de artículos de lujo e intentos de adquirir bienes inmuebles en México. [185]

Corrupción extranjera

El blanqueo de capitales asociado a la corrupción extranjera puede implicar que los ingresos de la corrupción extranjera pasen por el sistema financiero estadounidense o se trasladen a Estados Unidos, utilizando una variedad de métodos. Las fuerzas del orden informan que actores corruptos extranjeros a menudo buscan trasladar los beneficios de sobornos, malversaciones y otros actos corruptos a Estados Unidos, dada la estabilidad del mercado estadounidense y el potencial de retornos de inversión. Además, informan de que—paradójicamente— el fuerte estado de derecho en Estados Unidos en comparación con otras jurisdicciones ayuda a proteger los ingresos de actores corruptos frente al robo, la extorsión u otras actividades. Los ingresos corruptos extranjeros que se blanquean a través de Estados Unidos suelen implicar pagos de sobornos a funcionarios gubernamentales en países en desarrollo, especialmente en América Latina, a cambio de trato preferencial o la adjudicación de contratos gubernamentales. Los funcionarios de estos países suelen tener los mayores incentivos para trasladar sus ingresos corruptos a una economía geográficamente cercana y estable con fuertes protecciones de privacidad, siendo Estados Unidos un candidato ideal para estos fines ilícitos.

183 DOJ, "Directrices para la Investigación y Aplicación de la Ley de Prácticas Corruptas en el Extranjero (FCPA)," (9 de junio de 2025) https://www.justice. gobierno/dag/medios/1403031/dl.

184 DOJ, "Un funcionario de USAID y tres ejecutivos corporativos se declaran culpables de un esquema de soborno de una década que implicaba más de 550 millones de dólares en contratos; Dos empresas admiten responsabilidad penal por esquema de soborno y fraude de valores," (12 de junio de 2025) https://www.justice.gov/ usao-md/pr/usaid-oficial-y-propietarios-de-empresas-y-three-corporativos-declaran-culpable-de-década

185 DOJ, "Dos agentes de la CBP se declaran culpables de permitir la entrada de drogas en EE. UU. A través de sus carriles de inspección," (28 de julio de 2025) https://www.justice.gov/usao-sdca/pr/two-cbp-officers-plead-guilty-allowing-drugs-enter-us-through-their-inspection-lanes.

En un caso, un ciudadano colombiano fue condenado a 12 años y siete meses de prisión por conspirar para blanquear los fondos de sobornos. Como parte de su alegación, el hombre admitió que, mientras era funcionario portuario en Colombia, aceptó al menos 1.000.000 de dólares en sobornos ilegales que él y sus cómplices blanquearon a Estados Unidos desde Colombia. Como parte del plan, el hombre y sus cómplices blanquearon los fondos para su beneficio y usaron esos fondos para comprar vehículos de lujo y pagar alquileres de propiedades frente al mar, entre otras cosas. [186]

Dada la centralidad del sistema financiero estadounidense en la arquitectura global de pagos, entre otros factores, fondos asociados a sobornos extranjeros, malversación, sobornos u otras prácticas corruptas han transitado por Estados Unidos a través de cuentas bancarias corresponsales y otros canales. Estos pagos suelen estar relacionados con sobornos pagados por empresas extranjeras o nacionales a funcionarios gubernamentales en terceros países a cambio de adjudicación de contratos o trato preferencial.[187] El blanqueo de estos fondos implica frecuentemente facturas falsas, sobrefacturación de bienes o servicios, empresas pantalla nacionales y extranjeras, y cuentas bancarias offshore para ayudar a ocultar los pagos.

En diciembre de 2025, un empresario mexicano residente en Estados Unidos fue condenado por su participación en un esquema para sobornar a funcionarios del gobierno mexicano en Petróleos Mexicanos (PEMEX), la petrolera estatal de México, y su filial de propiedad total, PEMEX Exploración y Producción (PEP). Según documentos judiciales y pruebas presentadas en el juicio, el hombre pagó más de 150.000 dólares en sobornos a funcionarios de PEP para retener contratos y pagos de PEMEX y PEP y obtener otras ventajas indebidas en negocios con PEMEX y PEP, en beneficio de empresas asociadas a él. Las pruebas del juicio mostraron que entre aproximadamente 2019 y 2021, el hombre y sus cómplices ofrecieron pagar y pagaron sobornos en forma de pagos en efectivo, bienes de lujo y otros objetos valiosos a al menos tres funcionarios de PEMEX y PEP a cambio de que estos funcionarios tomaran ciertas acciones para ayudar a empresas asociadas con él a obtener y mantener negocios con PEMEX y PEP. Esas ventajas indebidas ayudaron a las empresas asociadas con el hombre a obtener contratos con PEMEX y PEP por valor mínimo de 2,5 millones de dólares. [188]

VII. Comercio ilícito

El tráfico de bienes robados, ilícitos o regulados es un negocio lucrativo que atrae a organizaciones criminales de todos los tamaños y niveles de sofisticación. Para los TCOs, esto también puede ser una forma de diversificar las fuentes de ingresos ilícitas y ampliar sus áreas de influencia. El comercio ilícito no es un delito sin víctimas; defrauda a los contribuyentes y priva al gobierno de ingresos vitales utilizados para reinvertir en Estados Unidos, al tiempo que amenaza industrias nacionales críticas, socava la confianza del consumidor y debilita la seguridad nacional. Para combatir el comercio ilícito, en agosto de 2025 el DOJ y el DHS lanzaron un Grupo de Trabajo Interinstitucional sobre Fraude Comercial para aplicar una aplicación contundente contra importadores y otras partes que buscan defraudar a Estados Unidos. El Grupo de Trabajo reforzará los mecanismos de coordinación existentes para llevar a cabo de forma enérgica acciones de cumplimiento contra cualquier parte que intente evadir aranceles y otros aranceles, así como contra contrabandistas que busquen importar bienes prohibidos a la economía estadounidense. [189]

El comercio ilícito ocurre en casi todos los sectores de la economía, aunque los esquemas específicos pueden variar mucho según el tipo de bien y las leyes y regulaciones existentes. Los beneficios del comercio ilícito suelen ser blanqueados siendo presentados como ingresos legítimos del comercio, respaldados por documentación fraudulenta, comerciantes cómplices o funcionarios corruptos. Además de generar ingresos mediante comercio ilícito, los delincuentes también pueden blanquear los beneficios de otros delitos como

186 DOJ, "Exfuncionario portuario colombiano condenado a más de doce años de prisión por blanqueo de dinero," (9 de mayo de 2025) https://www. justice.gov/opa/pr/former-colombian-port-official-sentenced-over-twelve-years-prison-money-laundering. 187 *Véase, por ejemplo,* DOJ, "Raytheon Company Pay Over $950M In Connection with Defective Pricing Schemes, Foreign Bribery, and Export Control Schemes," (16 de octubre de 21024) https://www.justice.gov/archives/opa/pr/raytheon-company-pay-over-950m-connection-defective-fiking-foreign-bribery-and-export.

188 DOJ, "Empresario de Texas condenado por esquema para sobornar funcionarios del gobierno mexicano," (5 de diciembre de 2025) https://www.justice.gov/ opa/pr/empresario-texano-convicto-esquema de sobornos.

189 DOJ, "Los Departamentos de Justicia y Seguridad Nacional colaboran en el Grupo de Trabajo sobre Fraude Comercial Interinstitucional," (29 de agosto de 2025) https:// www.justice.gov/opa/pr/departments-justice-and-homeland-security-partnering-cross-agency-trade-fraud-task-force.

parte de sus operaciones en esquemas TBML. Los ejemplos siguientes destacan solo algunas de las formas en que los criminales utilizan el comercio ilícito para obtener beneficios.

Contrabando de petróleo

En los últimos años, el robo de combustible y los esquemas de contrabando de crudo se han convertido en la fuente de ingresos no relacionada con las drogas más importante para las TCOs con sede en México.[190] Según se describe en una alerta FinCEN de mayo de 2025, los TCOs con sede en México utilizan intermediarios mexicanos cómplices para contrabandear y vender crudo robado a la empresa estatal energética mexicana, PEMEX, a pequeños importadores cómplices de petróleo y gas natural con sede en Estados Unidos.[191] Durante estas operaciones, el aceite robado y contrabandista suele ser etiquetado erróneamente como "aceite residual" u otro material supuestamente peligroso. Las empresas cómplices venden entonces los productos en los mercados energéticos de EE. UU. y a nivel mundial, y repatrian los ingresos ilícitos de vuelta a México.

En mayo de 2025, la OFAC sancionó a tres ciudadanos mexicanos y dos entidades con base en México involucradas en una red de narcotráfico, robo de combustible y contrabando de petróleo que genera cientos de millones de dólares anuales para la CJNG.[192] Ese mismo mes, dos ciudadanos estadounidenses fueron acusados formalmente de cargos relacionados con proporcionar apoyo material a la CJNG por supuestamente importar ilegalmente decenas de millones de dólares en crudo y conspirar para realizar transacciones financieras con el fin de ocultar y disfrazar la naturaleza y el origen de los beneficios del crudo contrabandeado. [193]

Evasión de tarifas

Para importar mercancías a Estados Unidos, la parte que realiza la entrada debe declarar, entre otras cosas, el valor de los bienes, si los bienes están sujetos a aranceles, el tipo arancelario aplicable y la cantidad adeudada. La CBP se apoya en estas representaciones para imponer y cobrar aranceles sobre mercancías importadas.[194] Quienes buscan evadir aranceles suelen recurrir a documentos fraudulentos para hacer declaraciones falsas a CBP. En un caso, una empresa indonesia de joyería, su copropietario indonesio y otros dos empleados indonesios e italianos fueron acusados de participar en un esquema para evadir ilegalmente más de 86 millones de dólares en aranceles y tarifas aduaneras sobre más de 1.200 millones de dólares en importaciones de joyería a Estados Unidos. Según los documentos presentados en este caso y las declaraciones hechas en el tribunal, los acusados participaron en al menos dos esquemas relacionados y superpuestos. En uno de los esquemas, la empresa y sus cómplices eludieron los derechos fabricando joyas en Indonesia y luego enviándolas a Jordania, que tenía un Acuerdo de Libre Comercio con Estados Unidos, antes de enviarlas a Estados Unidos. Los demandados entonces afirmaron falsamente que las joyas de la empresa se habían fabricado en Jordania, lo que evitaba el impuesto que de otro modo se aplicaría. [195]

Comerciantes cómplices

Los comerciantes cómplices pueden ayudar a organizaciones criminales comprando bienes robados para revenderlos o permitiendo que se vendan a través de sus mercados. Dependiendo del tipo de bien robado, estas transacciones pueden realizarse a través de intermediarios mayoristas, mercados online,[196] o minoristas físicos. Las redes de delincuencia doméstica también pueden generar cientos de millones de dólares gracias a comerciantes cómplices dispuestos a traficar con bienes robados. En julio de 2025, una

190 Tesoro, "Hacienda apunta a un gran cártel mexicano implicado en tráfico de fentanilo y robo de combustible," (1 de mayo de 2025) https://home.treasury. gov/news/press releases/sb0125.

191 Véase en general, FinCEN, "Alerta sobre esquemas de contrabando de petróleo en la frontera suroeste de EE. UU. asociados con cárteles con sede en México," (1 de mayo de 2025) https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-Oil-Smuggling-FINAL-508C.pdf.

192 Hacienda, "Hacienda apunta a un gran cártel mexicano implicado en el tráfico de fentanilo y el robo de combustible," (1 de mayo de 2025) https://home.treasury. gobierno/noticias/comunicados de prensa/SB0125.

193 DOJ, "Padre e hijo acusados por proporcionar apoyo material a cártel mexicano implicado en terrorismo," (30 de mayo de 2025) https://www. justice.gov/usao-sdtx/pr/father-and-son-indicted-providing-material-support-mexican-cartel-engaged-terrorism.

194 *Véase, por ejemplo,* DOJ, "Estados Unidos presenta una queja contra Barco Uniforms y sus proveedores, alegando violaciones de la Ley de Reclamaciones Falsas en Relación con Derechos Aduaneros Mal Pagados," (18 de abril de 2025) https://www.justice.gov/opa/pr/united-states-files-complaint-against- uniformes-barco-y-sus-proveedores-alegando-reclamaciones-falsas; DOJ, "Importador de Miami se declara

culpable de un plan para evadir aranceles estadounidenses sobre neumáticos de camiones fabricados en China," (6 de diciembre de 2024) https://www.justice.gov/usao-sdfl/pr/miami-importer-pleads-guilty-scheme-evade-us-tariffs- neumáticos de camiones fabricados en China.

195 DOJ, "Empresa de joyería indonesia, copropietario y otros dos empleados acusados en un esquema de evasión arancelaria y de aranceles a gran escala," (17 de noviembre de 2025) https://www.justice.gov/usao-nj/pr/indonesian-jewelry-company-co-owner-and-two-other-employees-charged-aranceles-y-aranceles.

196 *Véase, por ejemplo,* DOJ, "El primero de un par de hombres acusados en un esquema masivo de tráfico de bienes robados se declara culpable," (15 de septiembre de 2025) https://www.justice.gov/usao-wdwa/pr/first-pair-men-charged-massive-stolen-goods-trafficking-scheme-enters-guilty-plea.

Un hombre de Nueva Jersey se declaró culpable de liderar una operación multiestatal que robó miles de catalizadores de vehículos particulares y de recibir más de 600 millones de dólares a través de su negocio al revender los catalizadores robados a una refinería de metales que extraía los metales preciosos. [197]

Los comerciantes cómplices que trafican mercancías robadas también pueden ayudar a otros TCOs que atacan a estadounidenses. En un caso, un hombre se declaró culpable de recibir y comprar bienes robados, incluyendo joyas, relojes, bolsos y diversos objetos de lujo robados por equipos con base en Sudamérica, que viajaban por Estados Unidos cometiendo robos. El hombre y su coacusado fueron vinculados a al menos dos docenas de robos residenciales o comerciales en todo Estados Unidos. También compraron objetos en su local comercial en el Distrito de Diamantes de Manhattan a un detective encubierto después de que el detective informara a los acusados de que los objetos habían sido robados. [198]

Tráfico de fauna silvestre y otros delitos relacionados con la naturaleza

Como actualización de la sección de la NMLRA 2024 sobre tráfico de vida silvestre y otros delitos relacionados con la naturaleza, el Tesoro continúa monitorizando la intersección de esta actividad delictiva con otras amenazas como el narcotráfico y el crimen organizado transnacional. Los delitos relacionados con la naturaleza incluyen formas ilícitas de tala, minería, comercio de fauna, conversión de tierras y actividades delictivas asociadas, así como delitos asociados a la pesca ilegal, no declarada y no regulada (INDNR).[200] Esta amplia categoría de delitos implica que actores ilícitos abusen del sistema financiero internacional para blanquear los beneficios ilícitos asociados, obtener ventajas competitivas injustas sobre las empresas estadounidenses y robar a nuestro país su belleza natural y recursos. [201]

Estados Unidos ha intentado cortar los ingresos de los TCOs que se benefician de delitos relacionados con la naturaleza, incluida la pesca INDNR. Por ejemplo, en noviembre de 2024, la OFAC sancionó a cinco ciudadanos mexicanos asociados con CDG y actividades delictivas relacionadas con la pesca INDNR. A menudo, la pesca INDNDR es una fuente de ingresos para un número creciente de organizaciones criminales, y sus actividades ilícitas pueden representar una competencia desleal por pesca legal por parte de pescadores estadounidenses. La pesca INDNDR también representa una amenaza para la seguridad marítima de EE. UU., ya que las organizaciones criminales pueden utilizar las mismas embarcaciones para el contrabando de narcóticos y personas a través de fronteras. [202]

Actores ilícitos continúan atacando el sistema financiero estadounidense para facilitar grandes programas de contrabando de oro y blanqueo de capitales. Según las acusaciones en la acusación en un caso reciente, tres personas recibieron envíos de una empresa colombiana que supuestamente contenían varios tipos de productos metálicos cuando, en realidad, la mitad de los paquetes contenían cilindros de oro sin declarar que se insertaron dentro de los productos y se pintaron para evitar ser detectados. Los individuos extraían los cilindros de oro, vendían el oro a través de dos entidades corporativas estadounidenses y luego transferían los fondos entre las cuentas bancarias de las entidades antes de transferir finalmente los fondos a las cuentas de la empresa colombiana en Colombia.[203] Además, la OFAC sancionó a miembros de una de las familias más ricas de Guyana y a su empresa por promover la corrupción pública mediante la explotación del sector del oro del país. Por ejemplo, la entidad pagó sobornos a funcionarios del gobierno guyanés para facilitar la adjudicación de contratos gubernamentales. Una vez extraído, el oro de origen guyanano se vende y comercializa en mercados internacionales, incluidos Estados Unidos. [204]

197 DOJ, "Líder de la red nacional de robos de convertidores catalíticos se declara culpable y admite haber vendido bienes robados por más de 600 millones de dólares," (21 de julio de 2025) https://www.justice.gov/opa/pr/leader-national-catalytic-converter-theft-ring-pleads-guilty-and-admits-selling-stolen-goods. 198 DOJ, "El Distrito de Diamond Fence se declara culpable en relación con una operación de propiedad robada a gran escala," (18 de julio de 2025) https://www. justice.gov/usao-edny/pr/diamond-district-fence-pleads-guilty-connection-large-scale-stolen-property-operation. 199 *Ver, por ejemplo,* DOJ, "Ciudadano chino sentenciado por contrabando de tortugas desde Estados Unidos a Hong Kong," (14 de marzo de 2025) https://www. justice.gov/opa/pr/chinese-national-sentenced-smuggling-turtles-united-states-hong-kong.

200 Por el contrario, la definición del término "delito ambiental" varía según la jurisdicción.

201 A nivel mundial, el crimen relacionado con la naturaleza también tiene un impacto negativo significativo en las comunidades locales que de otro modo podrían beneficiarse del turismo o del comercio legal y sostenible. En países más pequeños (como en la región de las Islas del Pacífico y en ciertos países africanos como Madagascar), la pérdida de ingresos tiene un impacto desproporcionado en la economía.

202 Tesoro, "El Tesoro apunta a operaciones pesqueras ilegales, no declaradas y no reguladas habilitadas por cárteles," (6 de noviembre de 2024) https://home. treasury.gov/news/press-releases/jy2729.

203 DOJ, "Tres acusados por elaborado esquema transnacional de contrabando de oro y blanqueo de dinero de 24 millones de dólares," (13 de junio de 2025) https://www.justice.gov/usao-sdfl/pr/three-indicted-24-million-transnational-gold-smuggling-and-money-laundering-scheme. 204 Tesorería, "Tesorería ataca la red de corrupción en Guyana," (11 de junio de 2024)https://home.treasury.gov/news/press-releases/jy2401; DOJ, "Excandidato presidencial guyanés y empresario acusado de evasión fiscal y blanqueo de dinero de 50 millones de dólares," (28 de noviembre de 2025) evasión fiscal de https://www.justice.gov/usao-sdfl/pr/former-guyanese-presidential-candidate-and-businessman-charged-50 millones.

Una vulnerabilidad al blanqueo de dinero es algo que facilita o crea la oportunidad de blanquear dinero. Las vulnerabilidades pueden estar relacionadas con un sector financiero o producto específico, o una debilidad en la regulación, supervisión o aplicación. También pueden reflejar circunstancias únicas en las que puede ser difícil distinguir entre actividades legales e ilegales. Los métodos que permiten blanquear la mayor cantidad de dinero rápidamente o con poco riesgo de ser detectados presentan las mayores vulnerabilidades potenciales. Esta evaluación examina principalmente el riesgo residual de un sector o servicio concreto, teniendo en cuenta cualquier riesgo inherente restante tras tener en cuenta el efecto de medidas mitigadoras como la regulación, supervisión y aplicación, entre otros factores.

Las instituciones financieras y otras entidades están sujetas a distintos grados de requisitos AML/CFT dependiendo del riesgo inherente de sus operaciones. Existen requisitos más adaptados para ciertos tipos de transacciones financieras y entidades más vulnerables al abuso de blanqueo de capitales, como ciertas transacciones en efectivo, transferencias de bienes raíces residenciales no financiadas y empresas extranjeras que no son transparentes respecto a sus titulares reales. La mayoría de las instituciones financieras estadounidenses cumplen sus requisitos legales y regulatorios para prevenir, detectar e informar sobre posibles delitos de blanqueo de capitales, evasión de sanciones y otros delitos financieros. La pequeña minoría de entidades reguladas que no cumplen sus requisitos, ya sea por negligencia o por complicidad, están sujetas a sanciones disuasorias.

Los actores ilícitos siempre existirán y encontrarán formas de penetrar incluso en los sectores y productos financieros más regulados. A medida que los actores ilícitos modifican y modifican sus tácticas y técnicas, las autoridades estadounidenses responden y adaptan las estrategias policiales y las políticas regulatorias para responsabilizar a los actores ilícitos. Contrarrestar las finanzas ilícitas debería permitir, en última instancia, que los negocios legítimos prosperen. Las políticas, regulaciones e investigaciones deben estar equilibradas y no imponer costes desproporcionados a las personas y empresas estadounidenses con beneficios mínimos o marginales para las fuerzas del orden estadounidenses.

VIII. Instituciones financieras y entidades relacionadas

Bancos

Los bancos son la columna vertebral del sistema financiero estadounidense y un componente fundamental del sistema financiero global.[205] A diciembre de 2025, los bancos comerciales y cooperativas de crédito estadounidenses poseían aproximadamente 27 billones de dólares en activos totales.[206] El sector bancario no es monolítico; los diez bancos más grandes de EE. UU. representan aproximadamente la mitad del total de activos bancarios comerciales, y aproximadamente el 60 por ciento de los 3.800 bancos comerciales en Estados Unidos tienen 500 millones de dólares o menos en activos totales. [207]

La supervisión de todas las partes del sector bancario es madura y sólida, ya que la BSA tiene más de medio siglo de antigüedad.Las distintas agencias supervisoras coordinan eficazmente tanto a nivel estatal como federal, y la mayoría de los bancos cuentan con programas robustos de AML/CFT que prevenen, identifican y contrarrestan con éxito actividades ilícitas.

Los bancos siguen siendo un vector clave por el que los delincuentes buscan mover fondos, dado el enorme volumen de actividad financiera en el sector bancario. Los bancos estadounidenses se enfrentan a una amplia gama de riesgos de blanqueo de capitales que están influenciados por su base de clientes, productos y servicios financieros ofrecidos, canales de distribución y huella geográfica, entre otros factores. La mayoría de estos riesgos se mitigan con vigilancia y sólidos programas AML/CFT, ya que solo el uno por ciento de los bancos está sujeto a acciones de aplicación AML/CFT anualmente. Estas acciones de aplicación contundentes y públicas sirven tanto para disuadir comportamientos similares como para educar al sector bancario sobre cómo mitigar riesgos.

Los 205 bancos incluyen bancos comerciales, privados, cajas de ahorro, bancos industriales, asociaciones de ahorro y préstamo, cooperativas de crédito y otros tipos de entidades. Véase 31 CFR 1010.100(d).

206 FRB, "Activos y pasivos de bancos comerciales en Estados Unidos – H.8," (31 de diciembre de 2025) https://www.federalreserve.gov/releases/h8/current/default.htm; Administración Nacional de Cooperativas de Crédito (NCUA), "NCUA publica datos de rendimiento del sistema de cooperativas de crédito del tercer trimestre de 2025," (5 de diciembre de 2025) https://ncua.gov/newsroom/press-release/2025/ncua-releases-third-quarter-2025- datos de rendimiento del sistema de cooperativas de crédito.

207 Federal Deposit Insurance Corporation (FDIC), "Resumen de depósitos— Tablas resumidas, totales nacionales por tamaño de activo" (actualizado 30 de junio de 2025) https://banks.data.fdic.gov/bankfind-suite/SOD/summaryTables.

Aunque poco frecuentes, las acciones de cumplimiento pueden revelar importantes tendencias financieras ilícitas. Desde el 1 de enero de 2024, las agencias reguladoras federales de instituciones financieras han emitido 33 órdenes de cese y desistimiento o consentimiento, han realizado siete acuerdos formales e impuesto cinco sanciones civiles por un total de más de 2.000 millones de dólares contra cinco bancos por deficiencias en el cumplimiento de AML/CFT. [208]

Muchas de estas deficiencias están relacionadas con las amenazas descritas en esta evaluación, especialmente grupos criminales que buscan hacer un mal uso de los bancos para depositar dinero al por mayor y facilitar complejos esquemas de blanqueo de capitales. Aunque estos grupos a veces pueden aprovechar los servicios financieros para perpetuar actividades ilícitas, los bancos suelen identificar tipologías de TCO (por ejemplo, depósitos en efectivo a granel) mediante sistemas efectivos de monitorización de transacciones y la presentación de informes de actividad sospechosa/informes de transacciones de divisas (SAR/CTR), ya que estos se citan con menos frecuencia como parte de las acciones correctivas de los bancos en acciones de aplicación pública. Los programas de cumplimiento de sanciones OFAC de los bancos también suelen ser hábiles para identificar violaciones de sanciones económicas, ya que menos de un tercio de las acciones de cumplimiento durante este periodo de informe requirieron acciones correctivas relacionadas con los programas de sanciones OFAC.

Aunque la mayoría de los bancos establecen programas AML/CFT basados en el riesgo adecuados, una revisión de las acciones recientes de aplicación relacionadas con la AML/CFT muestra que las acciones correctivas suelen incluir ordenar a los bancos que realicen mejoras significativas en la identificación y comprensión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo que representan los actores ilícitos. El componente más común del programa AML/CFT de un banco citado en las acciones de cumplimiento fueron deficiencias en los controles internos (es decir, políticas, procedimientos y procesos insuficientes para gestionar riesgos), deficiencias relacionadas con el Oficial de la BSA y programas insuficientes de diligencia debida del cliente (CDD). Aunque los bancos llevan tiempo estableciendo programas CDD, incluso antes de que entraran en vigor los requisitos formales de la Regla CDD en mayo de 2018, los bancos reconocen que los cambios en el comportamiento de los clientes y la dinámica del mercado requieren una vigilancia constante y adaptaciones de estos programas.

Mientras los bancos deben adaptar continuamente sus programas para mantenerse al día con los nuevos riesgos, la actual Administración sigue centrada en calibrar mejor el equilibrio entre la carga y los resultados. Existen esfuerzos en curso para modernizar el régimen de la BSA AML/CFT en Estados Unidos para que sea eficaz, basado en riesgos y centrado en las mayores amenazas para las instituciones financieras y la seguridad nacional. Las cargas excesivas de cumplimiento que no se basan en el riesgo pueden resultar en gastos de recursos que no son proporcionales al efecto pretendido de proteger a las instituciones financieras de esquemas de financiación ilícita.

Los bancos se enfrentan a la presión para incorporar nuevos clientes rápidamente y así competir con otros proveedores emergentes de servicios financieros. En línea con la tendencia más amplia de consolidación del sector, las fusiones y adquisiciones bancarias también pueden llevar a algunos bancos a adquirir nuevos clientes. Como estos clientes habrían sido evaluados e integrados mediante diferentes procedimientos, el banco adquirente podría enfrentar dificultades para comprender y mitigar los riesgos de estos clientes. Otras deficiencias comunes incluyen no evaluar adecuadamente los riesgos de nuevos productos y servicios y adoptar nuevas soluciones AML/CFT mediante relaciones con terceros con proveedores de servicios que introducen vulnerabilidades que pueden ser explotadas por actores ilícitos.

Estudios de caso:

Oficina del Contralor de la Moneda (OCC) y la Junta de la Reserva Federal (FRB) emprendieron acciones penales y regulatorias paralelas contra TD Bank y anunciaron sanciones por un total aproximado de 3.100 millones de dólares. [209]

208 Tres bancos recibieron tanto una orden de cese y desistimiento como una multa económica civil durante el periodo de avaluación.

209 DOJ, "TD Bank se declara culpable de violaciones de la Ley de Secreto Bancario y de Conspiración de Blanqueo de Dinero en la Resolución de 1.800 millones de dólares," (10 de octubre de 2024) https:// www.justice.gov/archives/opa/pr/td-bank-pleads-guilty-bank-secrecy-act-and-money-laundering-conspiracy-violations-18b; FinCEN, "FinCEN evalúa una multa récord de 1.300 millones de dólares contra TD Bank," (10 de octubre de 2024) https://www.fincen.gov/news/news-releases/fincen-assesses-record- 13.000 millones de penalización contra el banco td; OCC, "OCC emite una orden de cese y desistimiento, evalúa una multa civil de 450 millones de dólares e impone restricciones de crecimiento a TD Bank, N.A. por deficiencias en BSA/AML," (10 de octubre de 2024) https://www.occ.treas.gov/news-issuances/news-releases/2024/ nr-occ-2024-116.html; FRB, "La Junta de la Reserva Federal multa con 123,5 millones de dólares al Banco Toronto-Dominion por infracciones relacionadas con las leyes contra el blanqueo de dinero," (10 de octubre de 2024) https://www.federalreserve.gov/newsevents/pressreleases/enforcement20241010a.htm.

Silvergate Bank: Desde aproximadamente 2014 hasta marzo de 2023, Silvergate se centró en proporcionar servicios bancarios y financieros a empresas extranjeras y nacionales dedicadas, entre otras cosas, a la compra y venta de activos digitales. En 2017, para facilitar transferencias bancarias internas en dólares estadounidenses entre clientes de Silvergate que compran y venden activos digitales, Silvergate lanzó la Red de Intercambio Silvergate (SEN), una plataforma interna de pagos que permitía a los clientes de Silvergate que participaban en la SEN realizar y recibir, casi en tiempo real, transferencias internas de dólares estadounidenses hacia y desde otros clientes bancarios que participaban en la SEN. Una investigación del FRB identificó deficiencias en la supervisión de las transacciones internas de Silvergate a través de la SEN. Silvergate anunció que se autoliquidaría en marzo de 2023. Posteriormente, en mayo de 2023, el FRB y el Departamento de Protección Financiera e Innovación (DFPI) de California emitieron una orden de cese y desistimiento para facilitar la autoliquidación voluntaria que Silvergate había anunciado. El FRB multó por separado a Silvergate con 43 millones de dólares por incumplimiento de las leyes AML. Silvergate completó su plan de liquidación y liquidación en julio de 2024, ha devuelto todos los depósitos a sus clientes y ya no funciona como banco. [210]

En los últimos años, los bancos se han asociado cada vez más con terceros, incluidas empresas de tecnología financiera (fintech), para ofrecer productos y servicios ampliados. A menudo denominado banca como servicio (BaaS), un banco suele integrar su infraestructura y servicios en las plataformas de fintechs u otras empresas. Aunque el BaaS puede aportar beneficios a los bancos (por ejemplo, nuevos ingresos por comisiones, acceso a datos) y a las fintechs (por ejemplo, entrada rápida y con poco capital en mercados y acceso a infraestructuras bancarias), existen varios riesgos asociados a estos acuerdos. Por ejemplo, las relaciones de terceros en capas pueden difuminar la responsabilidad de la supervisión AML/CFT y crear desafíos de atribución cuando ocurren fallos. Además, la rápida iteración de productos y el crecimiento impulsado por el capital de riesgo de las fintechs pueden impulsar el volumen más allá de la capacidad de personal y controles de cumplimiento.

En junio de 2023, la FRB, la Corporación Federal de Seguros de Depósitos (FDIC) y la OCC emitieron directrices para los bancos supervisados sobre los riesgos de las relaciones con terceros. La guía señalaba que el uso de terceros por parte de un banco no disminuye su responsabilidad de cumplir con sus requisitos regulatorios, y que el uso de terceros puede reducir el control directo del banco sobre sus actividades y puede introducir nuevos riesgos o aumentar los existentes.[211] En julio de 2024, el FRB, la FDIC y la OCC emitieron una declaración conjunta sobre los acuerdos de los bancos con terceros para ofrecer productos y servicios de depósito bancario, reafirmando las directrices existentes.[212] En junio de 2025, la OCC volvió a debatir en su Perspectiva de Riesgo semestral que las fintechs pueden no contar siempre con la experiencia, conocimientos técnicos y recursos adecuados, lo que podría socavar la capacidad para gestionar eficazmente estos riesgos asociados. [213]

Empresas de Servicios Monetarios (MSB)

Los MSB son instituciones financieras no bancarias que incluyen: (1) intermediarios o intercambiadores de divisas; (2) cobradores de cheques; (3) emisores de cheques de viajero o giros postales, o valor almacenado; (4) vendedores o canjeadores de cheques de viaje o dinero

210 FRB, "La Junta de la Reserva Federal multa a Silvergate Capital Corporation y Silvergate Bank con 43 millones de dólares por deficiencias en el monitoreo de transacciones de Silvergate en cumplimiento de la ley contra el blanqueo de capitales," (1 de julio de 2024) https://www.federalreserve.gov/newsevents/ pressreleases/enforcement20240701a.htm; DFPI, "Silvergate pagará 63 millones de dólares en sanciones combinadas tras investigaciones coordinadas por DFPI, socios federales," (1 de julio de 2024) https://dfpi.ca.gov/press_release/silvergate-to-pay-63-million-in-combined- sanciones tras investigaciones coordinadas por DFPI-socios federales/.

211 "Guía Interinstitucional sobre Relaciones con Terceros: Gestión de Riesgos," (9 de junio de 2023), https://www.federalregister.gov/documentos/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management.

212 FRB, FDIC y OCC, "Estado conjunto sobre los acuerdos de los bancos con terceros para entregar productos y servicios de depósito bancario," (25 de julio de 2024) https://www.occ.treas.gov/news-issuances/news-releases/2024/nr-ia-2024-85a.pdf.

213 OCC, "Perspectiva de riesgo semestral – Primavera 2025," (junio 2025) https://www.occ.treas.gov/publications-and-resources/publications/perspective/archives/pub-semiannual-risk-perspective-spring-2025.pdf de riesgo semestral. En noviembre de 2025, la OCC publicó una solicitud para

información (RFI) sobre la interacción de los bancos comunitarios con sus proveedores principales de servicios y otros proveedores de servicios externos esenciales. La RFI solicita comentarios sobre los principales desafíos y barreras que enfrentan los bancos comunitarios para relacionarse con sus proveedores de servicios principales y otros proveedores externos esenciales. La RFI se centra en garantizar que los bancos comunitarios puedan seguir siendo competitivos en un mercado en rápida evolución.

órdenes, o valor almacenado; (5) transmisores de dinero; y (6) el Servicio Postal de los Estados Unidos.[214] A fecha de 15 de diciembre de 2025, hay 29.514 MSB principales registrados en FinCEN conforme a las regulaciones de la BSA.[215] Hay más de 200.000 agentes MSB, que puede que no estén obligados a registrarse en FinCEN, pero sí están sujetos a los requisitos de licencias y supervisión de las autoridades bancarias estatales, incluyendo los requisitos AML/CFT. En general, los MSB, incluidos los agentes y sus principales, están obligados a desarrollar e implementar un programa AML/CFT, registrar CTRs y SARs, y mantener registros de ciertas otras transacciones y intercambios de divisas. [216]

Al igual que los bancos, las MSB se enfrentan a una variedad de riesgos de blanqueo de capitales influenciados por su base de usuarios, los servicios ofrecidos y su huella geográfica, entre otros factores. Los MSB emplean un modelo de negocio basado en transacciones, con riesgos derivados de transferencias transfronterizas, prevalencia de efectivo y requisitos de identificación de clientes más flexibles en comparación con otros tipos de instituciones financieras. Dado el gran número de MSB principales y agentes en todo Estados Unidos, los actores ilícitos también pueden repartir transacciones de blanqueo de capitales entre varios proveedores, estructurar actividades de efectivo por debajo de ciertos umbrales de notificación de la BSA y registrarse para servicios usando identidades falsas o robadas, dificultando que las fuerzas del orden rastreen los flujos financieros ilícitos. Durante el periodo de evaluación, Estados Unidos encontró que los MSB fueron explotados por actores ilícitos en relación con varios delitos subyacentes, incluyendo fraude interno,[217] fraude transnacional y sextorsión,[218] tráfico de drogas,[219] y contrabando de armas,220 , así como esquemas de financiación del terrorismo y proliferación. [221]

Los actores ilícitos también pueden explotar a MSB cómplices que descuidan deliberadamente las obligaciones AML/CFT, la mayoría de las veces al no presentar SAR y CTRs, estructurar transacciones o permitir el uso de identidades falsas.[222] Varios casos recientes han demostrado cómo los TCO con base en el extranjero utilizan MSBs cómplices para blanquear los ingresos del tráfico ilícito de drogas a México. En un caso, el propietario y operador de una MSB con ubicaciones en Oregón y Washington se declaró culpable de conspiración para blanquear los beneficios del tráfico de drogas. Según documentos judiciales, las tiendas de la mujer enviaron más de 4,2 millones de dólares en transferencias bancarias a lugares en México. La mujer y otros cómplices también aceptaron 49.500 dólares en efectivo representados como ingresos de drogas y blanquearon los fondos a través de sus tiendas. La mujer cobraba una comisión del diez por ciento para ayudar a blanquear el dinero. Admitió que al transferir estos fondos, utilizó información falsa del remitente, estructuró las transferencias en cantidades menores y utilizó diferentes tiendas que poseía para ayudar a ocultar

214 FinCEN, "Definición de negocio de servicios monetarios," (consultado el 15 de diciembre de 2025) https://www.fincen.gov/money-services-business- definición.

215 31 CFR 1022.380(a)-(f); FinCEN, "Búsqueda de Registrantes MSB," (actualizado el 15 de diciembre de 2025) https://www.fincen.gov/resources/msb-state- selector.

216 Véase en general 31 CFR Parte 1022. Muchos proveedores de servicios de activos digitales son MSB. Véase FinCEN, "Aplicación de las regulaciones de FinCEN a personas que administran, intercambian o utilizan monedas virtuales," (18 de marzo de 2013) https://www.fincen.gov/resources/statutes- regulaciones/orientación/aplicación-fincens-regulaciones-personas-administrando. Consulta la sección de Activos Digitales para una discusión sobre los riesgos de blanqueo de capitales asociados a proveedores de servicios digitales que también son MSB.

217 *Véase, por ejemplo,* DOJ, "Líder de un esquema de fraude bancario y robo de identidad de 1,4 millones de dólares se declara culpable de victimizar a clientes bancarios en todo el país," (4 de marzo de 2025) https://www.justice.gov/usao-wdwa/pr/leader-14-million-bank-fraud-and-identity-theft-scheme-pleads-guilty-victimizante-banco.

218 *Véase, por ejemplo,* DOJ, "Tres residentes de Nueva York condenados por fraude y blanqueo de capitales utilizando fondos de víctimas de estafas de lotería mayores," (18 de noviembre de 2024) https://www.justice.gov/usao-mdpa/pr/three-new-york-residents-sentenced-fraud-and-money-laundering-using- fondos a ancianos.

219 *Véase, por ejemplo,* DOJ, "Local man & woman se declara culpable de delitos de blanqueo de dinero y drogas," (2 de abril de 2025) https://www.justice.gov/usao-sdoh/ pr/local-man-woman-plead-guilty-drug-money-money-laundering-crimes; DOJ, "Hombre de California condenado por distribución de drogas, blanqueo de dinero y esquema de tráfico de personas," (7 de junio de 2024) https://www.justice.gov/usao-wdwa/pr/california-man-sentenced-drug-esquema de distribución, blanqueo de dinero y tráfico de personas.

220 *Ver, por ejemplo,* DOJ, "'Rey' de la banda violenta haitiana se declara culpable de contrabando de armas y blanqueo de dinero tras el caso del gobierno," (31 de enero de 2024) https://www.justice.gov/usao-dc/pr/king-violent-haitian-gang-pleads-guilty-gun-smuggling-and-money-laundering- después.

221 Véase Evaluación Nacional de Riesgos de Financiación del Terrorismo (NTFRA) 2026 y Evaluación Nacional de Riesgos de Financiación de Proliferación (NPFRA). 222 *Véase, por ejemplo,* el DOJ, "Empresa que transmite dinero se declara culpable de no informar de transacciones; Acepta renunciar a $700,000," (26 de junio de 2024) https://www.justice.gov/usao-sdca/pr/money-transmitting-business-pleads-guilty-failing-report-transactions-agrees-forfeit; DOJ, "El propietario

de Nueva Jersey de Check Casher and Money Service (sic) Empresa admite haber presentado más de 325 millones de dólares en informes falsos de transacciones de divisas, operar, ayudar y encubrir un negocio de transmisión de dinero sin licencia," (16 de octubre de 2024) https://www. justice.gov/usao-nj/pr/new-jersey-owner-check-casher-and-money-serivce-business-admits-filing-more-325-million.

La droga avanza.[223] Métodos similares se utilizaron en dos casos separados relacionados con CJNG y LNFM presentados en Atlanta, Georgia, en abril de 2025. [224]

En diciembre de 2025, FinCEN anunció una operación de varios niveles dirigida a más de 100 MSB estadounidenses que operan a lo largo de la frontera suroeste para examinar estos MSB en busca de posibles incumplimientos con las normativas diseñadas para detectar el blanqueo de capitales y combatir la financiación ilícita. La operación de FinCEN resultó en la emisión de seis avisos de investigación, decenas de derivaciones de examen a la división de Pequeñas Empresas/Autónomos (SBSE) del IRS y más de 50 cartas de divulgación de cumplimiento. Esta operación basada en datos se basa, entre otras cosas, en una revisión de más de un millón de CTRs y87.000 SAR.

Otra tipología, destacada por primera vez en la NMLRA de 2024, consiste en MSBs cómplices que cobran cheques para empresas constructoras pantalla para facilitar pagos en secreto a trabajadores de la construcción que a menudo no están legalmente autorizados para trabajar en Estados Unidos sin que se retengan impuestos ni se reporten al IRS. En un caso, según documentos judiciales y testimonios en el juicio, las empresas constructoras notificaban al presidente de una empresa de cambio de cheques cuando planeaban llevar los cheques a uno de sus puntos de cobro para asegurarse de tener suficiente efectivo disponible para completar la transacción. Se cobraban diariamente cientos de miles de dólares en cheques de nómina, y el hombre era consciente de que al menos uno de sus cómplices usaba un nombre y número de la Seguridad Social falsos. Actuando como oficial de cumplimiento, el hombre permitió que se presentaran cientos de informes regulatorios falsos sabiendo que contenían la identidad falsa. Durante su conspiración, el hombre y sus cómplices impidieron que el IRS cobrara más de 44 millones de dólares en impuestos sobre nóminas y renta adeudados sobre los salarios en efectivo. [225]

MSB no registrados

No registrar un MSB, a nivel federal o estatal, no es simplemente una omisión administrativa. Las entidades que operan como MSB no registradas suponen un riesgo desproporcionado dentro del sector MSB porque es poco probable que cumplan otros requisitos de la BSA, como desarrollar e implementar un programa AML/CFT o presentar CTRs y SARs. En febrero de 2025, FinCEN impuso una multa civil de 37 millones de dólares contra Brink's Global Services USA, Inc. (Brink's) por violaciones intencionadas de la BSA. Como resultado de los fracasos de Brink, cientos de millones de dólares en envíos de moneda al por mayor se transmitieron a través de la frontera suroeste en nombre de entidades de alto riesgo, incluyendo un cambista mexicano que posteriormente se declaró culpable de violar la BSA.[226] Como parte de un acuerdo de no procesamiento con el DOJ, Brink's también admitió que transportó dinero ilegalmente tanto a nivel nacional como internacional entre terceros y fuera de las limitadas protecciones regulatorias para los transportistas de divisas. Durante esta conducta ilegal, Brink's no implementó controles de cumplimiento para garantizar que sus actividades comerciales se mantuvieran dentro del puerto seguro regulatorio proporcionado a la industria de vehículos blindados. [227]

Los MSB no registrados también pueden incluir a personas que operan como parte de IVTS, o banca subtera, así como a personas que hacen un uso indebido de sus cuentas bancarias personales o empresariales para ofrecer transmisión de dinero de forma independiente

223 DOJ, "Propietario de negocio de servicios monetarios que reside ilegalmente en Estados Unidos se declara culpable de conspiración para blanquear ingresos de drogas," (24 de octubre de 2025) https://www.justice.gov/usao-or/pr/owner-money-service-business-unlawfully-residing-united-states- se declara culpable-conspiración.

224 DOJ, "Líderes de La Nueva Familia Michoacana y blanqueador de dinero con sede en Atlanta acusados," (15 de abril de 2025) https://www.justice.gov/ opa/pr/leaders-la-nueva-familia-michoacana-y-atlanta-bottom-launderer-inculpados; DOJ, "Miembros de una enorme red internacional de tráfico de drogas y blanqueo de dinero acusados en Atlanta," (15 de abril de 2025) https://www.justice.gov/usao-ndga/pr/members una red masiva internacional de tráfico de drogas y blanqueo de dinero acusados.

225 DOJ, "Oregon Check Casher condenado a prisión federal por un esquema de impuesto sobre la nómina que involucra 177 millones de dólares," (4 de febrero de 2025) https://www. justice.gov/usao-or/pr/oregon-check-casher-sentenced-federal-prison-payroll-tax-scheme-involving-177-million.

226 FinCEN, "FinCEN anuncia una multa civil de 37.000.000 de dólares contra Brink's Global Services USA, Inc. por violaciones de la Ley de Secreto Bancario," (6 de febrero de 2025) https://www.fincen.gov/news/news-releases/fincen-announces-37000000-civil-money-penalty-against-brinks- global-services-usa.

227 DOJ, "Brink's pierde 50 millones de dólares por no registrarse como negocio de transmisión de dinero," (6 de febrero de 2025) https://www.justice.gov/ usao-sdca/pr/brinks-forwits-50-million-failing-register-money-transmitting-business.

servicios.[228] En un caso, un ciudadano iraquí residente en Estados Unidos fue condenado a 54 meses de prisión tras su condena por remisión de dinero sin licencia. En la audiencia, el tribunal escuchó cómo el hombre prestó servicios económicos a organizaciones criminales por decenas de miles de dólares. Durante el juicio, el jurado escuchó pruebas sobre el negocio de transmisión de dinero del hombre, que gestionaba en su domicilio. Desde 2020, ha transferido y transferido millones de dólares de cuentas bancarias estadounidenses a cuentas de todo el mundo, incluyendo China, Indonesia e India. [229]

Corredores de bolsa y asesores de inversión

Los corredores de bolsa y asesores de inversión son dos tipos diferentes de firmas de valores, que ayudan a los clientes a hacer crecer y gestionar sus activos ofreciendo una amplia variedad de servicios que van desde transacciones puntuales hasta gestión patrimonial a largo plazo. Estas entidades tienen obligaciones variables en materia de AML/CFT y exposición a riesgos de blanqueo de capitales.

Corredores de bolsa

Los corredores de bolsa compran o venden valores ya sea para su propia cuenta o en nombre de clientes y, en general, gestionan menores volúmenes de transacciones en efectivo que los bancos. Según la Comisión de Bolsa y Valores (SEC), en 2024 había aproximadamente 3.300 corredores de bolsa con activos totales de aproximadamente 6,4 billones de dólares. [230]

Los activos dentro del sector de corredores y intermediarios están muy concentrados. La mayoría de los corredores de bolsa (67 por ciento) tienen menos de 5 millones de dólares en activos, y alrededor del dos por ciento del total de corredores representa el 94 por ciento del total de activos. Aunque el número de corredores ha disminuido en los últimos 15 años, sus activos han crecido en 1,7 billones de dólares, señal de consolidación del sector. [231]

Dadas las grandes sumas de fondos y otros activos que podrían mover a través de cuentas de clientes, los corredores de bolsa están expuestos a clientes que buscan disfrazar ingresos ilícitos en operaciones legítimas o participar en actividades fraudulentas (por ejemplo, esquemas de pump-and-dump que involucran valores de bajo precio). Los clientes con base en jurisdicciones de alto riesgo imponen otros riesgos relacionados con la AML/CFT a los corredores de bolsa, como los asociados a su fuente de riqueza o a las contrapartes con las que pueden operar. Los corredores de bolsa tienen obligaciones integrales y de larga trayectoria en la BSA. Están sujetos a la supervisión de múltiples reguladores federales y estatales, incluida la SEC, además de organizaciones autorreguladoras (SRO), como la Autoridad Reguladora de la Industria Financiera (FINRA).

Las prioridades de examen de la SEC para el año fiscal 2026 señalan que la División de Exámenes seguirá centrada en los programas AML y revisará si los corredores de bolsa y ciertas sociedades de inversión registradas (RIC), incluidos los fondos de inversión[232], están: 1) adaptando y actualizando adecuadamente su programa AML a su modelo de negocio y a los riesgos asociados de blanqueo de capitales, incluyendo la contabilización de riesgos asociados a cuentas ómnibus mantenidas para instituciones financieras extranjeras; 2) realizar adecuadamente pruebas independientes; 3) establecer un programa adecuado de identificación de clientes, incluyendo para los beneficiarios beneficiarios de los clientes de la entidad jurídica; y 4) cumplir con sus obligaciones de presentación de búsqueda y rescate. Los exámenes de ciertos RIC también revisarán políticas y procedimientos para la supervisión de los intermediarios financieros aplicables. Por último, los exámenes revisarán si los broker-dealers, asesores y RIC están monitorizando

228 *véase, por ejemplo,* el Departamento de Justicia, "Dos hombres responsables de gestionar el esquema Hawala que implica más de 65 millones de dólares condenados a tres años de prisión," (23 de abril de 2025) https://www.justice.gov/usao-sdny/pr/two-men-responsible-running-hawala-scheme-involving-more-65-million - condenados a tres; DOJ, "Cuatro nacionales hondureños acusados en Florida por un esquema de nómina no oficial de larga duración," (6 de mayo de 2025) https://www.justice.gov/opa/pr/four-honduran-nationals-indicted-florida-years-long-books-payroll-scheme; DOJ, "Negocios de Brooklyn Propietario condenado a 15 años de prisión por cobro ilegal de cheques de 55 millones de dólares, fraude bancario y esquema de evasión fiscal," (19 de noviembre de 2025) https://www.justice.gov/usao-edny/pr/brooklyn-business-owner-sentenced-15-years-prison-55-million-illegal-check-cashing.

229 DOJ, "Transmisor de dinero multimillonario sin licencia enviado a prisión," (16 de octubre de 2025) https://www.justice.gov/usao-sdtx/pr/transmisor de dinero multimillonario sin licencia enviado a prisión.

230 SEC, "SEC publica datos sobre corredores de bolsa, fusiones y adquisiciones, y empresas de desarrollo de negocio," (26 de junio de 2025) https://

www.sec.gov/newsroom/press-releases/2025-96-sec-publishes-data-broker-dealers-mergers-acquisitions-business-development- empresas.

231 Diana Knyazeva y Daniel Bresler, "Actividad de corredores de bolsa en Estados Unidos," (junio de 2025), p. 4, https://www.sec.gov/files/dera-broker-dealer-activity-2506.pdf.

232 Según la normativa FinCEN, los "fondos de inversión" (según la definición de 31 CFR 1010.100(gg)) son "instituciones financieras" y, en consecuencia, están sujetas a varias obligaciones bajo la BSA/AML, incluyendo el establecimiento de un programa de cumplimiento AML, la creación de un programa de identificación de clientes y la supervisión, detección y presentación de informes de actividad sospechosa.

Las sanciones de la OFAC y el cumplimiento de dichas sanciones. [233]

Durante el periodo de evaluación, la SEC tomó 12 acciones de cumplimiento contra corredores de bolsa en relación con incumplimientos relacionados con obligaciones AML/CFT, mientras que FINRA llevó a cabo 34 acciones de ejecución. Por ejemplo, en diciembre de 2024, la SEC llegó a un acuerdo de cargos contra SogoTrade, Inc., un corredor de bolsa registrado, por no presentar las SAR, y contra el antiguo responsable de cumplimiento de AML de SogoTrade, por ayudar y encubrir intencionadamente y causar las violaciones de SogoTrade. La SEC constató que en numerosas ocasiones, el Oficial de Cumplimiento de AML no investigó actividades sospechosas ni presentó informes de SAR relacionados con actividades sospechosas que los sistemas o personal de SogoTrade, o empleados de la firma de compensación de SogoTrade, le informaron. Según la orden de la SEC, también tenía la costumbre de alertar a los clientes de que los informes de vigilancia de SogoTrade habían identificado su actividad de trading sospechosa y aconsejaba o dirigía a los empleados a aconsejar a los clientes que mantuvieran sus actividades por debajo del umbral medio diario de volumen para evitar provocar una revisión de la empresa. [234]

Además, en julio de 2025, Interactive Brokers LLC, una empresa global de corredores electrónicos con sede en Greenwich, Connecticut, que ofrece servicios de corretaje e inversión a millones de clientes en todo el mundo a través de su plataforma de corretaje online, acordó pagar a OFAC casi 12 millones de dólares para resolver su posible responsabilidad civil por aparentes violaciones de múltiples programas de sanciones OFAC. [235]

Asesores de inversiones

Los asesores de inversiones (IA) ofrecen una variedad de servicios financieros relacionados con la gestión de activos. Entre los clientes de auditoría interna se encuentran gobiernos locales, estatales y extranjeros, inversores institucionales, inversores minoristas y personas con alto patrimonio neto. Ciertas IAs más grandes se registran en la SEC (Asesores de Inversiones Registrados, o RIAs). Ciertos IAs para fondos privados y fondos de capital riesgo están exentos de registro ante la SEC, pero aún presentan informes periódicos ante la SEC (Asesores de Reporte Exentos, o ERAs). Otros asesores de inversiones están exentos o tienen prohibido el registro ante la SEC, pero aún pueden estar obligados a registrarse en uno o más estados (IAs registrados por estados). [236]

Según se informó el 27 de abril de 2025, más de 15.900 RIA reportaban 148,5 billones de dólares en activos bajo gestión (AUM), con más de 26 billones de dólares en activos brutos agregados de fondos privados asesorados por RIA.[237] También existen cerca de 5.800 ERA, que solo pueden ofrecer asesoramiento de inversión a fondos privados, como fondos de cobertura, fondos de capital riesgo y fondos de capital privado. Según la SEC, según informó el 27 de abril de 2025, las ERAs reportaron aproximadamente 8,4 billones de dólares en activos brutos agregados de fondos privados asesorados por ERA.[238] Por último, según la Asociación de Administradores de Valores de América del Norte (NASAA), según se informó en septiembre de 2025, hay aproximadamente 16.500 IA registradas por el estado que gestionan más de 380.000 millones de dólares en activos. [239]

En febrero de 2024, el Tesoro publicó una evaluación sectorial de riesgos de la IA que identificó varias amenazas financieras ilícitas relacionadas con las IAs, incluyendo que las IA han servido como punto de entrada al mercado estadounidense para obtener beneficios ilícitos relacionados con corrupción extranjera, fraude, evasión fiscal y evasión de sanciones. La evaluación encontró que las ERAs enfrentaban los mayores riesgos financieros ilícitos en el sector de la auditoría interna, seguidas por las RIA que asesoran a fondos privados. La evaluación también destacó que las IA y sus fondos asesorados,

233 SEC, "Prioridades de examen del año fiscal 2026," (18 de noviembre de 2025) https://www.sec.gov/files/2026-exam-priorities.pdf. 234 SEC, "La SEC acusa a SogoTrade Inc. y al ex oficial de cumplimiento contra el blanqueo de capitales por no presentar informes de actividad sospechosa (SARs)," (17 de diciembre de 2024) https://www.sec.gov/enforcement-litigation/administrative-proceedings/34-101936-s.

235 OFAC, "Interactive Brokers LLC llega a un acuerdo con OFAC por 11.832.136 dólares relacionados con aparentes violaciones de múltiples regulaciones de sanciones," (15 de julio de 2025) https://ofac.treasury.gov/media/934501/download?inline.

236 Generalmente, la SEC regula los RIA que gestionan 100 millones de dólares o más en activos de clientes. Existen ciertas exenciones a esta norma que permiten el registro ante la SEC incluso si no se ha alcanzado el umbral de activos. En los casos en los que no se cumplen los requisitos de registro ante la SEC, los IA con menos de 100 millones de dólares en activos gestionados (AUM) suelen ser regulados por el regulador estatal del estado donde el asesor tiene su principal lugar de negocio. FINRA, "Asesores de Inversión", https://www.finra.org/investors/investing/working-with-investment - profesionales/asesores de inversión.

237 SEC, "Estadísticas de asesores de inversión: Datos del formulario ADV, periodo que termina diciembre de 2024," (27 de abril de 2025), p. 3, 5, https://www.sec.gov/files/ inversión/im-investment-adviser-statistics-20250430.pdf. Este total incluye activos regulatorios discrecionales y no discrecionales bajo gestión (RAUM), según se detalla en la instrucción 5.b. del Formulario ADV. Véase "FORM ADV (Versión en papel)" (consultado el 30 de diciembre de 2025), pp. 19-22, https://www.sec.gov/about/forms/formadv-instructions.pdf.

238 Ibid, p. 14. Consulta la SEC, "Asesor de Informes Exentos (ERA)" (consultado el 30 de diciembre de 2025) https://www.investor.gov/introduction-investing/ era de fundamentos de inversión/glosario/informes de exención.

239 NASAA, "Informe Anual 2025 de la Sección de Asesores de Inversiones de la NASAA" (8 de septiembre de 2025), p. 3, https://www.nasaa.org/wp-content/ subidas/2025/09/IA-Section-2025-Report-FINAL.pdf.

en particular, los fondos de capital riesgo, pueden ser utilizados por Estados extranjeros para acceder a ciertas tecnologías y servicios con implicaciones a largo plazo para la seguridad nacional mediante inversiones en empresas en fase inicial. [240]

Para abordar estos riesgos, el Tesoro finalizó una norma que impone obligaciones AML/CFT (por ejemplo, requisitos de programa, informes y registro AML/CFT) a ciertas IAs (es decir, RIAs y ERAs) (norma AML IA). El 31 de diciembre de 2025, FinCEN adoptó una norma final que retrasó la fecha de entrada en vigor de la norma AML de la IA hasta el 1 de enero de 2028.[241] Las actividades de muchas IA siguen estando sujetas a un programa AML/CFT a nivel empresarial o, de otro modo, indirectamente sujetas a dichos controles debido a sus afiliaciones o interacciones con otras instituciones financieras cubiertas (por ejemplo, bancos y corredores de bolsa).

Durante el periodo de evaluación, la SEC tomó dos medidas de aplicación relacionadas con AML contra las RIA.[242] En enero de 2015, la SEC acusó a Navy Capital Green Management, LLC (Navy Capital) de hacer tergiversaciones relacionadas con sus procedimientos AML y por incumplimientos. La orden de la SEC determinó que, desde al menos octubre de 2018 hasta enero de 2022, Navy Capital declaró en la oferta y otros documentos proporcionados a inversores potenciales y existentes de fondos privados que la firma estaba cumpliendo voluntariamente con las leyes de debida diligencia del cliente a pesar de que estas leyes no se aplicaban a las IA, incluyendo la realización de tipos específicos de due diligence sobre posibles inversores y la monitorización continua de la debida diligencia de los clientes sobre inversores existentes. Según la orden, los inversores en fondos privados de Navy Capital incluían múltiples entidades extranjeras con propiedad beneficiaria opaca y fuentes de riqueza. La orden determinó que Navy Capital no siempre realizó la debida diligencia con el cliente tal como se describe, incluyendo en lo relativo a una entidad propiedad de un individuo públicamente reportado con sospechas de conexiones con actividades de blanqueo de capitales. [243]

La OFAC también ha tomado dos medidas de cumplimiento contra los asesores de inversión durante el periodo de evaluación:

En diciembre de 2025, IPI Partners, LLC (IPI), una firma de capital privado con sede en Chicago especializada en la compra, desarrollo y operación de centros de datos, acordó pagar más de 11 millones de dólares a la OFAC para saldar su posible responsabilidad civil por aparentes violaciones de sanciones relacionadas con Ucrania y Rusia. En 2017 y 2018, IPI solicitó y recibió inversiones del oligarca ruso Suleiman Kerimov a través de una serie de estructuras legales y continuó manteniendo esas inversiones durante cuatro años tras la designación de la OFAC a Kerimov el 6 de abril de 2018. [244]

En junio de 2025, la OFAC emitió un Aviso de Sanción imponiendo una multa de 215 millones de dólares a GVA Capital Ltd., una firma de capital riesgo con sede en San Francisco, California, por violar las sanciones de la OFAC relacionadas con Ucrania y Rusia y por no cumplir con una citación de la OFAC. Entre abril de 2018 y mayo de 2021, GVA Capital gestionó conscientemente una inversión para el oligarca ruso sancionado Suleiman Kerimov, siendo consciente de su estatus bloqueado. En 2016, los responsables de GVA Capital se reunieron con Kerimov en su finca en Francia para obtener su aprobación personal para las inversiones. En abril de 2018, la OFAC sancionó a Kerimov. No obstante, GVA Capital continuó gestionando estas inversiones trabajando a través del sobrino de Kerimov, de quien GVA Capital sabía que actuaba como representante de Kerimov. [245]

240 Treasury, "Evaluación de riesgos de asesores de inversión," (febrero de 2024), https://home.treasury.gov/system/files/136/US-Sectoral-Illicit- Finance-Risk-Assessment-Investment-Advisers.pdf.

241 FinCEN, "Norma final: retrasando la fecha de vigencia del programa de prevención del blanqueo de capitales/contraataque de la financiación del terrorismo y los requisitos de presentación de informes de actividades sospechosas para asesores de inversiones registrados y asesores exentos de informe," (31 de diciembre de 2025), 91 FR 36, https://www.federalregister.gov/documents/2026/01/02/2025-24184/delaying-the-effective-date-of-the-anti-money la lucha contra la financiación del terrorismo.

242 Una de estas acciones de cumplimiento se llevó a cabo contra un corredor de bolsa y asesor de inversiones con doble registro.

243 SEC, "La SEC acusa a la consultora Navy Capital de tergiversar sus procedimientos contra el blanqueo de dinero a inversores," (14 de enero de 2025) https://www.sec.gov/newsroom/press-releases/2025-8.

244 OFAC, "IPI Partners, LLC llega a un acuerdo con OFAC por 11.485.352 dólares relacionados con aparentes violaciones de las sanciones relacionadas con Ucrania/Rusia," (2 de diciembre de 2025) https://ofac.treasury.gov/media/934786/download?inline.

245 OFAC, "OFAC impone una multa de 215.988.868 dólares a GVA Capital Ltd. por violar las sanciones y obligaciones de reporte relacionadas con Ucrania/Rusia," (12 de junio de 2025) https://ofac.treasury.gov/media/934366/download?inline

Casinos y juegos

Existen distintos niveles de riesgos asociados a los casinos y otras actividades de juego en Estados Unidos. Estos riesgos abarcan casinos tradicionales y clubes de cartas, juegos de azar no relacionados con casinos y actividades de juego (como apuestas deportivas, deportes de fantasía y competiciones de sorteos), y el mercado ilegal de juego. En estos mercados interrelacionados, el juego en Estados Unidos sigue siendo especialmente vulnerable al blanqueo de los beneficios del tráfico de drogas, el crimen organizado, actividades delictivas extranjeras y el juego ilegal y las apuestas de apuestas, entre otros delitos subyacentes. Estas actividades se ven agravadas por los marcos de licencias y normativas desiguales en los diferentes mercados de juego y por prácticas de cumplimiento deficientes. Sin embargo, como se describe más adelante, en general, los casinos y otras entidades de juego pueden estar sujetos a requisitos programáticos, de informes y de registro AML/CFT. En general, los riesgos de blanqueo de capitales asociados a estos sectores continúan creciendo y evolucionando, reflejando la trayectoria más amplia de las actividades de juego legales e ilegales a nivel nacional.

Casinos y Clubes de Cartas

Los casinos y clubes de cartas siguen siendo lugares atractivos para el blanqueo de fondos, con actores ilícitos que siguen dependiendo de métodos como el chip-walking, el juego mínimo, la estructuración, el uso de mulas de dinero y la colusión de los clientes en las apuestas para blanquear fondos. Las medidas AML/CFT y prácticas de reporte de los casinos, tal y como exige la BSA durante décadas, han tenido un efecto demostrable en la interrupción de actividades ilícitas.[246] Por el contrario, el incumplimiento de los casinos de sus obligaciones aplicables bajo la BSA crea oportunidades para que los blanqueadores de dinero procesen los ingresos ilícitos sin ser detectados.[247] Por ejemplo, en 2024, FinCEN impuso una multa económica civil de 900.000 dólares contra un club de tarjetas de California por sus controles AML/CFT deliberadamente deficientes, incluyendo controles internos inadecuados, falta de realización de pruebas independientes, falta de formación de personal y falta de detección e informe de actividades sospechosas y ciertas transacciones en divisas, entre otras debilidades. [248]

Otra deficiencia problemática de cumplimiento es la falta de aplicación por parte de la dirección del casino o de la falta de notificación de actividades sospechosas relacionadas con clientes que el casino conoce o sospecha que están inmersos en actividades delictivas. Se ha identificado que varios casinos no han realizado la debida diligencia ni presentado SARs contra casas de apuestas ilegales que frecuentan el casino. Por ejemplo, en agosto de 2024, la Junta de Control de Juegos de Nevada (NGCB) presentó una queja contra el casino Resorts World Las Vegas, alegando que el casino "daba la bienvenida a ciertas personas para apostar en su casino... mientras que los ejecutivos y empleados [de casinos] sabían, o deberían haber sabido, que ciertas personas probablemente eran casas de apuestas ilegales, que tenían condenas penales relacionadas con operaciones de juego ilegales o que tenían vínculos con el crimen organizado."[249] La NGCB alegó además que los ejecutivos del casino facilitaron "una cultura en la que la información sobre actividades sospechosas o ilegales es, como mínimo, negligentemente ignorada o, en el peor, ignorada deliberadamente para obtener beneficio económico." [250]

En línea con las conclusiones de la NMLRA de 2024, esta tendencia puede indicar que los casinos están subfinanciando o dejando de lado las funciones de cumplimiento de la BSA en favor de atraer clientes más rentables— aunque de mayor riesgo— .[251]

246 *Véase, por ejemplo,* DOJ, "Líder y blanqueador de dinero para la cuadrilla de seguimiento de drogas de KDY condenado a 160 meses en prisión federal," (17 de abril de 2025) https://www.justice.gov/usao-dc/pr/leader-and-money-launderer-kdy-drug-trafficking-crew-sentenced-160-months-federal-prisión; DOJ, "Hombre de Pensacola se declara culpable de delitos multimillonarios de tráfico de drogas y blanqueo de capitales" (27 de junio de 2025)

https://www.justice.gov/usao-ndfl/pr/pensacola-man-pleads-guilty-multi-million-dollar-drug-trafficking-and-money-laundering.

247 casinos y clubes de cartas generalmente se incluyen en la definición de institución financiera bajo la BSA, siempre que estén autorizados por el estado y tengan ingresos brutos anuales por juego (GAGR) superiores a 1 millón de dólares. En resumen, los casinos y clubes de tarjetas deben establecer programas AML/CFT, incluyendo procedimientos escritos de AML y controles internos, un oficial de cumplimiento designado, funciones independientes de pruebas y cumplir con ciertas obligaciones de informe, incluidas las obligaciones de presentación SAR (véase 31 CFR Parte 1021, Subpartes B, C y D). Aunque estas obligaciones han cambiado con el tiempo, los casinos estuvieron sujetos por primera vez a obligaciones de la BSA en 1985. El IRS examina casinos y clubes de tarjetas para comprobar el cumplimiento de estos requisitos de la BSA, delegados por FinCEN.

248 FinCEN, "FinCEN impone una multa civil de 900.000 dólares contra el Hotel y Casino Lake Elsinore por violaciones de la Ley de Secreto Bancario," (23 de octubre de 2024) https://www.fincen.gov/news/news-releases/fincen-assesses-900000-civil-money-penalty-against-lake-elsinore-hotel-and. 249 "Junta de Control de Juegos de Nevada vs. Resorts World Las Vegas, LLC," (15 de agosto de 2024) https://www.gaming.nv.gov/siteassets/content/juegos/quejas/NGC_24-04_Genting_Berhad.pdf 250 Id.

251 *Véase, por ejemplo,* NGCB, "Nevada Gaming Control Board y MGM Resorts International Entran en una Propuesta de Estipulación para Un Acuerdo Respecto a la Queja Disciplinaria," (18 de abril de 2025) https://www.gaming.nv.gov/siteassets/content/about/press-release/NGCB_News_Release_-_MGMRI_18April2025.pdf.

Relacionado con ello, existen riesgos significativos asociados a las prácticas de los casinos destinadas a facilitar el juego por parte de clientes extranjeros adinerados, mediante prácticas ilegales y no autorizadas de transmisión de dinero para ello. En septiembre de 2024, como parte de un Acuerdo de No Procesamiento, Wynn Las Vegas (WLV) admitió que utilizó ilegalmente empresas de transmisión de dinero no registradas para eludir el sistema financiero convencional. Por ejemplo, WLV contrataba regularmente agentes independientes externos que actuaban como empresas transmisoras de dinero sin licencia para reclutar jugadores extranjeros a WLV. Para que los jugadores pudieran pagar deudas a WLV o disponer de fondos para apostar en WLV, los agentes independientes transferían los fondos de los jugadores a través de empresas, cuentas bancarias y otros candidatos externos en América Latina y otros lugares, y finalmente a una cuenta bancaria controlada por WLV en California. Los fondos depositados en la cuenta controlada por WLV se transfirieron a la cuenta jaula de WLV. Los empleados de WLV, con el conocimiento de sus supervisores y trabajando con los agentes independientes, finalmente acreditaron el relato de WLV de cada usuario individual. Las transacciones complejas permitieron a los jugadores extranjeros en WLV evadir las leyes extranjeras y estadounidenses que regulan la transferencia y la presentación de información monetaria. [252]

Estas prácticas ilegales de transmisión de dinero también están estrechamente vinculadas a las CMLN, que han participado en actividades financieras ilícitas dentro o a través de casinos. Las actividades de CMLN estuvieron presentes en los esquemas de transferencia de dinero identificados en el caso previamente descrito contra el casino WLV. Además, supuestamente se han producido transferencias de efectivo y entregas por parte de CMLN en las instalaciones de casinos, como se documenta en la acusación de junio de 2024 contra un presunto CMLN que ayudó en el blanqueo de los ingresos del tráfico de drogas del Cártel de Sinaloa. [253]

Juegos y juegos de azar no relacionados con el casino

El mercado legal de juegos no relacionados con los casinos — incluyendo las apuestas deportivas, los deportes de fantasía y los casinos de sorteos— es vulnerable a muchos de los mismos métodos de blanqueo de capitales que los casinos tradicionales, así como a otras tipologías también asociadas con el fraude en internet y el ciberdelito. El juego no relacionado con casinos está sujeto a diferentes licencias y marcos regulatorios. Estas actividades a menudo no ocurren en relación con un casino cubierto por la BSA, aunque la guía de FinCEN ha indicado que ciertos negocios de juego pueden seguir regulados bajo la BSA como transmisores de dinero. [254]

En el caso de las apuestas deportivas autorizadas, hay indicios crecientes de que este sector está siendo mal utilizado con fines financieros ilícitos. El uso indebido por parte de blanqueadores de dinero de plataformas de apuestas deportivas online con licencia que utilizan información personal robada sigue siendo un riesgo importante. En abril de 2025, un hombre fue condenado a 46 meses de prisión por delitos relacionados con el blanqueo de cientos de miles de dólares de un fabricante de equipos de entrenamiento de fuerza en Columbus. El hombre utilizó el sitio de apuestas online FanDuel para conspirar para blanquear dinero. Él y otros robaban la identidad de una víctima y la usaban para crear una cuenta de FanDuel. Luego, los ingresos criminales se depositaban en la cuenta y luego se retiraban. En total, el hombre y otros utilizaron este esquema para depositar casi 572.000 dólares y retirar más de
485.000 dólares de los ingresos criminales. [255]

También existen riesgos crecientes asociados a los deportes de fantasía y las actividades de los casinos de sorteos, que generalmente están fuera del alcance de la regulación de casinos y juegos de azar en Estados Unidos. Esta falta de supervisión regulatoria aumenta el riesgo financiero ilícito. Los servicios de deportes de fantasía suelen ser ofrecidos por una amplia variedad de empresas, incluyendo muchas de las mismas plataformas que también ofrecen servicios de apuestas deportivas con licencia. Sin embargo, los deportes de fantasía se consideran "juegos de habilidad" y a menudo no están sujetos a requisitos de licencias o normativas relacionadas con el juego. No obstante, los deportes de fantasía (incluidos los deportes de fantasía diarios, o "DFS") han sido utilizados indebidamente con fines fraudulentos. Por ejemplo, en marzo de 2024, un hombre de Florida fue condenado a más de seis años de prisión por cometer fraude electrónico y participar en una transacción monetaria ilegal. Según documentos judiciales, el hombre llevó a cabo un esquema de fraude mediante el cual malversó aproximadamente 22.221.454 dólares de los Jacksonville Jaguars. Utilizó los ingresos de este proyecto, en

252 DOJ, "Wynn Las Vegas pierde 130 millones de dólares por conspiración ilegal con empresas transmisoras de dinero sin licencia," (6 de septiembre de 2024) https://www.justice.gov/usao-sdca/pr/wynn-las-vegas-forfeits-130-million-illegally-conspiring-unlicensed-money-transmitting. 253 Primera Acusación Sustitutiva, Estados Unidos contra Edgar Joel Martinez-Reyes, et al, No. 2:23-cr-545(A)-DMG (C.D. Cal. 4 de junio de 2024), p. 17,

https://www.justice.gov/archives/opa/media/1356301/dl?inline.

254 FinCEN, "Aplicación de las regulaciones de FinCEN a ciertos modelos de negocio que involucran monedas virtuales convertibles," (9 de mayo de 2019) https:// www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

255 DOJ, "Hombre de Nueva York condenado a prisión por delitos de blanqueo de capitales relacionados con casi medio millón de dólares robados a negocios locales mediante malware informático," (11 de abril de 2025) https://www.justice.gov/usao-sdoh/pr/new-york-man-sentenced-prison-money delitos relacionados con blanqueo de casi medio millón.

Total o parcialmente, para realizar apuestas en sitios de juego online.[256] Este caso ilustra el riesgo de que grandes sumas de ingresos criminales entren en el ecosistema de los deportes de fantasía, incluso si estas actividades pueden estar fuera del alcance de las actividades de juego autorizadas.

También existen riesgos asociados a los casinos de sorteos. La Asociación Americana de Juegos describe los casinos de sorteos como servicios que ofrecen juegos de casino tradicionales a los clientes de forma gratuita (normalmente online), pero que utilizan un sistema de doble moneda en el que los jugadores pueden ganar créditos o "monedas" específicos del juego que luego pueden canjear por moneda fiduciaria o activos digitales.[257] Este sistema de doble moneda permite que los sorteos no estén sujetos a muchas regulaciones de casinos o juegos de azar online. Aunque los casinos de lotería generalmente estén fuera del marco regulatorio de los casinos, siguen siendo vulnerables a muchas de las mismas metodologías de blanqueo de capitales que los casinos, y pueden ser espacios especialmente atractivos para que los delincuentes blanqueen fondos dada su falta de supervisión.

Juego ilegal

En todas las actividades de juego en Estados Unidos, los riesgos siguen siendo los más altos en el mercado de juego ilegal, que abarca casinos y salas de póker sin licencia, plataformas de juego ilegales en línea (incluidas las con sede en EE. UU. o domiciliadas en el extranjero) y otras formas.[258] Las operaciones de juego ilegal no solo generan ingresos ilícitos significativos para sus propietarios (fondos que posteriormente pueden ser blanqueados), sino que también ofrecen oportunidades para el blanqueo de capitales a gran escala por parte de los clientes de estas operaciones. Los operadores de juego ilegal generalmente no implementan medidas AML/CFT, ni medidas de verificación de identidad. Al contrario, a menudo es la falta de controles AML/CFT lo que puede atraer a delincuentes u otros jugadores de alto riesgo al mercado ilegal del juego.

Existen numerosos ejemplos recientes de operaciones de juego ilegal que se dedican a blanqueo de capitales o actividades relacionadas. En octubre de 2025, se publicó una acusación formal que acusaba a seis acusados de conspiración para fraude electrónico y conspiración para blanqueo de capitales por sus presuntos roles en un esquema para utilizar información privilegiada de jugadores y entrenadores de la National Basketball Association (NBA) para lucrarse con actividades ilegales de apuestas. Según se establece en la acusación, entre diciembre de 2022 y marzo de 2024, los acusados y sus asociados obtuvieron y utilizaron indebidamente información no pública sobre próximos partidos de la NBA para realizar apuestas deportivas fraudulentas con fines lucrativos y luego blanquearon los beneficios. [259]

Las plataformas de apuestas deportivas y juegos ilegales en línea son otra área de riesgo importante. Las plataformas de juego ilegal generan ingresos ilícitos para sus propietarios y operadores, además de ofrecer a los delincuentes la oportunidad de blanquear fondos con mayor anonimato mediante el uso indebido de sus servicios de juego y apuestas. Estas plataformas suelen estar ubicadas en jurisdicciones offshore que tienen regímenes regulatorios o de supervisión más permisivos para las actividades de juego, y las personas estadounidenses suelen apostar a través de estas plataformas utilizando redes privadas virtuales (VPN) u otras tecnologías que ocultan su ubicación en EE. UU. En un caso, diez personas se declararon culpables de gestionar una operación de apuestas deportivas multimillonaria. Según los acuerdos de culpabilidad, uno de los demandados comenzó a operar una organización de apuestas hace al menos 17 años. La organización acabó conociéndose como "Red44", y las actividades de apuestas y apuestas se realizaban en línea a través de un servidor offshore ubicado en Costa Rica. Se estima que la organización aceptó más de 2.000 millones de dólares en apuestas durante su existencia. [260]

256 DOJ, "Exempleado de los Jacksonville Jaguars condenado a más de seis años por malversación de más de 22 millones de dólares," (12 de marzo de 2024) https://www.justice.gov/usao-mdfl/pr/former-jacksonville-jaguars-employee-sentenced-more-six-years-embezzling-excess-22. 257 American Gaming Association, "Vigilancia regulatoria crítica para garantizar que los 'sorteos' no amenacen a los consumidores ni socaven la regulación del juego," (agosto de 2024) https://gamblingcompliance.vixio.com/sites/default/files/inline-files/AGA%20Sweepstakes%20 Memo%20(1).pdf. 258 Véase IC3, "Grandes probabilidades, alto riesgo: El FBI anima a los apostadores estadounidenses a conocer los riesgos del juego ilegal," (17 de diciembre de 2025) https:// www.ic3.gov/PSA/2025/PSA251217.

259 DOJ, "Jugadores actuales y anteriores de la National Basketball Association y otras cuatro personas acusadas de conspiración generalizada

de apuestas deportivas y blanqueo de capitales," (23 de octubre de 2025) https://www.justice.gov/usao-edny/pr/current-and-former-national-basketball-jugadores-asociación-y-cuatro-más-individuos.

260 DOJ, "Diez acusados se declaran culpables en un esquema multimillonario de apuestas deportivas y blanqueo de capitales," (12 de febrero de 2025) https://www.justice.gov/usao-ndal/pr/ten-defendants-plead-guilty-multi-million-dollar-sports-betting-and-money-laundering.

Insiders cómplices

Los insiders cómplices son empleados de instituciones financieras que cometen delitos financieros de forma independiente o en apoyo de otros actores ilícitos. Como se identificó por primera vez en la NMLRA de 2015, todas las organizaciones enfrentan amenazas internas, pero las apuestas son mayores para las instituciones financieras dado el volumen y valor de las transacciones en el sistema financiero estadounidense. Los cómplices internos en las instituciones financieras presentan distintos niveles de riesgo según su nivel de acceso y autoridad, así como la fortaleza de los controles internos de la institución. Los casos del periodo de evaluación muestran que los insiders cómplices siguen siendo una vulnerabilidad constante ante el fraude y el blanqueo de capitales al abrir y mantener cuentas fraudulentas, a veces a cambio de sobornos;[261] procesando transacciones fraudulentas a sabiendas;[262] y ayudar a actores ilícitos a evadir los sistemas de auditoría interna de una institución financiera que puedan detectar o interrumpir actividades sospechosas.[263] Los insiders cómplices en instituciones financieras también pueden malversar fondos ellos mismos sin intervención externa.[264] Estos riesgos existen tanto para empleados a tiempo completo como parcial, así como para contratistas. [265]

Los cómplices internos pueden ocupar cargos de cualquier nivel en una institución financiera.[266] Cuando los altos ejecutivos se ven comprometidos y no cumplen con los requisitos AML/CFT de una institución, puede conducir al fracaso institucional. En diciembre de 2025, un gran jurado federal emitió una acusación acusando al expresidente y director ejecutivo (CEO) del First National Bank of Lindsay por su implicación en una conspiración para cometer fraude bancario y otros delitos. Como se alega, el CEO obligó al banco a conceder préstamos a ciertos clientes, muchos de los cuales eran sus amigos y vecinos personales, que los prestatarios nunca devolvieron. Se alega que el CEO manipuló los registros del banco y falsificó varios informes bancarios para sobrestimar falsamente el rendimiento de los préstamos, incluso utilizando nuevos préstamos o transferencias de fondos propios para cubrir descubiertos de préstamos pendientes. La acusación alega que el CEO modificaba frecuentemente los registros bancarios para ocultar esta actividad al OCC, que era el regulador federal del banco, así como al Consejo de Administración del banco y a otros. Durante el verano de 2024, cuando la OCC realizaba una inspección in situ en el banco, el CEO supuestamente proporcionó al personal de la OCC un documento falso que ocultaba cientos de cambios que el hombre había realizado en los datos de préstamos. La acusación también alega que el CEO no implementó un programa AML en el banco como exige la BSA. Por ejemplo, el CEO supuestamente no presentó ningún SAR en su propio esquema fraudulento y aconsejó a los clientes bancarios que hicieran depósitos en efectivo por debajo de 10.000 dólares para evitar los requisitos de información relevantes. [267]

---

261 *Véase, por ejemplo,* DOJ, "TD Bank Insider se declara culpable de aceptar sobornos para abrir fraudulentamente más de 100 cuentas bancarias," (25 de junio de 2025) https://www.justice.gov/usao-nj/pr/td-bank-insider-pleads-guilty-accepting-bribes-fraudulently-open-more-100-bank-accounts.

262 *Véase, por ejemplo,* DOJ, "Dos residentes del East Bay, uno de los cuales era cajero de banco, acusados de cobrar cheques robados del Tesoro de EE.UU." (13 de febrero de 2025) https://www.justice.gov/usao-ndca/pr/two-east-bay-residents-one-whom-was-bank-teller-indicted-charges-cashing-stolenus.

263 *Véase, por ejemplo,* DOJ, "Exempleado bancario se declara culpable de su papel en conspiración internacional de blanqueo de capitales," (27 de febrero de 2025) https://www.justice.gov/usao-ma/pr/former-bank-employee-pleads-guilty-role-international-money-laundering-conspiracy.

264 *Ver, por ejemplo,* DOJ, "Exbanquero condenado por malversación" (14 de noviembre de 2025) https://www.justice.gov/usao-mdfl/pr/former- malversación sentenciada por banquero.

265 *Véase, por ejemplo,* DOJ, "Contratista bancario condenado por participación en un esquema de tarjetas de débito de 8 millones de dólares," (22 de julio de 2025) https://www.justice.gov/ usao-sdtx/pr/bank-contractor-sentenced-participation-8-million-debit-card-scheme.

266 *Véase, por ejemplo,* DOJ, "Cofundador de Paxful Inc. se declara culpable de conspiración para no mantener un programa eficaz contra el blanqueo de dinero," (8 de julio de 2024) https://www.justice.gov/archives/opa/pr/paxful-inc-co-founder-pleads-guilty-conspiracy-fail-maintain-effective-anti-money-blanqueado.

267 DOJ, "Expresidente de un banco fallido de Oklahoma acusado de fraude bancario," (4 de diciembre de 2025) https://www.justice.gov/usao-wdok/pr/ expresidente-que-quedado-banco-acusado-bancario-de-Oklahoma. Según la Oficina del Inspector General del Tesoro, la "causa principal del fracaso del Banco fue una falla crítica en los controles internos del Banco que permitió que ocurriera actividad fraudulenta que afectó a una parte sustancial de la cartera de préstamos y de los activos líquidos del Banco. Las deficiencias en la supervisión del Consejo del Banco, en los controles internos y otras prácticas inseguras o poco sólidas permitieron que uno o más empleados del Banco alteraran los registros bancarios y ocultaran debilidades en la cartera de préstamos del Banco a los examinadores. Como resultado de la identificación de discrepancias en sus libros y registros, el Banco tuvo que reconocer pérdidas que superaban el capital del Banco, lo que lo hizo insolvente." Tesorería, "Seguridad y solidez: revisión fallida de Bank Limited – First National Bank of Lindsay," (27 de marzo de 2025) https://oig.treasury.gov/system/files/2025-03/Failed-Bank-Limited-Review-Memorandum---First-National-Bank-of-Lindsay-508-Locked.pdf.

IX. Efectivo

Tras un descenso al inicio de la pandemia de COVID-19, el número de pagos en efectivo que realiza el estadounidense medio cada mes se ha mantenido estable, incluso cuando los pagos con tarjetas de crédito y débito han aumentado.El [268] Cash también sigue utilizándose con frecuencia en transacciones que involucran bienes y servicios ilícitos porque los pagos son inmediatos, de menor coste, ampliamente aceptados y relativamente anónimos, lo que permite a todas las partes involucradas evitar potencialmente el escrutinio inmediato de instituciones financieras y fuerzas de seguridad. Como resultado, las organizaciones criminales a menudo disponen de grandes cantidades de dinero que necesitan para lavar para su uso en Estados Unidos o para introducir en jurisdicciones extranjeras.

Generalmente, el primer paso para blanquear efectivo al por mayor es consolidar el dinero en un único punto dentro de una ciudad o región, dependiendo del tamaño y naturaleza de la operación criminal. Transportar dinero al por mayor es una actividad que consume mucho tiempo y que normalmente requiere una red de mensajeros para conducir o volar por Estados Unidos y recoger ingresos ilícitos en efectivo. [269]

Las organizaciones criminales entonces contratan a blanqueadores profesionales de dinero o toman medidas por sí mismas para sacar el mayor volumen del dinero fuera del país, introducir el dinero en el sistema financiero o blanquearlo a través de negocios intensivos en efectivo para adquirir bienes o mezclar el dinero ilícito con ingresos legítimos. Como se detalla en otras secciones, los delincuentes también pueden usar el efectivo para comprar bienes o bienes raíces o intercambiar el dinero por activos digitales a través de intercambiadores del mercado negro.

Contrabando de efectivo a granel

Es legal transportar cualquier cantidad de moneda u otro instrumento monetario hacia o fuera de Estados Unidos, pero si la cantidad supera los 10.000 dólares, el transportista, emisor o receptor debe presentar un Informe de Moneda o Instrumentos Monetarios (CMIR, también conocido como Formulario FinCEN 105).[270] El contrabando de efectivo a granel ocurre cuando una persona oculta a sabiendas más de 10.000 dólares en moneda u otros instrumentos monetarios para su transporte hacia o fuera de Estados Unidos con la intención de evadir un requisito de declaración de divisas, como un CMIR. Este requisito se aplica independientemente de cómo se transporte la moneda y la actividad no tiene por qué realizarse necesariamente en una frontera o puerto de entrada si se demuestra que la persona tenía la intención de cruzar la frontera. [271]

Según las fuerzas del orden, el contrabando de dinero al por mayor sigue siendo un método popular para que los TCOs trasladen los ingresos ilícitos fuera del país. El dinero puede estar oculto en vehículos privados o comerciales, en aeronaves privadas o comerciales, o en una persona física. Los mensajeros responsables del contrabando suelen estar dirigidos por blanqueadores profesionales o miembros senior de una TCO. En un caso, un ciudadano mexicano que residía ilegalmente en Arizona se declaró culpable de conspiración para blanqueo de capitales en relación con proporcionar más de 100.000 dólares en ingresos de la venta de drogas a mensajeros que introducían el dinero de contrabando en México para promover una operación de narcotráfico.[272] En otro caso, cuatro auxiliares de vuelo se declararon culpables de operar un negocio de transmisión de dinero sin licencia por aceptar dinero en efectivo de una organización de blanqueo de capitales, pasar la seguridad por el carril de Miembro Conocido de la Tripulación y pasar el dinero a

268 Federal Reserve Financial Services, "Hallazgos de 2025 del Diario de la Elección de Pago al Consumidor," (mayo de 2025), p. 4, https://www. frbservices.org/binaries/content/assets/crsocms/news/research/2025-diary-of-consumer-payment-choice.pdf.

269 *Véase, por ejemplo,* DOJ, "Dos miembros de una organización transnacional de blanqueo de capitales condenados por blanquear millones de dólares en ingresos de drogas," (11 de abril de 2025) https://www.justice.gov/opa/pr/two-members-transnational-money-laundering-organization-sentenced-blanqueo de millones.

270 Para una explicación completa de qué constituyen moneda e instrumentos monetarios, véase CBP, "Moneda / Instrumentos monetarios – Definición de instrumentos monetarios negociables para requisitos de declaración de monedas," (1 de mayo de 2025) https://www.help.cbp.gov/s/article/Article- 1413?language=en_US; FinCEN, "Informe sobre el transporte internacional de moneda o instrumentos monetarios," https://fincen105.cbp. dhs.gov/#/.

271 Inmigración y Control de Aduanas de EEE. UU. (ICE), "Combatiendo el contrabando de efectivo a granel", (actualizado el 29 de mayo de 2025) https://www.ice.gov/ sobre-ice/hsi/centers-labs/bcsc/faq.

272 DOJ, "Hombre mexicano se declara culpable de violar la ley federal de jefe y blanqueo de dinero en relación con la Organización Transnacional de Tráfico de Drogas con sede en Arizona," (8 de julio de 2025) https://www.justice.gov/usao-wdpa/pr/mexican-man-pleads-guilty violación de estatuto de capo federal y blanqueo de dinero.

co-conspiradores en la República Dominicana. Según la denuncia, los acusados introdujeron aproximadamente 8 millones de dólares en efectivo al granel. [273]

El dinero en efectivo también puede ser traído de vuelta a Estados Unidos como parte del proceso de blanqueo o para realizar planes criminales. En marzo de 2025, FinCEN publicó una alerta describiendo cómo los TCOs pueden introducir de contrabando ingresos ilícitos en efectivo hacia México y luego traer ese dinero de vuelta a Estados Unidos a través de servicios de vehículos blindados, declarando el efectivo como el ingreso legítimo de las empresas con sede en México. Este dinero puede luego introducirse en la economía estadounidense y transferirse de vuelta a México.[274] Como se señaló antes, en febrero de 2025, FinCEN impuso una multa civil de 37 millones de dólares contra Brink's por violaciones de blanqueo de capitales relacionadas con el transporte de efectivo a granel. [275]

Los TCO también pueden introducir dinero en efectivo de contrabando en Estados Unidos para comprar armas para exportar a México y así avanzar en sus campañas de terror. En un caso, un ciudadano mexicano se declaró culpable de su papel en una conspiración de blanqueo de dinero que implicaba el contrabando de moneda e instrumentos monetarios desde México hacia Estados Unidos para realizar pedidos a gran escala de munición a través de varios minoristas en línea. La munición fue posteriormente enviada a varios lugares del Valle del Río Grande para su exportación ilegal prevista a México. [276]

Cuentas de embudo

Los delincuentes también introducirán directamente en el sistema financiero estadounidense ingresos ilícitos en efectivo, a pesar del riesgo de que las instituciones financieras presenten informes de la BSA que atraigan el escrutinio de las fuerzas del orden. Un método común es el uso de cuentas embudo, que son cuentas bancarias, a menudo a nombre de representantes, utilizadas para "canalizar" depósitos de efectivo de varias personas, a menudo desde diferentes ubicaciones. Según las fuerzas del orden, los blanqueadores profesionales que operan a nivel nacional tienden a abrir cuentas embudo en grandes bancos con presencia nacional para que sus mensajeros puedan depositar efectivo al por mayor desde cualquier parte del país y minimizar el tiempo que deben pasar transportando dinero a granel por las autopistas.

En algunos casos, los delincuentes pueden estructurar depósitos en efectivo en las cuentas embudo por cantidades inferiores a 10.000 dólares para evitar que el banco presente CTRs. Sin embargo, si la organización criminal opera varias cuentas bajo propietarios nominales en diferentes bancos y realiza depósitos usando identificaciones falsas, puede optar por depositar efectivo sin tener en cuenta los umbrales de reporte, creyendo que estos pasos de ofuscación pueden obstaculizar las investigaciones policiales. Los fondos se mueven a través de varias instituciones financieras diferentes, transferencias bancarias transfronterizas o empresas pantalla, lo que dificulta su rastreo.

Depósitos pequeños y dispares en diferentes ubicaciones pueden parecer legítimos a nivel local al principio. Solo a nivel agregado se revela el patrón de embudo, generalmente después de que el dinero ha sido transferido de la cuenta. En diciembre de 2024, un exempleado de TD Bank con base en Florida fue arrestado y acusado penalmente de facilitar el blanqueo de dinero en Colombia. Como alega la denuncia, después de que otro empleado de TD Bank abriera cuentas a nombre de empresas pantalla con propietarios nominales, el hombre ayudó a la red de blanqueo de capitales emitiendo decenas de tarjetas de débito para las cuentas a cambio de sobornos. Supuestamente, esas cuentas se usaron para blanquear millones de dólares en ingresos de narcóticos mediante retiradas de efectivo en cajeros automáticos en Colombia. [277]

---

273 DOJ, "Azafata acusada en relación con el contrabando de dinero de drogas a la República Dominicana," (8 de mayo de 2024) https://www. justice.gov/usao-sdny/pr/flight-attendants-charged-connection-smuggling-drug-money-dominican-republic; DOJ, "Cuatro Azafata se declaran culpables de contrabando de dinero de drogas a la República Dominicana," (14 de agosto de 2024) https://www.justice.gov/usao-sdny/ pr/four-flight-azafatas-declararse-culpable de contrabando-dinero-droga-República Dominicana.

274 FinCEN, "Alerta FinCEN sobre el contrabando y repatriación de efectivo a granel por organizaciones criminales transnacionales con sede en México," (31 de marzo de 2025) https://www.fincen.gov/system/files/shared/BCS-Alert-FINAL-508C.pdf.

275 FinCEN, "FinCEN anuncia una multa civil de 37.000.000 de dólares contra Brink's Global Services USA, Inc. por violaciones de la Ley de Secreto Bancario," (6 de febrero de 2025) https://www.fincen.gov/news/news-releases/fincen-announces-37000000-civil-money-penalty-against-brinks- global-services-usa.

276 DOJ, "Red de contrabando de munición de un millón de dólares desmantelada," (28 de junio de 2024)

https://www.justice.gov/usao-sdtx/pr/million-dollar-red de contrabando de munición desmantelada.

277 DOJ, "TD Bank Insider arrestado y acusado de facilitar el blanqueo de capitales," (11 de diciembre de 2024) https://www.justice.gov/archivos/opa/pr/td-bank-insider-arrestado-y-acusado-facilitar-blanqueo de capitales; *véase también,* Orden de Consentimiento FinCEN Número 2024-02 (10 de octubre de 2024), pp. 31-32, https://www.fincen.gov/system/files?file=enforcement_action/2024-10-10/FinCEN-TD-Bank-Consent-Order-508FINAL.pdf.

Negocios intensivos en liquidez

Los delincuentes utilizan negocios intensivos en efectivo para blanquear ingresos ilícitos porque es más fácil mezclar transacciones ilícitas y legítimas en efectivo en comparación con otros métodos de pago, ya que los negocios intensivos en efectivo suelen hacer depósitos masivos en sus cuentas bancarias en lugar de reportar cada transacción por separado. En algunos casos, los delincuentes pueden poseer directamente un negocio intensivo en efectivo y usarlo como empresa pantalla, y en otros pueden comprar productos en un negocio externo con mucha liquidez que, sin saberlo o cómplicemente, ayuda a los delincuentes a blanquear su dinero. Para combatir este método de blanqueo de capitales, las empresas están obligadas a presentar un Informe de Pagos en Efectivo por Más de 10.000 $ en una Operación o Negocio (Formulario 8300) cuando reciben más de 10.000 $ en efectivo en una sola transacción o en transacciones relacionadas. [278]

Si un negocio es intensivo en liquidez depende del tipo de bienes y servicios que ofrece, de las costumbres sociales de la ciudad o región en la que opera y de las políticas o preferencias del propietario del negocio. Según la Reserva Federal, el uso de efectivo por parte de los estadounidenses se ha estabilizado tras un descenso al inicio de la pandemia de COVID-19, con una media de aproximadamente siete pagos en efectivo por consumidor al mes. El efectivo sigue utilizándose con mayor frecuencia en negocios donde los pagos presenciales son habituales, como supermercados, restaurantes, gasolineras y tiendas de productos generales. [279]

En septiembre de 2025, un hombre de Florida fue condenado a prisión por blanquear dinero a través de varios negocios que poseía, incluyendo un supermercado y un restaurante. Según documentos judiciales y pruebas presentadas en la audiencia de sentencia, el hombre anunció sus habilidades para blanquear dinero en varios estados y países. El hombre dijo a los agentes encubiertos que quizá necesitarían crear facturas para que pareciera que estaban comprando o vendiendo mercancía, y mencionó que no depositaría la moneda recibida de golpe; en su lugar, lo dividía y depositaba el dinero en incrementos de unos 5.000 dólares al día. [280]

X. Activos Digitales [281]

Desde la publicación de la NMLRA 2024, el ecosistema de activos digitales ha crecido considerablemente. Por ejemplo, el número de transacciones mensuales exitosas en blockchains públicas alcanzó máximos de 3.800 millones a principios de 2025, un aumento interanual del 96 por ciento.[282] proveedores de servicios de activos digitales desempeñan una amplia variedad de roles dentro del ecosistema de activos digitales. Además, otras entidades, como los bancos, continúan evaluando productos y servicios relacionados con activos digitales, incluyendo la oferta de custodia de activos digitales, préstamos respaldados por activos digitales y productos cotizados en bolsa que rastrean el precio de los activos digitales o emiten sus propios activos digitales. En general, el volumen de blanqueo de capitales a través de activos digitales sigue muy por debajo del realizado mediante moneda fiduciaria y otros métodos que no involucran activos digitales. Sin embargo, ciertos actores ilícitos, especialmente aquellos implicados en delitos nativos de activos digitales, pueden utilizar principalmente activos digitales en el proceso de blanqueo.

Las personas utilizan activos digitales para una variedad de fines legítimos, incluyendo inversiones, remesas y pagos por bienes y servicios. La capacidad de transferir activos rápidamente a través de fronteras y la percepción de anonimato, que atraen a algunos usuarios de activos digitales, también hacen que los activos digitales resulten atractivos para actores ilícitos. A medida que el uso de activos digitales ha crecido, los actores ilícitos se han familiarizado más con los activos digitales y han cometido cada vez más actividades ilícitas relacionadas con activos digitales, incluyendo estafas de inversión en activos digitales o el uso de activos digitales en sus propios fines

278 IRS, "Formulario 8300 y reporte de pagos en efectivo superiores a 10.000 dólares," (actualizado el 24 de julio de 2025) https://www.irs.gov/businesses/small- empresas-autónomas/Formulario-8300-y-reportando-pagos-de-más de 10.000.

279 Federal Reserve Financial Services, "Hallazgos de 2025 del Diario de la Elección de Pagos al Consumidor," (mayo de 2025) https://www.frbservices. org/binaries/content/assets/crsocms/news/research/2025-diary-of-consumer-payment-choice.pdf.

280 DOJ, "Hombre de Jacksonville condenado a prisión federal por aceptar blanquear más de 250.000 dólares," (8 de septiembre de 2025) https://www.justice. gov/usao-mdfl/pr/jacksonville-man-sentenced-federal-prison-agreeing-launder-over-250.000.

281 Aunque partes del gobierno de EE. UU. y el sector privado utilizan varios términos, este informe utiliza el término activo digital

para referirse a cualquier representación digital de valor registrada en un libro mayor distribuido, incluyendo criptomonedas, tokens digitales y stablecoins. Para fines de coherencia, esta terminología también se utiliza en casos concretos, pero solo pretende facilitar la comprensión del riesgo de financiación ilícita y no altera ninguna obligación legal existente.

282 a16zcrypto, "Estado del Índice Cripto", https://a16zcrypto.com/stateofcryptoindex. Estos datos sirven como proxy de la actividad en ciertas blockchains (concretamente, Ethereum, Polygon, Solana, Avalanche, Fantom, Celo, Optimism, Base y Arbitrum).

Procesos de blanqueo. En particular, muchos actores ilícitos que utilizan activos digitales prefieren las stablecoins debido a su relativa estabilidad respecto a otros activos digitales, así como a la liquidez en los mercados de stablecoins. Como parte del proceso de blanqueo, los actores ilícitos suelen intentar convertir activos digitales, específicamente stablecoins, en moneda fiduciaria a través de redes difusas de corredores de venta extrabursátil (OTC) en terceros países. Estos brókeres OTC pueden recibir comisiones sustanciales de actores ilícitos por ofrecer servicios de retirada de efectivo que aprovechan cuentas proxy para eludir los procesos CDD de los proveedores de servicios de activos digitales o explotar a proveedores con controles AML/CFT más débiles, entre otras tácticas.

Estados Unidos está tomando medidas para garantizar que los marcos existentes de AML/CFT y sanciones estén correctamente definidos para mitigar los riesgos financieros ilícitos asociados a los activos digitales, fomentando la innovación y protegiendo la libertad y la privacidad de los estadounidenses. En julio de 2025, el Grupo de Trabajo del presidente Trump sobre Mercados de Activos Digitales publicó un informe titulado "Fortalecimiento del liderazgo estadounidense en tecnología financiera digital", que incluía recomendaciones para establecer un marco integral de activos digitales en Estados Unidos.[283] Las recomendaciones destacan que una regulación efectiva y clara, junto con acciones policiales contra actores maliciosos, puede generar confianza entre los usuarios y empresas estadounidenses que buscan crecer a nivel nacional y asegurar que los innovadores estadounidenses lideren la industria de activos digitales. También en julio de 2025, el presidente firmó la Ley Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS), que creó el primer sistema regulatorio federal para stablecoins, proporcionando claridad regulatoria a los emisores de stablecoins.[284] Mientras Estados Unidos sigue adelante con este trabajo, los marcos existentes de AML/CFT y sanciones continúan aplicándose a los activos digitales y a los proveedores de servicios cubiertos relacionados.

En Estados Unidos, los proveedores de servicios de activos digitales tienen obligaciones AML/CFT si se encajan bajo la definición de institución financiera de la BSA.[285] Actualmente, la mayoría de los proveedores de servicios de activos digitales autorizados o registrados en Estados Unidos están registrados como MSB. Sin embargo, dependiendo de las actividades en las que participe el proveedor de servicios, ciertos proveedores pueden considerarse otro tipo de institución financiera, como corredores de bolsa o FCM, y tienen obligaciones AML/CFT diferentes en comparación con los registrados como MSB. Además, los proveedores de servicios de activos digitales que son personas estadounidenses, dondequiera que se encuentren, están obligados a cumplir con los programas de sanciones económicas administrados y aplicados por la OFAC. Las personas no estadounidenses también pueden tener obligaciones de cumplimiento de sanciones de la OFAC en algunas circunstancias. Las obligaciones de cumplimiento de sanciones son las mismas independientemente de si una transacción está denominada en activos digitales o en moneda fiduciaria. [286]

Para algunos delitos subyacentes, incluyendo ciertas estafas de inversión y ataques de ransomware, los activos digitales son la principal forma en que se generan y blanquean fondos. Para otros, como el narcotráfico, el fraude y el blanqueo profesional de capitales, los activos digitales son una de las muchas formas de blanquear ingresos ilícitos, junto con el mal uso de empresas pantalla, el contrabando masivo de efectivo o las transferencias bancarias. Como se describe a continuación, las formas más comunes en que actores ilícitos hacen un mal uso de activos digitales incluyen: 1) la explotación de proveedores estadounidenses de activos digitales que no cumplen con las obligaciones AML/CFT; 2) arbitraje jurisdiccional; 3) herramientas y métodos de ofuscación; y 4) uso de activos digitales fuera de una institución financiera regulada.

Incumplimiento de las obligaciones AML/CFT

Cuando los proveedores de servicios de activos digitales cubiertos no se registran ante el regulador correspondiente, no establecen ni mantienen controles AML/CFT suficientes o no cumplen con las obligaciones sancionadas, los delincuentes pueden explotar sus servicios con fines ilícitos. En algunos casos, los proveedores de servicios de activos digitales pueden afirmar no estar sujetos a la jurisdicción estadounidense a pesar de operar total o en parte sustancial en Estados Unidos. Algunos proveedores de servicios de activos digitales incluso han ordenado a clientes estadounidenses que proporcionen información falsa o utilicen un privado virtual

283 La Casa Blanca, "Fortaleciendo el liderazgo estadounidense en tecnología financiera digital" (julio de 2025),

https://www.whitehouse.gov/wp- contenido/subidas/2025/07/Digital-Assets-Report-EO14178.pdf.

284 La Casa Blanca, "Hoja informativa: El presidente Donald J. Trump firma la Ley GENIUS en ley" (julio de 2025), https://www.whitehouse.gov/fact- sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/.

285 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

286 Treasury, "Directrices de cumplimiento de sanciones para la industria de la moneda virtual," (octubre de 2021) https://ofac.treasury.gov/media/913571/ descargar?en línea; *véase, por ejemplo,* OFAC, "Preguntas frecuentes" (19 de marzo de 2018), https://ofac.treasury.gov/faqs/topic/1626; OFAC, "Preguntas frecuentes: 646," (15 de octubre de 2021) https://ofac.treasury.gov/faqs/646; OFAC, "Preguntas frecuentes: 1021," (11 de marzo de 2022) https://ofac.treasury.gov/faqs/1021.

para ocultar su presencia en EE. UU. al establecer cuentas en el momento de la incorporación para ocultar su base de clientes estadounidenses en un intento de parecer que la empresa estaba exenta de los requisitos regulatorios estadounidenses. [287]

Algunos proveedores de servicios de activos digitales, incluidos supuestos servicios de finanzas descentralizadas (DeFi) o plataformas P2P, pueden afirmar no estar regulados como instituciones financieras sujetas a la BSA. Determinar si una entidad, incluidos supuestos servicios DeFi, es una entidad financiera cubierta dependerá de hechos y circunstancias específicas que rodean sus actividades financieras.[288] En otros casos, los proveedores de servicios de activos digitales cubiertos no han cumplido con los requisitos del programa AML u otros requisitos bajo la BSA y sus normativas de implementación, permitiendo así que actores ilícitos blanqueen sus ingresos ilícitos. En algunos casos, los proveedores de servicios de activos digitales obligados por la BSA no recopilan información de identificación del cliente o, al introducir posteriormente los requisitos de información, solo los implementan al incorporar nuevos clientes. [289]

En un caso que se desveló en junio de 2025, un ciudadano ruso fue acusado de varios delitos relacionados con el uso de su empresa de activos digitales Evita para canalizar más de 500 millones de dólares en pagos extranjeros a través de bancos estadounidenses y intercambios de activos digitales, ocultando el origen y el propósito de las transacciones. Como se alega en la acusación, el hombre utilizó sus empresas para permitir que clientes extranjeros — muchos de los cuales tenían fondos en bancos rusos autorizados— le proporcionaran activos digitales, que luego blanqueó a través de carteras digitales y cuentas bancarias estadounidenses. Finalmente, el hombre convirtió los fondos en dólares estadounidenses u otras monedas fiduciarias y luego realizó pagos a través de cuentas bancarias en Manhattan en nombre de sus clientes extranjeros. En el proceso, las fuentes de los fondos se ocultaron, ocultando la pista de auditoría y ocultando las verdaderas contrapartes de las transacciones. [290]

Los proveedores de servicios de activos digitales deberían contar con controles adecuados para mitigar los riesgos asociados a los intercambios "anidados", que se refieren a los proveedores de servicios de activos digitales que ofrecen servicios de trading y agrupan los depósitos de los clientes en una cuenta alojada por un exchange más grande para ofrecer servicios ampliados a sus propios clientes. Los intercambios anidados pueden cumplir propósitos legítimos, como proporcionar mayor liquidez a sus clientes, pero también pueden presentar riesgos financieros ilícitos.[291] Por ejemplo, los intercambios anidados pueden operar total o parcialmente dentro de la infraestructura del proveedor anfitrión, en lugar de como una entidad única, lo que potencialmente proporciona a los actores ilícitos una capa adicional de ofuscación. En tales casos, las transacciones de intercambio anidadas pueden parecer realizadas por el proveedor anfitrión, lo que puede retrasar o dificultar los esfuerzos policiales para investigar actividades sospechosas. Además, esta ofuscación puede agravarse si el intercambio anidado carece de controles AML/CFT, lo que podría permitir que actores ilícitos accedan a los servicios del proveedor anfitrión sin proporcionar información identificativa y probablemente sin ser detectados. Para mitigar este riesgo, se espera que los proveedores de servicios de activos digitales sujetos a la BSA (por ejemplo, aquellos registrados como MSB) aseguren que su programa AML cuente con políticas, procedimientos y controles internos apropiados para identificar la actividad "anidada" y cumplir con los requisitos aplicables de la BSA.

---

287 *Véase, por ejemplo,* el DOJ, "OKX se declara culpable de violar las leyes estadounidenses contra el blanqueo de dinero y acepta pagar sanciones por un total de más de 500 millones de dólares," (24 de febrero de 2025) https://www.justice.gov/usao-sdny/pr/okx-pleads-guilty-violating-us-anti-money-laundering-laws-and- acepta-pagar-sanciones.

288 Treasury, "Evaluación del riesgo de finanzas ilícitas de las finanzas descentralizadas," (abril de 2023), p. 2, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

289 *Véase, por ejemplo,* el Departamento de Justicia, "OKX se declara culpable de violar las leyes estadounidenses contra el blanqueo de dinero y acepta pagar sanciones que suman más de 500 millones de dólares," (24 de febrero de 2025) https://www.justice.gov/usao-sdny/pr/okx-pleads-guilty-violating-us-anti-money-laundering-laws-and- acuerda-pagar-sanciones; DOJ, "Kucoin se declara culpable de cargo por transmisión de dinero sin licencia y acepta pagar multas que suman casi 300 millones de dólares," (27 de enero de 2025) https://www.justice.gov/usao-sdny/pr/kucoin-pleads-guilty-unlicensed-money-transmission sanciones por acusar y acuerda pagar; DOJ, "Cofundador de Paxful Inc. se declara culpable de conspiración para no mantener un programa eficaz contra el blanqueo de capitales," (8 de julio de 2024) https://www.justice.gov/usao-edca/pr/paxful-inc-co-founder-pleads-guilty-conspiracy-fail- mantener-efectivo-anti-dinero.

290 DOJ, "Fundador de empresa de pagos con criptomonedas acusado de evadir sanciones y controles de exportación, defraudar

instituciones financieras y violar la Ley de Secreto Bancario," (9 de junio de 2025)
https://www.justice.gov/opa/pr/founder-cryptocurrency-payment acusaciones de empresa por evadir sanciones y controles de exportación.

291 *Véase, por ejemplo,* FinCEN, "Orden de Consentimiento Número 2023-04," (noviembre de 2023), p. 34, https://www.fincen.gov/system/files?file=enforcement_acción/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf.

Además, el uso de quioscos de activos digitales en estafas se ha disparado en los últimos años.[292] En 2024, el IC3 recibió más de 10.956 denuncias sobre el uso de quioscos de activos digitales, con pérdidas de víctimas reportadas de aproximadamente 246,7 millones de dólares.[293] Esto representa un aumento del 99 por ciento en el número de quejas y un incremento del 31 por ciento en las pérdidas de víctimas reportadas respecto a 2023.[294] Este aumento de la actividad ilícita puede estar relacionado con tasas sustanciales de incumplimiento de los requisitos regulatorios AML/CFT por parte de los operadores de quioscos.[295] quioscos de activos digitales se consideran MSB bajo la BSA.[296] Según las fuerzas del orden, los estafadores han dirigido a las víctimas a quioscos específicos de activos digitales, a veces a través de fronteras estatales, probablemente para evitar operadores de quioscos digitales con fuertes controles AML/CFT.

Enfoque especial: Aumento del uso indebido de las stablecoins

Los actores ilícitos utilizan cada vez más stablecoins para facilitar transacciones y almacenar los ingresos. El gobierno de EE. UU. ha identificado el uso indebido de las stablecoins para evadir sanciones;[297] fraude;[298] financiación del terrorismo;[299] y financiación por proliferación;[300], entre otros delitos. La liquidez, la estabilidad relativa y la rápida liquidación de las stablecoins atraen a actores ilícitos de la misma manera que atraen a usuarios lícitos para fines legítimos.[301] A menudo, actores ilícitos utilizan stablecoins como uno de los elementos de un complejo proceso de blanqueo que puede incluir el uso de proveedores de servicios de activos digitales, el cambio entre stablecoins y otros activos digitales, y transferencias entre monederos autoalojados. Los actores ilícitos también pueden utilizar stablecoins en la última fase de su transacción, ya que convierten sus activos digitales ilícitos en moneda fiduciaria, que a menudo es necesaria para comprar bienes y servicios. Algunos facilitadores implicados en el intercambio de ingresos ilícitos en activos digitales por moneda fiduciaria, incluidos los corredores de activos digitales de venta libre, pueden solicitar stablecoins en lugar de otros activos digitales teniendo en cuenta las características mencionadas anteriormente.

Ciertos emisores de stablecoins desarrollan y mantienen el contrato inteligente subyacente que soporta la stablecoin. En algunos casos, los emisores incorporan funcionalidades que les permiten mantener el control y modificar el uso de sus tokens. Esto puede incluir la posibilidad de prohibir que direcciones concretas de monedero interactúen con los contratos inteligentes de stablecoin, "congelando" efectivamente los fondos de stablecoins que se mantienen en esas direcciones. Los emisores también pueden eliminar permanentemente las stablecoins de la circulación. Las fuerzas del orden han colaborado con emisores de stablecoins para incautar cientos de millones de

292 FTC, "Cajeros automáticos de Bitcoin: Un portal de pagos para estafadores," (3 de septiembre de 2024) https://www.ftc.gov/news-events/data-visualizations/data- spotlight/2024/09/bitcoin-cajeros automáticos-payment-portal-estafadores.

293 IC3, "Internet Crime Report 2024," (23 de abril de 2025), p. 36, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

294 Ibid.

295 FinCEN, "Aviso de FinCEN sobre el uso de quioscos de moneda virtual convertibles para pagos fraudulentos y otras actividades ilícitas," (4 de agosto de 2025) https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf.

296 Como MSB, cualquier persona no exenta que participe en la transmisión de dinero debe registrarse en FinCEN en un plazo de 180 días desde que comience a participar en la transmisión de dinero. Véase 31 C.F.R. § 1022.380. Los transmisores de dinero también deben cumplir con las obligaciones de registro, reporte y supervisión de transacciones establecidas en las partes 1010 y 1022 del capítulo X del 31 CFR. Ejemplos de tales requisitos incluyen la presentación de Informes de Transacciones de Divisas (31 C.F.R. § 1022.310) y Informes de Actividad Sospechosa (31 C.F.R. § 1022.320), así como obligaciones generales de registro (31 C.F.R. § 1010.410).

297 *Ver, por ejemplo,* Tesorería, "Treasury Expone Red de Blanqueo de Capitales que utiliza activos digitales para evadir sanciones," (4 de diciembre de 2024) https:// home.treasury.gov/news/press-releases/jy2735 298 *Ver, por ejemplo,* DOJ, "Mayor incautación de fondos jamás registrada relacionada con estafas de confianza en criptomonedas," (18 de junio de 2025) https://www.justice.gov/usao-dc/ pr/más grande-jamás decomis-fondos-decompresión-relacionados-cripto-estafas.

299 *Véase, por ejemplo,* DOJ, "Departamento de Justicia interrumpe el esquema de financiación terrorista de Hamás mediante la incautación de criptomonedas," (27 de marzo de 2025) https://www.justice.gov/usao-dc/pr/justice-department-disrupts-hamas-terrorist-financing-scheme-through-seizure; DOJ, "United Estados publican la demanda civil presentada contra aproximadamente 2 millones de dólares en moneda digital involucrada en la recaudación de fondos de Hamás," (22 de julio de 2025) https:// www.justice.gov/opa/pr/united-states-unseals-civil-action-filed-against-approximately-2m-digital-currency-involved. 300 *Ver, por ejemplo,* el Departamento de Justicia, "El Departamento de Justicia anuncia acciones a nivel nacional para combatir la generación ilícita de ingresos del gobierno norcoreano," (14 de noviembre de 2025) https://www.justice.gov/opa/pr/justice-department-announces-nationwide-actions-combat-illicit-north-korean- gobierno.

301 *Véase, por ejemplo,* Tesorería, "Evaluación Nacional del Riesgo de Financiación del Terrorismo," (febrero de 2024) https://home.treasury.gov/system/files/136/2024- National-Terrorist-Financing-Risk-Assessment.pdf; Consejo de Seguridad de la ONU, "Informe final del Panel de Expertos presentado conforme a la resolución 2680," (marzo de 2024)

https://documents.un.org/doc/undoc/gen/n24/032/68/pdf/n2403268.pdf; UNODC, "Casinos, blanqueo de capitales y crimen organizado transnacional en Asia Oriental y Sudoriental: una amenaza oculta y acelerada," (enero de 2024) https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf, .

Stablecoins por valor de dólares involucrados en actividades ilícitas aprovechando esta capacidad. [302]

Arbitraje jurisdiccional

Como se destacó en anteriores NMLRA, la regulación y supervisión desiguales y a menudo inadecuadas entre jurisdicciones permite que los proveedores de servicios de activos digitales y actores ilícitos realicen arbitraje regulatorio. Esta cuestión es especialmente preocupante para los proveedores de servicios de activos digitales, dado que tienen la capacidad de transferir activos virtuales a través de fronteras casi instantáneamente en comparación con otras transferencias financieras, el hecho de que muchos proveedores de servicios de activos digitales operan o tienen arquitectura en varias jurisdicciones, y la amplitud de las brechas en la implementación de los estándares internacionales AML/CFT establecidos por el Grupo de Acción Financiera (FATF).

En 2019, el GAFI aclaró cómo se aplican sus estándares globales sobre AML/CFT a los activos digitales y proveedores de servicios de activos digitales.[303] Aunque muchos países han avanzado en el desarrollo de marcos AML/CFT para proveedores de servicios de activos digitales, una encuesta del GAFI identificó que, a mediados de 2025, casi 30 países no habían determinado su enfoque AML/CFT para los proveedores de servicios de activos digitales.[304] Además, muchos países con marcos AML/CFT para proveedores de servicios de activos digitales aún no los han puesto en marcha. Las fuerzas del orden han observado que actores ilícitos aprovechan estas lagunas, utilizando proveedores extranjeros de servicios de activos digitales para ocultar la propiedad y ubicación de los beneficios ilícitos como parte de su proceso de blanqueo.[305] Al hacerlo, estos actores pueden buscar proveedores de servicios que no requieran, entre otras cosas, que los clientes proporcionen información personal identificativa o documentos de identidad.

En un caso, el DOJ presentó una demanda civil solicitando la confiscación de activos digitales valorados en aproximadamente 7,1 millones de dólares, que fueron incautados en la investigación de un esquema de fraude de inversión relacionado con el petróleo y el gas. Según la presentación de la confiscación y otros registros del caso, desde al menos agosto de 2022 hasta agosto de 2024, los co-conspiradores convencieron a las víctimas para que enviaran dinero a lo que se presentó como cuentas de depósito en garantía para comprar depósitos de depósito de petróleo en Róterdam, Países Bajos, o Houston. El dinero se trasladó rápidamente a una o más de al menos 81 cuentas diferentes en instituciones financieras, se trasladó al extranjero o a una o más de al menos 19 cuentas diferentes, donde se utilizó para la compra de activos digitales, incluyendo Bitcoin, Tether, USD Coin y Ether. Muchos de los activos digitales se transfirieron a cuentas en el proveedor de servicios de activos digitales Binance. Algunos de los activos digitales adquiridos con fondos de las víctimas también fueron enviados a proveedores de servicios de activos digitales en Rusia y Nigeria, al menos uno de los cuales se alega que facilitó el blanqueo de capitales para TCOs, incluyendo organizaciones terroristas y organizaciones que violan sanciones comerciales internacionales. [306]

Herramientas y métodos de ofuscación

Los delincuentes suelen utilizar herramientas, servicios y métodos de ofuscación que suponen desafíos para los investigadores que intentan rastrear activos digitales ilícitos. Estas herramientas y servicios incluyen mezcladores, criptomonedas que mejoran el anonimato (AECs) y servicios de blanqueo de capitales a través de mercados de la darknet. Además de vender drogas ilícitas y otros contrabandos, los mercados de la darknet suelen ofrecer servicios de blanqueo de capitales, mezclando activos digitales utilizados para la compra de bienes y servicios en el mercado. En algunos casos, actores ilícitos pueden depositar fondos y posteriormente retirarlos de los mercados de la darknet sin realizar ninguna compra como técnica de blanqueo. [307]

Los actores ilícitos también utilizan métodos diseñados para ocultar la trazabilidad de las transacciones en blockchains públicas, lo que puede frustrar investigaciones policiales así como a proveedores de servicios de activos digitales que intentan detectar si

302 *Ver, por ejemplo,* DOJ, "Agentes del Departamento de Justicia incautan 8,5 millones de dólares en criptomonedas y desbaratan esquema de fraude en inversiones," (18 de diciembre de 2025) https://www.justice.gov/usao-ednc/pr/department-justice-agents-seize-85-million-cryptocurrency-and-disrupt-investment- fraude.

303 El GAFI utiliza los términos "activos virtuales" y "proveedores de servicios de activos virtuales (VASP)". Consulta el GAFI,

"Activos Virtuales", https://www.fatf-gafi. org/en/topics/virtual-assets.html.

304 FATF, "Actualización Dirigida sobre la Implementación de los Estándares FATF en Activos Virtuales y Proveedores de Servicios de Activos Virtuales," (junio de 2025) https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

305 Consulta la sección de Estafas de Inversión en Activos Digitales para más ejemplos.

306 DOJ, "EE. UU. inicia una acción civil para perder 7,1 millones de dólares en criptomonedas vinculadas a un esquema de fraude en almacenamiento de petróleo y gas," (22 de julio de 2025) https://www.justice.gov/usao-wdwa/pr/us-commences-civil-action-forfeit-71-million-cryptocurrency-tied-oil-and-gas-storage.

307 *Véase, por ejemplo,* el DOJ, "Hacker de Bitfinex condenado por conspiración de blanqueo de dinero que involucra miles de millones en criptomonedas robadas," (14 de noviembre de 2024) https://www.justice.gov/archives/opa/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen.

Los fondos entrantes están ligados a actividades ilícitas. Los actores pueden hacer un intercambio de cadena intercambiando activos digitales en una blockchain por activos digitales en otra, incluso utilizando puentes entre cadenas. Otros métodos de ofuscación incluyen el intercambio de activos utilizando servicios DeFi para realizar cientos de miles de transacciones rápidas a través de una gran red de direcciones, creando una compleja red de transacciones.[308] Aunque muchas de las direcciones en estas webs suelen ser monederos autoalojados, también pueden ser cuentas de proveedores de servicios de activos digitales que operan fuera de la cadena.[309] Los actores ilícitos pueden utilizar información falsa de identificación de clientes para abrir cuentas en estos proveedores como parte de su proceso de blanqueo. [310]

Uso de activos digitales fuera de instituciones reguladas

Muchos activos digitales pueden ser autocustodiados y transferidos sin la intervención de una institución financiera intermediaria. Estas transacciones P2P pueden limitar la recopilación y el acceso de las autoridades a la información de clientes y transacciones. Aunque el marco de la BSA abarca a muchos proveedores de servicios de activos digitales en Estados Unidos, el marco legislativo actual no contempla claramente protocolos totalmente descentralizados, donde la gobernanza o la toma de decisiones se distribuyen entre comunidades de usuarios y los protocolos pueden ser inmutables. El informe del presidente del Grupo de Trabajo sobre Mercados de Activos Digitales de julio de 2025 señaló que, para proporcionar claridad a la industria y permitir soluciones adaptadas para mitigar los riesgos financieros ilícitos, el Congreso debería considerar un enfoque basado en principios para definir los distintos actores del ecosistema DeFi. De forma relacionada, algunos servicios DeFi pueden quedar fuera del marco AML/CFT en Estados Unidos y, como tal, pueden no implementar medidas para mitigar el riesgo financiero ilícito.[311] Estos casos pueden presentar una vulnerabilidad, aunque estas transacciones pueden ocurrir en blockchains públicas proporcionando cierta transparencia. [312]

XI. Productos y Servicios Financieros

Las instituciones financieras y otras entidades ofrecen una amplia gama de productos y servicios financieros que permiten a sus clientes transferir y almacenar valor. Los riesgos de blanqueo de capitales de estos productos y servicios varían en función de varios factores, incluyendo el nivel de adopción, la velocidad de pagos, la cantidad de valor transferido, el nivel de integración del producto o servicio con el sistema financiero en general y las obligaciones AML/CFT de los proveedores. Aunque la disponibilidad y adopción de productos y servicios más recientes como los pagos P2P y los activos digitales están creciendo, los productos y servicios tradicionales como las tarjetas de crédito y los pagos ACH también han ido creciendo en los últimos años, superando los niveles previos a la pandemia. Según una encuesta realizada por el FRB, los pagos con tarjetas de crédito y débito representaron casi dos tercios de todos los pagos a consumidores en 2024, seguidos de efectivo (14 por ciento), ACH (13 por ciento), otros (cinco por ciento), cheques (tres por ciento) y aplicaciones de pago móvil (menos del uno por ciento). [313]

Tecnologías más recientes, como herramientas de análisis de redes que revelan conexiones ocultas, bots para reforzar los esfuerzos de identificación de clientes y IA generativa para la incorporación y monitorización de transacciones, han permitido a los proveedores mitigar parte del riesgo mejorando la detección y prevención de actividades ilícitas. Pero los actores ilícitos también han intentado utilizar estas herramientas para explotar productos y servicios vulnerables. Las instituciones financieras están obligadas a evaluar los riesgos de productos y servicios,

especialmente a medida que se introducen nuevos, y la eficacia de estos esfuerzos continuos

308 DOJ, "Hombre canadiense acusado en esquemas de hackeo de criptomonedas de 65 millones de dólares," (3 de febrero de 2025) https://www.justice.gov/opa/pr/canadian- hombre acusado-de-65 millones de esquemas de hackeo de criptomonedas; Acusación, Estados Unidos de América contra Andean Medjedovic, Nº 1:24-cr-00529- NGG (E.D.N.Y. 30 de diciembre de 2024) ¶ 49 https://www.justice.gov/opa/media/1388021/dl.

309 Acusación, Estados Unidos de América contra Andean Medjedovic, Nº 1:24-cr-00529-NGG (E.D.N.Y. 30 de diciembre de 2024) ¶ 56-57, 81 https:// www.justice.gov/opa/media/1388021/dl..

310 Ibid, ¶ 55-66.

311 La Casa Blanca, "Fortaleciendo el liderazgo estadounidense en tecnología financiera digital," (julio de 2025) p. 106-7 https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf. Si una entidad que opera en el ámbito DeFi es una institución financiera cubierta por la BSA depende de hechos y circunstancias específicas que rodean sus actividades financieras. 312 *Ver, por ejemplo,* el DOJ, "El Departamento de Justicia solicita la confiscación de más de 5 millones de dólares en Bitcoin robado en estafas de intercambio de SIM," (9 de septiembre de 2025)

https://www.justice.gov/usao-dc/pr/justice-department-seeks-forfeiture-over-5-million-bitcoin-stolen-sim-swapping-scams.

313 Federal Reserve Financial Services, "Hallazgos de 2025 del diario de la elección de pagos al consumidor," (mayo de 2025), p. 5, https://www. frbservices.org/binaries/content/assets/crsocms/news/research/2025-diary-of-consumer-payment-choice.pdf. "Otros" pagos incluyen acceso prepago, transferencias de cuenta a cuenta, deducciones de ingresos, giros postales y otros métodos que no encajaban en las categorías existentes.

es un componente fundamental para garantizar que los productos y servicios financieros, tanto nuevos como antiguos, no se conviertan en vectores de delitos financieros.

Tarjetas de crédito y acceso prepago

Las tarjetas de crédito, tarjetas de débito y accesos prepago presentan diversas vulnerabilidades en materia de finanzas ilícitas. Los delincuentes explotan las tarjetas para blanqueo de capitales, fraude y otros esquemas financieros ilícitos, aprovechando la alta liquidez de las tarjetas y su integración fluida en el comercio legítimo. Las tarjetas de pago son ampliamente aceptadas y fácilmente convertidas en efectivo o bienes, lo que permite mover rápidamente los ingresos ilícitos mediante transacciones rutinarias. Los operadores de sistemas de tarjetas de crédito están sujetos a los requisitos de programa, informes y registro AML/CFT.[314] Además, bajo la BSA, ciertos proveedores y vendedores de acceso prepago se consideran MSB y también están sujetos a los requisitos del programa, informes y registro AML/CFT. [315]

Las tipologías de blanqueo de capitales suelen variar según el tipo de tarjeta, y los delincuentes explotan las vulnerabilidades específicas de cada una. Por ejemplo, las tarjetas prepago y regalo son una opción popular para blanquear fondos ilícitos debido a su anonimato, transferibilidad y al hecho de que generalmente no se necesita una cuenta; Las tarjetas de crédito y débito requieren una cuenta, por lo que los esquemas que involucran estas tarjetas suelen depender de identidades robadas; y los requisitos laxos sobre el uso de chips EMV en tarjetas de transferencia electrónica de beneficios (EBT) las convierten en un objetivo popular para "desviar" información de tarjetas de la banda magnética de una tarjeta.

El acceso prepago, incluidas las tarjetas regalo, merece un escrutinio especial tanto por fraude como por blanqueo de capitales. Las tarjetas prepago de propósito general, también llamadas tarjetas regalo de bucle abierto, que operan en las principales redes de tarjetas, son valiosas para los delincuentes porque los fondos pueden cargarse en efectivo o transferencia, retirarse en cajeros automáticos o usarse para compras, permitiendo el movimiento de dinero ilícito con menos supervisión que las transferencias bancarias tradicionales. Una estafa común consiste en que un estafador contacta con una víctima y le dice que debe dinero (por ejemplo, para pagar impuestos atrasados o atrasos de una póliza de seguro de vida). Se indica a la víctima que compre tarjetas prepago y proporcione al delincuente el número de la tarjeta. El acceso prepago en circuito cerrado (es decir, tarjetas con marca de tienda o tarjetas regalo) también se utiliza ampliamente en esquemas de fraude y blanqueo de capitales. [316]

Otro esquema común de tarjetas regalo implica el "drenaje de tarjetas", en el que los delincuentes roban tarjetas regalo de los expositores comerciales y registran la información, vuelven a sellar las tarjetas en su embalaje original y vuelven a colocar las tarjetas regalo en las estanterías de las tiendas. Una vez que un cliente compra la tarjeta regalo y carga fondos en ella, el delincuente tiene acceso a los fondos sin que el cliente lo sepa.[317] Estos esquemas se han vinculado a grupos de crimen organizado chinos, y Homeland Security Investigations (HSI) estima que las operaciones de drenaje de tarjetas oscilan entre cientos de millones de dólares. Las tarjetas regalo también se utilizan a menudo como un paso en el ciclo de vida del lavado de capitales debido a su anonimato, portabilidad (tanto física como mediante la transferencia del código) y facilidad para convertirse en mercancías. Los delincuentes pueden comprar tarjetas regalo con el producto del delito, a veces vendiéndolas a otros con descuento, y otras veces usándolas para adquirir bienes de alto valor, que luego revenden. [319]

Otras tipologías que involucran tarjetas se dirigen específicamente a tarjetas de crédito y débito, que se basan en cuentas. Al igual que los cheques, las tarjetas de crédito y débito robadas en esquemas de robo de correo pueden usarse para comprar bienes para reventa o personales

314 31 CFR Capítulo X, Parte 1028: Normas para operadores de sistemas de tarjetas de crédito.

315 31 CFR Capítulo X, Parte 1022: Normas para los MSB.

316 FTC, "Evitando y reportando estafas con tarjetas regalo," (julio de 2023) https://consumer.ftc.gov/articles/avoiding-and-reporting-gift-card-scams.

317 *Véase, por ejemplo,* DOJ, "Ciudadano chino condenado a prisión federal por fraude con dispositivos de acceso," (3 de abril de 2025), https://www.justice.gov/usao- mdfl/pr/chino-nacional-sentenciado-federal-penitencia-dispositivo-fraude.

318 HSI, "Combatiendo el aumento del fraude con tarjetas regalo" (actualizado el 15 de agosto de 2025) https://www.ice.gov/about-ice/hsi/news/hsi-insider/tackling-gift- fraude con tarjetas.

319 *Véase, por ejemplo,* DOJ, "Tres hombres del condado de Los Ángeles condenados a prisión federal por blanquear tarjetas regalo compradas por víctimas de estafas telefónicas," (26 de marzo de 2024) https://www.justice.gov/usao-cdca/pr/three-los-angeles-county-men-sentenced-federal-prison- lavado-tarjetas-regalo-comprado.

Úsate.[Las tarjetas 320] de crédito y débito también son objetivo mediante dispositivos de desviación de tarjetas y mediante esquemas de "fuga", en los que los delincuentes defraudan a los bancos abriendo cuentas de tarjeta, a menudo con identidades robadas, y luego "escapan" realizando grandes compras. En un caso, un ciudadano con doble nacionalidad estadounidense y griego fue acusado en relación con una conspiración de fraude bancario multimillonaria. Según documentos presentados en el caso y declaraciones hechas en el tribunal, el hombre y los co-conspiradores crearían empresas pantalla y abrieron cuentas bancarias a nombre de dichas empresas. Luego financiaban esas cuentas con fondos nominales. Luego, tras unos meses sin actividad, financiaban las cuentas mediante transferencias desde fuentes externas, incluidas las que controlaban. Varias semanas después, realizaban compras de débito muy grandes a lo largo de varios días desde esas cuentas, lo que provocaba que esas cuentas acumularan saldos significativamente negativos. Ejecutaron este esquema en numerosas ocasiones en seis instituciones financieras víctimas entre julio de 2022 y julio de 2023, causando a esas instituciones pérdidas de aproximadamente 2,8 millones de dólares. [321]

El skimming de tarjetas, en el que los delincuentes instalan dispositivos skimmer en cajeros automáticos, bombas de gasolina o terminales de punto de venta para robar datos y PINs de la tarjeta, también aborda la vulnerabilidad inherente de los pagos con tarjeta. En concreto, las tarjetas EBT son un objetivo atractivo para actores ilícitos porque, en gran medida, no están habilitadas para chip, lo que las hace mucho más fáciles de comprometer y[cobrar.322] Según el Servicio Secreto de EE. UU. (USSS), se estima que el desvío de EBT por sí solo cuesta a las instituciones financieras y a los consumidores más de 1.000 millones de dólares cada año.[323] El USDA fomenta la funcionalidad de los chips pero deja la adopción a manos de los estados; California comenzó a emitir tarjetas EBT con chip en enero de 2025, con la adopción prevista en algunos otros estados.[324] En agosto de 2025, un inmigrante ilegal de Rumanía fue condenado a 120 meses de prisión federal por desviar decenas de miles de tarjetas EBT en California y Nueva York. El hombre entró en Estados Unidos con un visado de turista en 2020, pero se quedó más tiempo de su visado. Viajó por Los Ángeles y el Inland Empire instalando sofisticados dispositivos de skimming en cajeros automáticos y terminales de punto de venta para registrar la información de las cuentas de las personas que usaban esos dispositivos. Trabajó con varios miembros de un TCO de Rumanía para llevar a cabo este plan. Una orden de registro para la residencia de uno de sus cómplices reveló que les había enviado más de 36.000 números de tarjetas EBT robadas durante tres años. [325]

Pagos entre Personas

Las plataformas de pago peer-to-peer (P2P), como Zelle, Venmo, PayPal, Cash App y Apple Pay, se han utilizado ampliamente en Estados Unidos durante la última década. Estos servicios permiten transferencias instantáneas y de bajo coste entre individuos y, aunque son convenientes para los consumidores, también presentan vulnerabilidades que los actores ilícitos pueden explotar. Los delincuentes pueden explotar plataformas P2P para blanqueo de capitales, esquemas de fraude, venta de bienes ilegales y otros fines financieros ilícitos, aprovechando la rapidez y escala de estos sistemas. Las plataformas de pago P2P pueden cumplir con la definición de MSB y estar sujetas a los requisitos de programa, informes y registro AML/CFT. [326]

Los pagos P2P son rápidos, ampliamente adoptados y a menudo irrevocables, lo que los hace ideales para mover y disfrazar fondos ilícitos. En 2024, la red doméstica estadounidense Zelle por sí sola procesó más de 1 billón de dólares en 3.600 millones de[transferencias (327),] un volumen enorme en el que los delincuentes pueden intentar integrarse. Muchas plataformas P2P no cobran comisiones y funcionan las 24 horas del día, los 7 días de la semana,

320 *Véase, por ejemplo,* DOJ, "Mujer de Carson y exempleada del Servicio Postal de EE. UU. condenada a más de 5 años de prisión federal por robar cheques y tarjetas de crédito del correo," (8 de diciembre de 2025) https://www.justice.gov/usao-cdca/pr/carson-woman-and-former-us-postal- empleado-servicio-sentenciado-más-5-años-federal.

321 DOJ, "Doble ciudadano estadounidense y griego arrestados por conspiración multimillonaria de fraude bancario," (6 de marzo de 2024) https://www.justice.gov/ usao-nj/pr/dual-estadounidense-y-griego-nacional-arrestado-multimillonaria-fraude-bancaria-conspiración.

322 FBI, "Skimming," (actualizado el 18 de noviembre de 2025) https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and- estafas/skimming.

323 USSS, "Agencias de aplicación de la ley realizan fraudes EBT y divulgación de robo de tarjetas," (31 de enero de 2025) https://www.secretservice. gov/newsroom/releases/2025/01/agencias de aplicación de la ley realizan fraude ebt y cartas desviadas.

324 USDA, "Modernización SNAP EBT," (actualizado el 7 de diciembre de 2025) https://www.fns.usda.gov/snap/ebt/modernization.

325 DOJ, "Hombre rumano condenado a 10 años en prisión federal por desviar decenas de miles de tarjetas de asistencia social en cajeros automáticos," (4 de agosto de 2025), https://www.justice.gov/usao-cdca/pr/romanian-man-sentenced-10-years-federal-prison-skimming-tens-thousands-welfare-tarjetas.

326 31 CFR Capítulo X, Parte 1022: Normas para MSB.

327 Zelle, "Zelle rompe récords con 1 billón de dólares enviado en un solo año," (12 de febrero de 2025) https://www.zellepay.com/press-releases/zelle- rompe récords de 1 billón enviado-un solo año.

mientras que las transferencias bancarias pueden tardar días y ser relativamente caras. Esta comodidad también significa que las transferencias fraudulentas o ilegales pueden ocurrir rápidamente y ser difíciles de revertir, dejando a las víctimas y a las instituciones financieras poco tiempo para detectar o recuperar pagos ilícitos. Además, las plataformas P2P suelen integrarse con las cuentas bancarias, tarjetas de débito o tarjetas de crédito de los usuarios, permitiendo a los delincuentes mover fondos rápidamente a través de múltiples instituciones.

Los blanqueadores de dinero utilizan plataformas P2P para agrupar e integrar los beneficios ilícitos de delitos subyacentes. El tráfico de drogas, el fraude y otras empresas criminales han utilizado extensamente transferencias P2P para mover dinero sucio dentro y a través del sistema bancario. En un caso, una mujer se declaró culpable de conspiración para distribuir sustancias controladas y blanqueo de capitales. Una revisión de los registros bancarios de la mujer reveló que recibió y gastó más de 2 millones de dólares entre 2017 y 2023.
Los agentes rastrearon sus transacciones de drogas a través de aplicaciones P2P como Zelle y Cash App. [328]

Las plataformas P2P también pueden ser solo un componente de complejos esquemas de blanqueo de capitales que se basan en varios métodos para ocultar el origen y la propiedad. En junio de 2025, el Departamento de Justicia desclasificó una acusación que acusaba a dos hombres de fraude bancario y robo de identidad agravado. Según documentos judiciales, un hombre se hizo cargo de varias cuentas bancarias pertenecientes a dos víctimas mayores en dos bancos diferentes. Los dos hombres canalizaron el dinero robado a través de cuentas de paso creadas a nombre de las víctimas. Finalmente, se repartieron el dinero a sí mismos mediante retiradas de efectivo en cajeros automáticos, cheques personales, transacciones con Western Union, transacciones Zelle, pagos a tarjetas de crédito, juegos de azar online y la compra de un Mercedes. [329]

Los esquemas de fraude dirigidos a consumidores aprovechan cada vez más las plataformas P2P para robar fondos, ya que los estafadores aprovechan la rapidez y la finalización de estas transacciones. Según la FTC, las pérdidas reportadas por fraude en aplicaciones de pago han crecido una media del 47 % interanual en los últimos cuatro años, alcanzando los 390 millones de dólares en 2024. Esto probablemente representa solo una fracción del fraude total.[Las estafas 330] que involucran pagos P2P suelen comenzar con el estafador contactando a sus víctimas por correo electrónico y llamadas telefónicas y terminan con el estafador dirigiendo a la víctima para enviar dinero a través de una plataforma P2P para "revertir" una transacción fraudulenta ficticia realizando un pago P2P a lo que cree que es su propia cuenta, pero que en realidad es, Una cuenta controlada por los estafadores. [331]

Más allá del fraude y el blanqueo de capitales, las plataformas P2P se utilizan a menudo para facilitar pagos por bienes y servicios ilegales, que van desde la venta de drogas hasta el juego sin licencia o incluso las tarifas de tráfico de personas. Estos esfuerzos pueden ser facilitados por plataformas P2P que no cumplen con sus obligaciones AML/CFT. En enero de 2025, Block, Inc. (Block) pagó una multa de 80 millones de dólares a 48 estados y al Distrito de Columbia y acordó emprender acciones correctivas por violaciones de las leyes BSA y AML en relación con su servicio de pago móvil, Cash App.[332] Reguladores estatales determinaron que Block no cumplía ciertos requisitos, lo que creaba la posibilidad de que sus servicios pudieran utilizarse para apoyar el blanqueo de capitales, la financiación del terrorismo u otras actividades ilegales. [333]

328 DOJ, "Mujer de Rosedale se declara culpable de conspiración para distribuir sustancias controladas y blanqueo de dinero," (4 de junio de 2025), https:// www.justice.gov/usao-md/pr/rosedale-woman-pleads-guilty-conspiracy-distribute-controlled-substances-and-money. 329 DOJ, "Cuñados acusados por esquema de adquisición bancaria y robo de identidad agravado," (17 de junio de 2025) https://www.justice.gov/usao-edca/pr/brothers-law-acusado-esquema-adquisición-bancaria-y-robo-de_identidad_agravado.

330 Las pérdidas reportadas fueron de 87,3 millones de dólares en 2020, 129,3 millones en 2021, 163,5 millones en 2022, 209,9 millones en 2023 y 391 millones en 2024. Consulta la FTC, el panel público de Tableau https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/ PaymentContactMethods.

331 FTC, "¿Usáis aplicaciones de pago como Venmo, CashApp o Zelle? Lee esto," (14 de agosto de 2023) https://consumer.ftc.gov/consumer-alertas/2023/08/¿usas-apps-pago-venmo-cashapp-o-zelle-read;" *véase, por ejemplo,* el DOJ, "Florida Man Confesss Defrauding Users Zelle" (21 de mayo de 2024), https://www.justice.gov/usao-ct/pr/florida-man-admits-defrauding-zelle-users.

332 Conference of State Bank Supervisors (CSBS), "Los reguladores estatales imponen una multa de 80 millones de dólares a Block, Inc., Cash App por violaciones de BSA/AML," (15 de enero de 2025) https://www.csbs.org/newsroom/state-regulators-issue-80-million-penalty-block-inc-cash-app-bsaaml-violations. 333 Por separado, en abril de 2025, Block, Inc. pagó una multa de 40 millones de dólares al Departamento de Servicios Financieros de Nueva York (NY DFS) por fallos significativos en su programa de cumplimiento BSA/AML. La investigación del DFS de Nueva York reveló lagunas críticas en el programa BSA/AML de Block, incluyendo un CDD inadecuado, la falta de implementación de controles basados en riesgos adecuados para prevenir el blanqueo de capitales y actividades ilícitas, y la falta de monitorización efectiva y oportuna de las transacciones. Cabe destacar que el trato laxa de Block hacia las transacciones de alto riesgo de Bitcoin permitió que transacciones mayormente anónimas avanzaran sin el debido escrutinio. Además, el rápido crecimiento de Block entre 2019 y 2020 contribuyó a un grave retraso en alertas de transacciones, que Block dejó sin abordar durante un periodo significativo. NY DFS, "La superintendente Adrienne A. Harris asegura un acuerdo de 40 millones de dólares con Block, Inc. por fallos inadecuados en el programa contra el lavado de capitales y el cumplimiento de monedas virtuales en la plataforma de Cash App," (10 de abril de 2025) https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202504101.

Giros postales

Un giro postal es un instrumento monetario prepagado que el beneficiario puede negociar igual que lo haría con un cheque. Los giros postales suelen comercializarse a consumidores sin bancarización o con pocos ingresos, vendidos en oficinas de correos y agentes de MSB, como Western Union y MoneyGram, además de bancos. A diferencia de los cheques personales, el comprador de un giro postal no está obligado a mantener una cuenta bancaria. Los giros postales no pueden ser rebotados porque el remitente ha pagado la cantidad total en el momento de la compra, y normalmente se emiten con un valor individual máximo de hasta 1.000 dólares.

Los giros postales siguen siendo explotados para blanquear los ingresos de una amplia variedad de delitos. Pueden resultar atractivas para los delincuentes por varias razones: los giros postales ofrecen una forma de convertir fondos ilícitos en un instrumento monetario que no es intrínsecamente sospechoso porque el valor se paga por adelantado y se garantiza, lo que los convierte en efectivo para muchos fines; pueden adquirirse de forma anónima en miles de agencias de todo el país; pueden comprarse con efectivo en grandes cantidades en cadenas consecutivas numeradas de giros postales que suman menos de 3.000 dólares; no caducan; y pueden ser físicamente más ligeras que un valor equivalente en efectivo. El número de SARs presentados por instituciones financieras en relación con giros postales ha caído casi un 30 por ciento entre 2021 y 2024, lo que sugiere un posible descenso en su uso para financiación ilícita. [334]

Los riesgos asociados a los giros postales se mitigan parcialmente porque los emisores o vendedores de giros postales están sujetos a los requisitos de la BSA. Los emisores o vendedores de giros postales se clasifican como MSB si venden o emiten giros postales por una cantidad superior a 1.000 dólares a cualquier persona en cualquier día en una o más transacciones.[335] Como MSB, emisores y vendedores están sujetos a ciertos requisitos de registro, registro, programa AML e informes conforme a la BSA y sus normativas de implementación, incluyendo la presentación de SAR y CTRs.[336] Para compras en divisas de 3.000 dólares o más (incluyendo compras múltiples de giros postales individuales que suman 3.000 dólares o más), los emisores y vendedores deben verificar y registrar la identidad del comprador; sin embargo, esa información no se valida necesariamente de forma instantánea o retroactiva, lo que los actores ilícitos explotan usando identificación falsa o sintética. [337]

Una revisión de los casos policiales de los últimos dos años revela que giros postales a veces se utilizan para blanquear fondos ilícitos u obtenidos fraudulentamente, como los beneficios del ciberdelito o el tráfico de drogas. Los giros postales son utilizados por los delincuentes para estructurar y eludir los umbrales de registro e informes como parte del blanqueo de ingresos ilícitos.[338] Tras comprar giros postales con fondos ilícitos, los delincuentes depositan los fondos en sus propias cuentas o en las de cómplices, a veces utilizando cuentas bancarias abiertas con identidades robadas.[339] Una vez depositados en el sistema financiero, los ingresos de los giros postales pueden transferirse a otras cuentas bancarias, usarse para comprar artículos de lujo o reinvertirse en la empresa criminal.

Seguros

Los productos de seguros suponen un menor riesgo de blanqueo de capitales que otros productos financieros porque generalmente se mantienen durante largos periodos y no son suficientemente flexibles para el blanqueo de ingresos ilícitos.[340] Las compañías de seguros que ofrecen productos cubiertos, como ciertas anualidades y productos de seguro de vida, están sujetas a la BSA y se someten regularmente a exámenes AML/CFT y tienen obligaciones de presentación de SAR, lo que mitiga aún más el dinero

334 instituciones financieras presentaron 478.568 y 336.832 SARs en relación con giros postales en 2021 y 2024, respectivamente. A fecha de 30 de noviembre de 2025, han presentado 271.558 SAR, continuando una tendencia decreciente. FinCEN, "Estadísticas de informes de actividad sospechosa (SAR Stats)", https:// www.fincen.gov/reports/sar-stats.

335 31 C.F.R. § 1010.100(ff)(3).

336 31 C.F.R. § 1022.210, 1010.311, 1022.320.

337 31 C.F.R. § 1010.415 338 *Véase, por ejemplo,* DOJ, "Raymore Man Sentenceed for Narnarcotrafficing, Illegal Fireguns," (13 de diciembre de 2024) https://www.justice.gov/usao- wdmo/pr/raymore-man-sentenciado-narcotráfico-ilegal-armas de fuego.

339 *Véase, por ejemplo,* DOJ, "Hombre y mujer del condado de Wyoming sentenciados por evadir los requisitos de información financiera," (21 de octubre de 2024) https://www.justice.gov/usao-sdwv/pr/wyoming-county-man-and-raleigh-county-woman-sentenced-evading-financial- informe.

340 Véase el GAFI, "Guía para un enfoque basado en el riesgo: Sector de seguros de vida," (2018), p. 9, https://www.fatf-gafi.org/content/dam/fatf-gafi/ guía/RBA-Life-Insurance.pdf.coredownload.pdf.

Riesgo de blanqueo. En 2024, las compañías de seguros y las instituciones depositarias presentaron algo más de 1.000 SARs relacionadas con actividades sospechosas relacionadas con productos de seguro cubiertos. [341]

Cuando se utilizan productos de seguro cubiertos para blanquear ingresos ilícitos, el delito subyacente suele ser el fraude, a veces relacionado con el propio producto cubierto. Por ejemplo, en julio de 2025, un matrimonio y una mujer fueron condenados a 12 y cuatro años de prisión, respectivamente, tras ser condenados por un esquema de fraude de seguros. Según documentos judiciales y pruebas presentadas en el juicio, la pareja conspiró para defraudar a las compañías de seguros obteniendo más de 40 pólizas de seguro de vida para solicitantes al falsear su cobertura de salud, patrimonio y seguro de vida existente. El total de beneficios por fallecimiento de estas pólizas superó los 20 millones de dólares. Para ocultar el fraude, la pareja transfirió el dinero que ganaron a través de múltiples cuentas bancarias, incluidas cuentas a nombre de fideicomisos. [342]

XII. Entidades y Acuerdos Legales

Los actores ilícitos suelen abusar de entidades y acuerdos legales para blanquear beneficios ilícitos, aunque la sofisticación de los planes individuales varía mucho según el delito subyacente, la ubicación de los perpetradores, la ubicación de la entidad o acuerdo legal y el grado en que los perpetradores intenten disfrazar sus identidades.

Empresas pantalla

Las empresas pantalla[343] son entidades empresariales legales que no tienen presencia física, pocos o ningún empleado y generan poco o ningún valor económico independiente. Generalmente se organizan como sociedades de responsabilidad limitada (LLC) o sociedades porque esas entidades son fáciles y económicas de constituir y administrar. La mayoría de las empresas pantalla en Estados Unidos son legítimas y se utilizan porque pueden limitar la responsabilidad, facilitar fusiones y adquisiciones, ayudar en la planificación fiscal y proporcionar privacidad. Como la mayoría de las empresas estadounidenses, las empresas pantalla suelen constituirse bajo la ley estatal.

Las empresas pantalla se utilizan en esquemas de blanqueo de capitales porque pueden permitir que actores ilícitos presenten transferencias ilícitas como actividad empresarial legítima y oculten su identidad cuando son propiedad de mulas de dinero o nominados. Esto puede dificultar que las instituciones financieras eviten que actores ilícitos hagan un mal uso de sus productos y servicios, y que las fuerzas del orden identifiquen a los responsables de actividades ilícitas. Durante el periodo de evaluación, las empresas pantalla se utilizaron para facilitar varios tipos diferentes de delitos financieros, incluyendo evadir sanciones, pagar y recibir sobornos, defraudar programas sanitarios y blanquear los beneficios del tráfico de drogas, ciberdelincuencia y esquemas de fraude, entre otros delitos.

Las empresas pantalla nacionales se utilizan en esquemas de blanqueo de capitales de terceros, como aquellos que involucran mulas de dinero y CMLNs, porque los delincuentes creen que pueden mover más fondos a través de una institución financiera cuando las transacciones se disfrazan de pagos empresariales. Sin embargo, las instituciones financieras suelen ser hábiles identificando e informando sobre actividades de blanqueo de capitales que involucran a empresas pantalla, y las fuerzas del orden pueden utilizar esos informes para desmantelar los esquemas. En un caso, seis miembros de un prolífico CMLN, incluidos cuatro ciudadanos chinos, se declararon culpables de cargos de blanqueo de capitales relacionados con el tráfico de drogas. Según documentos judiciales, el CMLN blanqueó más de 92 millones de dólares en fondos ilícitos. El organizador ordenó a un grupo de mensajeros que recogieran grandes cantidades de dinero procedentes de actividades ilegales, incluido el tráfico de narcóticos, de particulares de todo Estados Unidos. Los mensajeros depositaban estos fondos ilícitos, que generalmente superaban los 10.000 dólares, en cuentas bancarias de empresas pantalla

341 compañías de seguros y instituciones depositarias, respectivamente, presentaron 696 y 372 SARs relacionadas con productos de seguros en 2024. FinCEN, "Estadísticas de Informes de Actividad Sospechosa (SAR Stats)", https://www.fincen.gov/reports/sar-stats.

342 DOJ, "Pareja de Maryland condenada por esquema de fraude de seguros de 20 millones de dólares," (8 de julio de 2025) https://www.justice.gov/opa/pr/maryland-couple- sentenciado-esquema de fraude de seguros de 20 años.

Las empresas 343 Shelf son un tipo de empresa pantalla creada sin un propósito inmediato y puesta en la "estantería" para envejecer. Los actores legítimos pueden comprar empresas de estantería para evitar tener que crear las suyas propias o acceder a actividades comerciales en una determinada jurisdicción. Los actores ilícitos también pueden comprar empresas de estantería para que su actividad parezca más legítima.

controlados por la CMLN para ocultar la naturaleza de los fondos ilícitos. [344]

Las empresas pantalla extranjeras presentan riesgos elevados para la seguridad nacional y las finanzas ilícitas porque a menudo son utilizadas por actores amenazantes que operan desde jurisdicciones autorizadas, como Irán, y porque su uso puede permitir que actores ilícitos expatrien ingresos ilícitos fuera del alcance de las fuerzas del orden estadounidenses.[345] Las fuerzas del orden estadounidenses disponen de una amplia gama de herramientas que pueden emplear para identificar a los beneficiarios beneficiarios de entidades legales estadounidenses, como a través de registros estatales, datos del IRS, bases de datos comerciales y registros en manos de instituciones financieras u otras empresas, pero identificar a los propietarios beneficiarios de empresas fantasma extranjeras o de propiedad extranjera mediante solicitudes de asistencia legal mutua puede llevar años o incluso estar prohibido por las leyes de privacidad de datos de un país extranjero. Según las normativas de FinCEN, ciertas entidades jurídicas extranjeras están obligadas a informar sobre la titularidad beneficiaria (BOI). [346]

Los siguientes casos demuestran cómo actores ilícitos utilizan empresas pantalla extranjeras para perpetrar varios tipos de delitos financieros, incluyendo financiación por proliferación, fraude y soborno:

Financiación de la proliferación: En abril de 2025, se desclasificó una denuncia que acusaba a dos ciudadanos iraníes y a una empresa iraní de conspirar para adquirir piezas estadounidenses para vehículos aéreos no tripulados (UAVs, también conocidos como drones), conspirar para proporcionar apoyo material al Cuerpo de Guardias Revolucionarias Islámicas (IRGC)— una organización designada para la FTO— y conspirar para cometer blanqueo de capitales. Según documentos judiciales, los demandados utilizaron diversas empresas pantalla o empresas pantalla para pagar piezas de UAV y para ocultar el verdadero destino final y la verdadera identidad de los usuarios autorizados, incluido el IRGC, que adquiría piezas fabricadas en EE. UU. a través de la empresa iraní. Los hombres utilizaron al menos tres empresas pantalla, todas con sede en los EAU, para pagar a una empresa con sede en la RPC que enviaba facturas a la empresa iraní por la venta de motores. Esos pagos se procesaban a través de cuentas bancarias de corresponsales con sede en EE. UU. Los hombres también utilizaron dos de estas empresas pantalla para pagar a una empresa separada con sede en la RPC por la venta de mástiles neumáticos, un componente de operación de drones. [347]

Estafas de inversión en activos digitales: En septiembre de 2025, un hombre de California fue condenado a 51 meses de prisión federal por su papel en el blanqueo de más de 36,9 millones de dólares de víctimas en una conspiración internacional de estafa de inversión en activos digitales llevada a cabo desde centros de estafa en Camboya. Según documentos judiciales, el hombre era copropietario de la empresa Axis Digital Limited, con sede en las Bahamas. Se transfirieron más de 36,9 millones de dólares en fondos de las víctimas desde cuentas bancarias estadounidenses controladas por los co-conspiradores a una única cuenta en Deltec Bank en las Bahamas, abierta a nombre de Axis Digital Limited. El hombre y otros co-conspiradores ordenaron a Deltec Bank convertir los fondos de las víctimas en stablecoins y transferir esos fondos convertidos a una cartera de activos digitales controlada por particulares en Camboya. [348]

344 DOJ, "Los tres miembros finales acusados en un prolífico esquema chino de blanqueo de capitales se declaran culpables de blanquear decenas de millones en ingresos por drogas," (7 de julio de 2025) https://www.justice.gov/opa/pr/final-three-members-charged-prolific-chinese-money-laundering-scheme se declaran culpables de blanqueo.

345 Como se ha señalado respecto a las empresas pantalla nacionales, muchas empresas pantalla extranjeras son legítimas y se utilizan porque pueden limitar la responsabilidad, facilitar fusiones y adquisiciones, ayudar en la planificación fiscal y proporcionar privacidad. Por ejemplo, es común que las estructuras de fondos privados cuenten con un vehículo de fondos offshore que facilite inversiones fiscalmente eficientes por parte de inversores estadounidenses exentos de impuestos.

346 FinCEN, "Revisión de requisitos de reporte de información sobre titularidad beneficiaria y prórroga de plazo," (Norma Final Interina, 90 FR 13688, 13697 (26 de marzo de 2025) https://www.federalregister.gov/documents/2025/03/26/2025-05199/beneficial-ownership-information- revisión de requisitos de reporte y prórroga-plazo.

347 DOJ, "Compañía iraní y dos ciudadanos iraníes acusados de conspirar para proporcionar apoyo material al Cuerpo de Guardias Revolucionarias Islámicas (IRGC) y de un plan para adquirir tecnología estadounidense para drones de ataque iraníes," (1 de abril de 2025) https://www.justice.gov/opa/ pr/empresa-iraní-y-dos-ciudadanos-iraníes-acusados-de-conspirar-proporcionar-apoyo-material. *Véase también,* Tesorería, "Los Departamentos del Tesoro y de Justicia Actúan contra la Red de Adquisición de Armas Iraní" (1 de abril de 2025) https://home.treasury.gov/news/ comunicados de prensa/sb0066.

348 DOJ, "Hombre de California condenado por su papel en conspiración de estafa global de inversión en activos digitales que resultó en robo de más de 36,9 millones de dólares a víctimas," (8 de septiembre de 2025) https://www.justice.gov/opa/pr/california-man-sentenced-role-global-digital-asset-investment estafa-conspiración-resultante.

Pago de sobornos: En marzo de 2024, Gunvor S.A. (Gunvor), parte del Grupo Gunvor, una de las mayores firmas de comercio de materias primas del mundo, se declaró culpable de un cargo de conspiración para violar la Ley de Prácticas Corruptas en el Extranjero (FCPA). Según las confesiones de la empresa y documentos judiciales, entre 2012 y 2020, Gunvor y sus cómplices pagaron más de 97 millones de dólares a intermediarios, entendiendo que parte del dinero se usaría para sobornar a numerosos funcionarios ecuatorianos. Los pagos de sobornos se encaminaban a través de bancos en Estados Unidos mediante empresas pantalla en Panamá y las Islas Vírgenes Británicas controladas por los co-conspiradores de Gunvor. A cambio de estos sobornos, altos funcionarios ecuatorianos ayudaron a Gunvor a conseguir contratos para conceder una serie de préstamos respaldados por petróleo a Petroecuador. En total, Gunvor obtuvo más de 384 millones de dólares en beneficios del negocio que obtuvo corruptamente relacionado con Petroecuador. [349]

Fraude en beneficios gubernamentales: En noviembre de 2025, un hombre fue condenado a 10 años de prisión por su papel en el caso de 300 millones de dólares Feeding Our Future en Minnesota, el mayor esquema de fraude por COVID-19 en Estados Unidos. Como se demostró en el juicio, el hombre y sus coacusados robaron más de 47 millones de dólares en fondos de programas al afirmar servir 18 millones de comidas a niños en más de 30 puntos de distribución de alimentos. El hombre y sus cómplices participaron en una conspiración para blanquear los beneficios de su esquema de fraude utilizando una serie de empresas pantalla tanto en Estados Unidos como en Kenia. El hombre ayudó a distribuir millones de dólares en ingresos fraudulentos entre sus entidades de blanqueo de capitales. El hombre también creó su propia empresa pantalla que utilizó para recibir y blanquear su parte de los beneficios del fraude disfrazándolos de "consultoría" y pagos similares. En total, el hombre utilizó su empresa pantalla para recibir más de 900.000 dólares en fondos de fraude. [350]

El Tesoro también sigue supervisando los esfuerzos de los socios extranjeros para recopilar el BOI y utilizar eficazmente esos datos para investigar y procesar casos que involucran a empresas pantalla. Algunos países, por ejemplo, han establecido registros BOI y requisitos de recaudación más completos, pero esto puede no mitigar completamente el riesgo, ya que vastas bases de datos de información enviada por los usuarios pueden contener datos de registro fraudulentos, inexactos, vagos o usados repetidamente.

A nivel nacional, la Regla CDD de FinCEN y la implementación personalizada de la Ley de Transparencia Corporativa (CTA) han mejorado la capacidad de acceder a la BOI e identificar y detener actividades delictivas. La norma CDD entró en vigor en 2018 y exige que ciertas instituciones financieras identifiquen y verifiquen la identidad de los beneficiarios beneficiarios cuando un cliente de la entidad legal abre por primera vez una cuenta en dicha entidad. Las fuerzas del orden pueden acceder a esta información en determinadas circunstancias, lo que lleva a investigaciones rápidas sobre delitos financieros. Promulgada como parte de la Ley Anti-Blanqueo de Capitales de 2020 (Ley AML), la CTA exige que las "empresas informantes" específicas proporcionen BOI a FinCEN, incluso en el momento de la creación o registro. FinCEN almacena estos datos en una base de datos segura, a la que pueden acceder ciertas agencias policiales para facilitar las investigaciones. En marzo de 2025, FinCEN emitió una norma provisional final que define a las empresas informantes como entidades formadas bajo la ley de un país extranjero y registradas para operar en Estados Unidos.[351] Esta revisión reflejaba los hallazgos de FinCEN sobre el aumento de los riesgos de seguridad nacional y financiación ilícita que plantean los actores ilícitos extranjeros, como demuestran los ejemplos de casos anteriores. Estas empresas informantes debían presentar BOI a FinCEN con efecto a partir del 25 de abril de 2025.

Regular a las entidades legales para combatir el blanqueo de capitales requiere un equilibrio entre proteger el sistema financiero de actividades ilícitas y evitar una carga indebida para las empresas legítimas, especialmente para las más pequeñas. A pesar del mal uso de empresas pantalla nacionales y extranjeras por parte de actores ilícitos, que probablemente no se dejarían intimidar por

349 DOJ, "Gunvor S.A. se declara culpable de conspirar para sobornar a funcionarios ecuatorianos y se le ordena pagar más de 600 millones de dólares en sanciones penales," (1 de marzo de 2024) https://www.justice.gov/usao-edny/pr/gunvor-sa-pleads-guilty-scheme-bribe-ecuadorian-officials-and-ordered-pay- más de 600.

350 DOJ, "Alimentando a nuestro futuro acusado condenado a 10 años de prisión," (24 de noviembre de 2025) https://www.justice.gov/usao-mn/pr/ que alimenta a nuestro futuro acusado condenado a 10 años de prisión.

351 FinCEN, "Revisión de requisitos de reporte de información sobre titularidad beneficiaria y prórroga de plazo," (Provisional Final Rule, 90 FR 13688, 13697 (26 de marzo de 2025)) https://www.federalregister.gov/documents/2025/03/26/2025-05199/beneficial-ownership-information-revisión-requisito-de reporte y-prórroga-plazo.

incluso en los regímenes regulatorios más estrictos, las fuerzas del orden estadounidenses, en su enfoque de seguir el dinero, han sido, y seguirán siendo, el líder mundial en desmantelar la propiedad de los nominados, incluso en casos transfronterizos de blanqueo de capitales.

Empresas pantalla

En el contexto de la financiación ilícita, las empresas pantalla son entidades legales que proporcionan bienes o servicios legítimos y utilizan esa actividad económica como una "tapadera" para disfrazar actividades ilícitas. Como se ha descrito anteriormente, las empresas pantalla tienen varios usos legítimos, mientras que las empresas pantalla, por definición, siempre están involucradas en actividades ilícitas. Las instituciones financieras y auditores suelen ser capaces de identificar transacciones anómalas indicativas de blanqueo de capitales en empresas pantalla, obligando a los blanqueadores de dinero a fabricar documentos o hacer declaraciones falsas para explicar dichas operaciones. Según las regulaciones de FinCEN que implementan la CTA, las empresas pantalla que cumplan la definición de empresa informante estarían obligadas a informar a la BOI. Las empresas pantalla pueden utilizarse para evadir sanciones y blanquear los beneficios ilícitos del fraude y el tráfico de drogas, entre otros delitos. [352]

En un caso, según las acusaciones contenidas en la acusación, el director financiero de una empresa multinacional de medios conspiró con otros para participar en un extenso esquema transnacional para blanquear al menos aproximadamente 67 millones de dólares de fondos obtenidos ilegalmente a cuentas bancarias a nombre de la empresa mediática y entidades relacionadas (colectivamente, las "Entidades Mediáticas"). Los participantes del esquema utilizaron activos digitales para comprar conscientemente decenas de millones de dólares en ingresos del delito, incluidos beneficios fraudulentos del seguro de desempleo, que se habían cargado en decenas de miles de tarjetas de débito prepago. Una vez comprados los ingresos del delito, los participantes del esquema usaron la información personal robada para abrir cuentas, incluyendo cuentas de tarjetas de débito prepago, cuentas de activos digitales y cuentas bancarias, que se utilizaron para transferir los ingresos del delito a cuentas bancarias asociadas a las Entidades de Medios. Cuando los bancos, incluidos dos bancos con sede en EE. UU., preguntaron al director financiero sobre el aumento de transacciones que entraban en las cuentas bancarias de las entidades mediáticas, el director financiero mintió, alegando que el aumento de fondos provenía de donaciones. [353]

Fideicomisos

Los fideicomisos son relaciones en las que una persona posee el título de una propiedad y está sujeta a la obligación de conservar o utilizar la propiedad en beneficio de otra.[Los fideicomisos 354] se forman bajo la ley estatal y se utilizan ampliamente para fines legítimos, especialmente en planificación patrimonial y fiscal. Permiten a familias y empresas gestionar los activos de forma discreta, proteger los intereses de menores o beneficiarios con poca experiencia financiera y, en el caso de herencias, evitar la sucesión y, en algunas circunstancias, reducir las obligaciones fiscales.

Los fideicomisos establecidos en el extranjero (fideicomisos extranjeros) que se conectan con el sistema financiero estadounidense, especialmente aquellos utilizados para poseer activos como bienes raíces, representan el mayor riesgo de blanqueo de capitales. Los fideicomisos extranjeros suelen limitar el acceso de las fuerzas del orden a la titularidad beneficiaria y a la información relacionada, aumentando su vulnerabilidad a la evasión de sanciones y permitiendo el lavado de los beneficios ilícitos de un delito subyacente con un nexo extranjero, como la corrupción o el fraude.[355] Aunque las fuerzas del orden han identificado cierto uso indebido de fideicomisos establecidos en Estados Unidos (fideicomisos domésticos) relacionados con fraudes

352 *Véase, por ejemplo,* DOJ, "Ciudadano venezolano y ciudadano estadounidense arrestados por evasión de sanciones y contrabando en esquema para abastecer a la industria estatal del acero de Venezuela," (16 de junio de 2025) https://www.justice.gov/opa/pr/venezuelan-national-and-us-citizen-arrested-sanctions- esquema de evasión y contrabando-suministro; DOJ, "Empresario de Michigan condenado a tres años de prisión por blanqueo de dinero y obstrucción al IRS," (4 de marzo de 2024) https://www.justice.gov/archives/opa/pr/michigan-business-owner-sentenced-three-years- prisión de blanqueo de dinero y obstrucción del IRS; DOJ, "Ciudadano mexicano condenado a más de cinco años de prisión por conspirar para traficar cocaína y blanqueo de capitales," (4 de septiembre de 2025) https://www.justice.gov/usao-ma/pr/mexican-national-sentenced-more- cinco años de prisión por conspiración por tráfico de cocaína y dinero.

353 DOJ, "Director Financiero de una Empresa Multinacional de Medios acusado de participar en un esquema para blanquear al menos 67 millones de dólares en ingresos por fraude," (3 de junio de 2024) https://www.justice.gov/usao-sdny/pr/chief-financial-officer-multinational-media-company-charged-esquema participante; 354 IRS, "Definición de fideicomiso," (actualizado el 30 de enero de 2025) https://www.irs.gov/charities-non-profits/definition-of-a-trust. 355 *Véase, por ejemplo,* DOJ, "Tribunales federales autorizan citaciones 'John Doe' del IRS a entidades del fideicomiso Trident," (30 de enero de 2025) https://www.justice. gov/opa/pr/federal-courts-authorize-irs-john-doe-summonses-trident-trust-entities.

Frente a un beneficiario o delitos fiscales, los fideicomisos nacionales tienen un perfil de riesgo general menor en materia de blanqueo de capitales y evasión de sanciones, ya que requieren conocimientos especializados para establecerlos y administrarlos. Los actores financieros ilícitos suelen elegir métodos menos complejos y que requieren mucho tiempo, ya que los fideicomisos suelen involucrar a varias partes, como el constituyente, el fiduciario y los beneficiarios. A diferencia de los fideicomisos extranjeros, las fuerzas del orden pueden solicitar información sobre fideicomisos nacionales, como información sobre constituyentes o beneficiarios, a través de canales judiciales o administrativos.

Además, debido a la Regla CDD, las instituciones financieras cubiertas están obligadas a tener políticas y procedimientos de CDD basados en el riesgo que consideren a fideicomisos y fiduciarios. Por ejemplo, generalmente se espera que los fiduciarios informen a las instituciones financieras cubiertas de su estatus como fiduciarios durante el proceso de apertura de cuenta. Además, independientemente de dónde se forme un fideicomiso, si hay personas estadounidenses que puedan ser constituyentes o beneficiarios, o que realicen transacciones tanto con ingresos de origen estadounidense como con ciertos ingresos extranjeros, el fideicomiso podría seguir sujeto a obligaciones fiscales federales ante el IRS.[356] Estos requisitos crean transparencia adicional para cualquier fideicomiso con un nexo estadounidense. La administración de fideicomisos también sigue sujeta a estatutos estatales o territoriales y a la supervisión judicial. Muchos estados también exigen declaraciones de impuestos o de sucesiones para fideicomisos con vínculos locales. Las obligaciones fiduciarias del common law, como los deberes de lealtad, prudencia, imparcialidad, conservación de registros y divulgación, se aplican a los fiduciarios. Estas obligaciones legales ofrecen recursos contra el abuso y aumentan la rendición de cuentas. La norma del Tesoro sobre transferencias de bienes raíces residenciales no financiados por fideicomisos o entidades legales, que entra en vigor el 1 de marzo de 2026, exigirá la presentación de información sobre titularidad beneficiaria en la mayoría de las transacciones inmobiliarias residenciales no financiadas en Estados Unidos.[357] La norma reduce significativamente la capacidad de los actores ilícitos para blanquear los ingresos a través de bienes inmuebles estadounidenses mantenidos en estructuras de fideicomisos.

La creación y administración de fideicomisos suele estar vinculada a los guardianes descritos en la siguiente sección. Por ejemplo, en diciembre de 2025, una persona estadounidense natural accedió a pagar 1.092.000 dólares para resolver una posible responsabilidad civil ante la OFAC por aparentes violaciones de sanciones relacionadas con Ucrania y Rusia. La persona es abogada y exfuncionaria del gobierno de EE. UU. La conducta que dio lugar a las aparentes violaciones tuvo lugar entre 2018 y 2022, cuando la persona ejerció como fiduciario del fideicomiso familiar de un oligarca ruso autorizado. Durante el tiempo que la persona fue fiduciaria, autorizó la transferencia de activos del fideicomiso, pagó a varios proveedores de servicios en nombre del fideicomiso y autorizó diversas acciones sustantivas tomadas por el fideicomiso, lo que resultó en un total de 122 aparentes violaciones del Reglamento de Sanciones Relacionadas con Ucrania y Rusia. [358]

XIII. Guardianes

Los guardianes son profesionales y entidades de confianza que pueden ayudar a sus clientes a acceder al sistema financiero. Aunque estas entidades pueden tener algunas obligaciones federales o estatales de AML/CFT, no están sujetas a requisitos integrales de AML/CFT y pueden ser explotadas por actores ilícitos en esquemas de blanqueo de capitales, de forma involuntaria o involuntaria. Ciertos guardianes se enfrentan a una amplia gama de riesgos de blanqueo de capitales que están influenciados por su base de clientes, los servicios ofrecidos y su huella geográfica, entre otros factores. Esta evaluación de riesgos analiza el riesgo que representan cuatro de los mayores sectores guardianes de Estados Unidos que podrían ser explotados para delitos financieros.

356 Generalmente, el fiduciario del fideicomiso nacional no otorgante está obligado a presentar el Formulario 1041 (Declaración de la Renta de EE. UU. para Patrimonios y Fideicomisos) para declarar los ingresos del fideicomiso, si los hay. Se requieren formularios fiscales específicos que identifiquen a los beneficiarios del fideicomiso y declaren su parte de ingresos para un año fiscal si se realizan distribuciones. El fiduciario de un fideicomiso extranjero no otorgante generalmente está obligado a presentar el Formulario 1040-NR (Declaración de la Renta de Extranjeros No Residentes de EE. UU.) para declarar ingresos de origen estadounidense y ciertos ingresos extranjeros, si los hay. Un fideicomiso extranjero con un propietario estadounidense también debe presentar el Formulario 3520-A (Declaración Anual de Información de Fideicomiso Extranjero con un Propietario de EE. UU.).

357 FinCEN, "Preguntas frecuentes sobre la norma de bienes raíces residenciales," (actualizado el 18 de diciembre de 2025) https://www.fincen.gov/rre-faqs. 358 OFAC, "OFAC llega a un acuerdo con un individuo por 1.092.000 dólares relacionados con aparentes violaciones de sanciones relacionadas con Ucrania/Rusia," (9 de diciembre de 2025) https://ofac.treasury.gov/media/934806/download?inline.

El informe de julio de 2024 del GAFI de julio de 2024 "Revisión Horizontal del Cumplimiento Técnico de los Guardianes de la Corrupción" define a los guardianes por sector, específicamente 1) abogados, notarios y otros profesionales legales independientes, 2) contables, 3)

proveedores de servicios fiduciarios y empresariales, y 4) agentes inmobiliarios, que son empresas y profesiones no financieras designadas que pueden realizar tareas financieras específicas para clientes (véase "Las Recomendaciones del GAFI, " (actualizado octubre de 2025), pp. 19-21, https://www.fatf-gafi.org/content/dam/fatf-gafi/recomendaciones/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf).

Abogados

Los abogados en Estados Unidos pueden suponer un riesgo de blanqueo de capitales cuando actúan como intermediarios entre los clientes y el sistema financiero, como gestionando los fondos de los clientes; crear, operar o gestionar entidades legales de clientes; O comprar y vender bienes raíces. Al realizar estos servicios, los abogados pueden ayudar a los clientes a blanquear dinero ocultando el origen de los ingresos ilícitos. En comparación con otros profesionales que ofrecen servicios similares, los abogados pueden facilitar este blanqueo con mayor facilidad debido a la opacidad que ofrece el privilegio abogado-cliente y el deber de confidencialidad del abogado. Aunque la promoción de actos delictivos por parte de abogados no está cubierta por este privilegio (la "excepción al fraude delictivo"), esta limitación es aplicada de forma restrictiva por los tribunales y la existencia de la excepción no resulta, por sí sola, en la divulgación de casos de financiación ilícita facilitada por abogados a las fuerzas del orden.

Aunque los abogados en Estados Unidos no están sujetos a regulaciones integrales de AML/CFT, están sujetos a ciertas prácticas éticas destinadas a disuadir la financiación ilícita en el sector legal y, debido a la dependencia del sector de servicios financieros altamente regulado para realizar transacciones, existen medidas como la CDD y la notificación de actividades sospechosas, en instituciones financieras cubiertas que ayudan a mitigar riesgos financieros ilícitos en el sector legal. En particular, la American Bar Association (ABA), que es una organización voluntaria dirigida por sus miembros, mantiene una serie de Reglas Modelo de Conducta Profesional (las Reglas Modelo). Muchos colegios de abogados estatales basan sus normas de conducta profesional en las Reglas Modelo. Como se discute en la NMLRA de 2024, en 2023 las Normas Modelo se modificaron para incluir los riesgos de blanqueo de capitales entre los factores que un abogado debe considerar a la hora de decidir si rechazar o retirarse de la representación de un cliente. En agosto de 2024, la ABA emitió su primera guía sobre las enmiendas de 2023, señalando una "obligación implícita de llevar a cabo una investigación razonable basada en el riesgo, no una superficial ni una que implique una operación de tipo red para descubrir cada hecho sobre cada cliente." [360]

Un área de riesgo particular es la "Participación en las Cuentas Fiduciarias de Abogados" (IOLTAs),[que] son cuentas agrupadas con intereses y que son cuentas agrupadas que mantiene un abogado en nombre de sus clientes. Los abogados y despachos de abogados utilizan IOLTAs, que son obligatorios por la mayoría de las leyes estatales y las normas de responsabilidad profesional, para gestionar los fondos fiduciarios de los clientes. Las instituciones financieras que poseen IOLTAs normalmente solo conocen la identidad del abogado cuyo nombre lleva el título de la IOLTA y no conocen la identidad de los clientes subyacentes que son los verdaderos propietarios de los fondos. Dada la limitada visibilidad de los bancos sobre el verdadero propietario y origen de los fondos, un abogado que permita a los clientes usar su cuenta para mover ingresos ilícitos puede evitar o retrasar alertas en el banco.

En un caso, un abogado fue condenado a nueve meses de prisión federal por transferir a sabiendas y ayudar y facilitar la transferencia de 3 millones de dólares para impedir la incautación legal de los fondos. Las pruebas obtenidas en la investigación revelaron que el abogado ordenó, ayudó y facilitó la transferencia de 3 millones de dólares para sus clientes tras la ejecución de órdenes federales de registro e incautación en California. El abogado ordenó la transferencia de una cuenta en las Bahamas a su cuenta fiduciaria, y posteriormente combinó los fondos para su uso personal. [362]

Aunque las normas de los colegios de abogados estatales rigen las IOLTA, estas normas generalmente están destinadas a proteger a los clientes e imponer obligaciones a los abogados de no hacer un mal uso de los fondos de la IOLTA. A pesar de estas normas de conducta profesional, algunos abogados han abusado de las IOLTAs para defraudar a sus clientes. Por ejemplo, en marzo de 2025, un abogado fue condenado a más de cinco años de prisión federal por blanqueo de capitales y fraude electrónico. Según la declaración de culpabilidad, el acusado ejerció como abogado con licencia para ejercer en Nueva York, Pensilvania y Nueva Jersey, y fue socio designado en un bufete. Durante varios años, el demandado hizo creer a los clientes que tenían acceso inmediato al dinero en dos cuentas de despacho de abogados IOLTA, pero el abogado estaba ordenando a los empleados que transfirieran el dinero de los clientes a otras cuentas que él controlaba. El esquema causó más de 2,4 millones de dólares en pérdidas a los clientes del bufete. El abogado utilizó los fondos robados para pagar gastos personales. [363]

360 ABA, "Opinión formal 513: Deber de investigar y evaluar los hechos y circunstancias de cada representación," (23 de agosto de 2024), p. 7, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-513.PDF. Énfasis en el original.

361 Véase ABA, "Resumen de IOLTA" (consultado el 17 de diciembre de 2025) https://www.americanbar.org/groups/interest_lawyers_trust_accounts/overview/.

362 DOJ, "Abogado jefe de Hilton sentenciado por transferir a sabiendas 3 millones de dólares para impedir la incautación legal de los fondos," (21 de febrero de 2025) https://www.justice.gov/usao-sc/pr/hilton-head-lawyer-sentenced-knowingly-transferring-3m-prevent-lawful-seizure-funds.

363 DOJ, "Abogado de California condenado a más de cinco años de prisión federal por fraude electrónico y blanqueo de dinero," (7 de marzo de 2025)

https://www.justice.gov/usao-md/pr/california-lawyer-sentenced-more-five-years-federal-prison-wire-fraud-and-money.

Contables

Los contables estadounidenses presentan un bajo nivel de riesgo de blanqueo de capitales porque, a diferencia de otras jurisdicciones, generalmente ofrecen servicios de gestión o asesoramiento financiero en lugar de gestionar o mantener fondos de clientes, comprar bienes raíces o establecer empresas o fideicomisos.[364] Aunque los contables podían facilitar esquemas financieros ilícitos debido a su conocimiento del sistema financiero, no conservan ninguna capacidad especial para registrar empresas, abrir cuentas bancarias o autorizar transacciones financieras no accesibles para ciudadanos comunes. En los últimos diez años, los contables rara vez han sido implicados en casos en los que han utilizado sus habilidades profesionales para ofrecer servicios de blanqueo de capitales a terceros. Cuando se acusa a contables de blanqueo de capitales, suele ser en conjunto con fraude o malversación perpetrada contra un cliente o el gobierno. [365]

Procesadores de pagos de terceros

Los procesadores de pagos, también conocidos como procesadores de pagos externos, actúan como intermediarios en transacciones no en efectivo — como tarjetas de crédito y débito, ACH y transacciones con monedero móvil— permitiendo a los comerciantes aceptar pagos de clientes tanto en línea como en persona sin necesidad de contar con su propia cuenta bancaria. Los procesadores de pagos son clientes de los bancos. Operan entre comerciantes e instituciones financieras y facilitan la transmisión de datos de transacciones, autorizaciones y liquidaciones, y a menudo ofrecen servicios adicionales como detección de fraude y gestión de contracargos, cifrado y seguridad, y análisis de datos. Dado el aumento de pequeños comercios electrónicos, especialmente desde la pandemia de COVID-19; el crecimiento de las transacciones con tarjetas de crédito, débito y carteras digitales; Y la aparición de nuevos esquemas de pago como "Compra ahora, paga después", el mercado de procesadores de pagos ha ido creciendo y se espera que siga creciendo rápidamente en los próximos años. [366]

Según las normativas de implementación de la BSA y FinCEN, los procesadores de pagos pueden estar exentos de cumplir con la definición de MSB si cumplen ciertos criterios.[367] En una resolución administrativa del FinCEN de 2013 que describe las exenciones regulatorias de la definición de MSB (es decir, no un transmisor de dinero), un procesador de pagos puede beneficiarse de la "exención para procesadores de pagos" y no estar sujeto a la BSA cuando: (a) la entidad debe facilitar la compra de bienes o servicios, o el pago de facturas por bienes o servicios (no la transmisión de dinero en sí); (b) la entidad opera mediante sistemas de compensación y liquidación que admiten únicamente instituciones financieras reguladas por la BSA; (c) la entidad presta servicios de pago conforme a un acuerdo formal; y (d) la entidad tiene al menos un contrato con el comerciante o acreedor que recibe los fondos.[368] Una entidad que cumple las cuatro condiciones no se considera un transmisor de dinero según las normas de la BSA y, por tanto, generalmente no está obligada a registrarse como MSB ni a implementar un programa completo AML/CFT. Esta exclusión regulatoria reconoce que dichos procesadores operan dentro de la supervisión del sistema bancario;

---

364 Véase GAFI, "Profesión Contable: Orientación para un enfoque basado en el riesgo," (junio de 2019), p. 11, https://www.fatf-gafi.org/content/dam/fatf- gafi/guidance/RBA-Accounting-Profession.pdf.coredownload.pdf.

365 *Véase, por ejemplo,* DOJ, "Contable Público Certificado de California Acusado por presentar declaraciones de impuestos falsas y esquema de fraude postal," (24 de julio de 2025) https://www.justice.gov/opa/pr/california-certified-public-accountant-indicted-filing-false-tax-returns-and-mail-fraud; DOJ, "Dos Empresarios, un contable público certificado y cuatro empresas con sede en Puerto Rico acusadas de fraude, soborno y blanqueo de capitales" (3 de abril de 2025) https://www.justice.gov/usao-pr/pr/two-businessmen-certified-public-accountant-and-four-puerto-rico-negocios.

366 Véase FRB Financial Services, "Federal Reserve Payments Insights Brief: Consumer Payments Study" (2024) https:// fedpaymentsimprovement.org/wp-content/uploads/2024-consumer-payments-study.pdf.

367 31 C.F.R. 1010.100(ff)(5)(ii)(B).

368 FinCEN, "FIN-2013-R002: Si una empresa que ofrece un mecanismo de pago basado en giros a pagar a sus clientes comerciales es un transmisor de dinero," (13 de noviembre de 2013), p. 3, https://www.fincen.gov/system/files/administrative_ruling/FIN- 2013-R002.pdf. *Véase también,* FinCEN, "Aplicación de regulaciones empresariales de servicios monetarios a una empresa que actúa como organización independiente de ventas y procesador de pagos," (27 de agosto de 2024), p. 2, https://www.fincen.gov/system/files/administrative_ruling/FIN- 2014-R009.pdf.

sin embargo, también puede crear una vulnerabilidad en el régimen AML/CFT. [369]

Los procesadores de pagos desempeñan un papel de control de acceso a los fondos que procesan en el sistema financiero porque se presume que los comerciantes han cumplido con los estrictos requisitos establecidos por las redes de tarjetas y cualquier requisito adicional de diligencia debida establecido por los bancos adquirentes. Dado que muchos procesadores de pagos están fuera de la regulación directa de la BSA, pueden ser una vía atractiva para la financiación ilícita. Esto puede aumentar el riesgo para los bancos que proporcionan cuentas a procesadores de pagos, ya que no mantienen relaciones directas con los comerciantes y, por tanto, dependen del procesador para realizar la debida diligencia y verificar la identidad y las prácticas comerciales del comerciante.[370] Los procesadores de pagos fuera del alcance de la BSA no tienen obligación legal de realizar la debida diligencia de clientes ni de presentar SAR; como resultado, algunos procesadores de pagos pueden carecer de controles sólidos para evaluar a los comerciantes o transacciones que gestionan. Los comerciantes de mayor riesgo que no pueden acceder fácilmente a cuentas bancarias directas pueden recurrir a procesadores externos, y los comercios fraudulentos pueden utilizar procesadores externos debido a controles percibidos más bajos.

Una de las formas en que los delincuentes utilizan procesadores de pagos para actividades ilícitas es a través del "blanqueo de transacciones", por el cual los delincuentes se hacen pasar por comerciantes legítimos para procesar transacciones ilegales a través del sistema de pagos. En un esquema típico de blanqueo de transacciones, los pagos ilícitos (por ejemplo, pagos por productos falsificados, drogas ilegales, juego, etc.) se disfrazan de ventas ordinarias al pasarlas por una cuenta comercial aparentemente legítima. A veces, los comerciantes fraudulentos crean empresas pantalla con sitios web aparentemente legítimos para crear su propia cuenta de comerciante en un procesador de pagos; Otros esquemas implican que un comerciante legítimo con una cuenta existente en un procesador de pagos procese transacciones en nombre de un comerciante fraudulento. En los esquemas de blanqueo de transacciones, a menudo tanto los consumidores como los comerciantes son cómplices en la defraudación de procesadores de pagos, redes de tarjetas y bancos.

En un caso, un hombre fue condenado a 10 años de prisión por defraudar a usuarios de internet mediante alertas de virus fraudulentas y distribuir sustancias controladas en línea. El hombre y sus cómplices facilitaron ventas online de varios proveedores extranjeros de drogas y recibieron sustancias controladas del extranjero antes de reempaquetarlas y distribuirlas por todo Estados Unidos. Para ocultar la naturaleza de las transacciones, el hombre y sus cómplices utilizaron PayPal y cuentas de comerciantes que supuestamente pertenecían a empresas de consultoría, tiendas de suplementos de salud, proveedores de repuestos de automóviles y agencias de viajes inexistentes. En algunos casos, el hombre y sus cómplices crearon itinerarios de viaje y recibos falsos para engañar a los procesadores de tarjetas de crédito en Estados Unidos y evitar que el negocio de las drogas fuera detectado. [371]

Los procesadores de pagos cómplices también pueden abusar de su posición como guardianes y realizar actividades ilícitas de forma independiente o coludir con sus clientes comerciantes para cometer fraude contra el consumidor, así como contra la red de tarjetas y los bancos implicados. Existen numerosas permutaciones de esquemas fraudulentos que involucran a procesadores de pagos, que a menudo se complican por el número de entidades en el panorama de pagos. Por ejemplo, en junio de 2025, un procesador de pagos con sede en el Reino Unido aceptó pagar 5 millones de dólares y quedar permanentemente prohibido de procesar pagos para operadores de soporte tecnológico para resolver una acción ante la FTC. La acción de la FTC alegó que el procesador de pagos abusó del sistema estadounidense de tarjetas de crédito y permitió que operadores extranjeros engañosos accedieran a él, costando a los consumidores millones de dólares. La

denuncia acusaba al procesador de pagos de abrir cuentas de comerciantes afirmando ser un "comerciante registrado"

369 Los procesadores de pagos de activos digitales no califican para la exención de procesadores de pagos porque, en general, no pueden cumplir la segunda condición, ya que no operan, ni total ni parcialmente, mediante sistemas de compensación y liquidación que solo admiten como miembros instituciones financieras reguladas por la BSA. Véase FinCEN, "FIN-2019-G001: Aplicación de las regulaciones de FinCEN a ciertos modelos de negocio que involucran monedas virtuales convertibles," (9 de mayo de 2019), pp. 21-23, https://www.fincen.gov/system/files/2019-05/FinCEN%20_Guidance%20CVC%20FINAL%20508.pdf.

370 En junio de 2023, el FRB, la FDIC y la OCC emitieron directrices para los bancos supervisados sobre los riesgos de las relaciones con terceros, incluidas aquellas con procesadores de pagos. La guía señalaba que el uso de terceros por parte de un banco no disminuye su responsabilidad de cumplir con sus requisitos regulatorios, y que el uso de terceros puede reducir el control directo del banco sobre sus actividades y puede introducir nuevos riesgos o aumentar los existentes. Orientación interinstitucional sobre relaciones con terceros: Gestión de riesgos, 88 Fed. Reg. 37920 (9 de junio de 2023) https://www.occ.gov/news-issuances/federal-register/2023/88fr37920.pdf.

371 DOJ, "Hombre de Michigan que orquestó fraudes informáticos internacionales y esquemas de distribución de drogas en línea

condenado a una década de prisión," (18 de junio de 2024), https://www.justice.gov/usao-ma/pr/michigan-man-who-orchestrated-international-computer-fraud-and distribución de drogas en línea.

o "revendedor" de software, luego utilizaba estas cuentas para procesar pagos con tarjeta en nombre de numerosos comerciantes terceros no relacionados, y permitía que esquemas extranjeros accedieran al sistema de tarjetas de crédito y cobraran pagos de consumidores estadounidenses, y evadieran la detección por bancos mercantiles y redes de tarjetas. [372]

XIV. Bienes y propiedades de alto valor

Los delincuentes compran bienes y propiedades de alto valor para blanquear ingresos ilícitos porque estos objetos pueden revenderse fácilmente en grandes volúmenes en todo el mundo debido a su transportabilidad y retención de valor. Estos tipos de bienes y propiedades incluyen metales preciosos, piedras y joyas (PMSJ), relojes y otras joyas, bolsos y otros artículos de cuero fino, prendas de diseñador, arte, automóviles y electrónica, entre otros. Aunque las obligaciones de la BSA se aplican a los concesionarios PMSJ como se describe a continuación, la mayoría de los demás comerciantes que operan con bienes y propiedades de alto valor solo están obligados a presentar un Formulario 8300 cuando reciben más de 10.000 dólares en efectivo en una sola transacción o en transacciones relacionadas.[373] Muchos delincuentes compran bienes y propiedades de alto valor para su propio disfrute personal, pero blanqueadores profesionales, incluidos los CMLN, también utilizan estos artículos para facilitar operaciones transfronterizas de blanqueo de capitales. Los delincuentes también han atacado al sector inmobiliario para blanquear ingresos ilícitos, especialmente mediante compras en efectivo realizadas por entidades legales.
La norma final del Tesoro sobre bienes raíces, que impone requisitos de notificación y conservación de registros a una categoría limitada de transferencias de mayor riesgo de bienes inmuebles residenciales, permitirá a las fuerzas del orden investigar estas transferencias con mayor facilidad.

Metales Preciosos, Piedras y Joyas (PMSJ)

El sector PMSJ tiene un alto riesgo inherente de blanqueo de capitales y otras actividades ilícitas, debido al valor y la fungibilidad de estos bienes, el tamaño y la estructura del sector, y la naturaleza a menudo informal de estos negocios y transacciones. La densidad de valor de estos materiales los convierte en un vehículo muy atractivo y eficaz para los delincuentes que buscan mover o transferir grandes sumas, mientras que sus cadenas de suministro opacas e internacionales conllevan riesgos significativos a nivel ascendente relacionados con sanciones y evasión de aranceles, trabajo forzado y abusos de derechos humanos, y crimen organizado transnacional. El sector, que comprende más de 20.000 concesionarios, cuenta con un gran flujo de caja que puede ser mal utilizado para ocultar actividades ilícitas, y sus negocios mayoritariamente pequeños y familiares tienen distintos niveles de experiencia en prácticas de debida diligencia AML/CFT y de clientes.[374] Las obligaciones de la BSA que se aplican a los comerciantes de metales preciosos, piedras y joyas (distribuidores PMSJ)[375] abordan riesgos probados exigiendo que ciertos distribuidores PMSJ establezcan y mantengan programas AML/CFT basados en riesgos y reporten ciertas transacciones en divisas que superen los 10.000 dólares utilizando el Formulario 8300.[376] Estas obligaciones de la BSA abordan riesgos inherentes que no se mitigan de otro modo, pero el sector sigue siendo vulnerable debido a su estructura y a los bienes que fluyen por él.

En los últimos dos años, ha habido varios tipos de actividades financieras ilícitas— incluyendo fraude, blanqueo de capitales y robo— asociadas al sector PMSJ, sus operadores y sus clientes. Estos casos frecuentemente implican a personas que venden o empeñan bienes ilícitos (incluidas joyas robadas), en ocasiones con pleno conocimiento del negocio sobre la naturaleza ilícita de los bienes;[377] personas blanquean ingresos ilícitos mediante lingotes de oro u otros metales preciosos;[378] y

372 FTC, "Paddle pagará 5 millones de dólares para resolver las acusaciones de la FTC sobre prácticas injustas de procesamiento de pagos y facilitación de esquemas engañosos de soporte tecnológico," (16 de junio de 2025) https://www.ftc.gov/news-events/news/press-releases/2025/06/paddle-will-pay-5-million-settle-ftc acusaciones-prácticas-inleales-procesamiento-pago-facilitación.

373 IRS, "Formulario 8300 e informes de pagos en efectivo superiores a 10.000 dólares," (actualizado el 24 de julio de 2025) https://www.irs.gov/businesses/small empresas-autónomas/formulario 8300 y reportando-pagos-de-más de 10.000.

374 Véase RIN 1506-AA58 31 CFR 103 70 FR 33702 375 Véase 31 CFR 1027.

376 La BSA obliga a los concesionarios PMSJ a informar de transacciones que superen los 10.000 dólares, que es inferior al umbral de 15.000 dólares del GAFI, que para los concesionarios PMSJ.

377 *Véase, por ejemplo,* DOJ, "Diamond District Fence se declara culpable en relación con una operación de propiedad robada a gran escala," (18 de julio de 2025) https:// www.justice.gov/usao-edny/pr/diamond-district-fence-pleads-guilty-connection-large-scale-stolen-property-operation.

378 *Véase, por ejemplo,* DOJ, "Dos ciudadanos indios acusados en fraude a ancianos con mensajería de barras de oro," (23 de

febrero de 2024) https://www.justice.gov/usao- ndoh/pr/dos-nacionales-indios-acusados-fraude-anciano-mensajero-de barra-de oro.

Propietarios o empleados de negocios que estafan a sus clientes o proveedores,[379] o roban a sus propios negocios. [380] En un caso notable, el propietario de un depósito de metales preciosos fue condenado a un máximo legal de 65 años de prisión tras su condena por fraude postal, fraude electrónico y evasión de impuestos. Las pruebas presentadas en el juicio y en el proceso de sentencia revelaron que el hombre robó al menos 76 millones de dólares a sus clientes y que más de 1.000 cuentas de clientes no tenían metales preciosos. Fuentes del sector han caracterizado este esquema fraudulento como el mayor robo en la historia de Estados Unidos en un depósito de metales preciosos. [381]

Como se menciona en la sección de Comercio Ilícito, los actores ilícitos también explotan el sector PMSJ para violar o evadir sanciones, aranceles u otros aranceles de importación estadounidenses. Estos riesgos se agravan por la opacidad de las cadenas de suministro de estos bienes. Una tipología consiste en que importadores de joyería etiquetan o transbordan deliberadamente productos erróneamente para eludir restricciones de importación, financieras o comerciales. Otra tipología de riesgo notable implica el uso indebido de negocios de joyería como tapaderas para realizar transacciones financieras ilegales para clientes, incluyendo convertir efectivo en cheques o transferencias bancarias a cambio de comisiones sustanciales sin registrarse como empresas transmisoras de dinero ante FinCEN u otras autoridades. Un caso ejemplifica ambas tipologías. En enero de 2025, un hombre afincado en India y Nueva Jersey que dirigía empresas de joyería en el Distrito de Diamantes de la ciudad de Nueva York fue condenado a 30 meses de prisión por liderar un plan para evadir ilegalmente aranceles aduaneros por más de 13,5 millones de dólares en importaciones de joyería a Estados Unidos y por procesar ilegalmente más de 10,3 millones de dólares a través de un negocio transmisor de dinero sin licencia.[382] Las fuerzas del orden también han denunciado esquemas comerciales ilícitos similares relacionados con la importación de diamantes desde Rusia, empresas mineras vinculadas al Grupo Wagner en África y otras minas de diamantes que violan los derechos humanos, en violación de las prohibiciones de importación y/o sanciones financieras de EE. UU. [383]

Arte

El mercado del arte de alto valor representa un bajo riesgo residual de blanqueo de capitales para el sistema financiero estadounidense. Aunque la estructura inherente del mercado y sus vulnerabilidades crean un entorno moderado de riesgo de blanqueo de capitales, como al presentar oportunidades para que los estafadores generen y blanqueen ingresos ilícitos, y para que los actores sancionados evadan restricciones, esta actividad sigue siendo limitada. Varias cualidades inherentes al arte de alto valor, el mercado de arte de alto valor y los participantes del mercado pueden hacer que el mercado sea atractivo para actores ilícitos que blanquean ingresos ilícitos o evadan sanciones. Específicamente, los altos valores en dólares de las transacciones individuales, la volatilidad y subjetividad de los precios de mercado, la transportabilidad del arte, la cultura de privacidad de larga data en el mercado, la prevalencia de ventas y transacciones privadas, y el uso creciente del arte como inversión o activo financiero contribuyen a las vulnerabilidades del arte al blanqueo de capitales.[384] Pero el tamaño y la dinámica del mercado de arte de alto valor presentan varios factores atenuantes que reducen su perfil de riesgo de blanqueo de capitales

Un reciente informe de tipologías del GAFI sobre complejos esquemas de evasión de sanciones demostró que una táctica común de los evasores de sanciones es recurrir a intermediarios terceros y empresas pantalla para ocultar la implicación de una persona sancionada en una transacción prohibida.[385] El mercado del arte es inherentemente vulnerable a tal complejidad

379 *Ver, por ejemplo,* Fiscal del Condado de Nueva York, "El fiscal Bragg anuncia declaración de culpabilidad en intercambio de diamantes," (28 de febrero de 2025) https:// manhattanda.org/d-a-bragg-announces-guilty-plea-in-diamond-swap/.

380 *Ver, por ejemplo,* DOJ, "Supervisor de una empresa de joyería de lujo condenado por robo y venta de millones de dólares en metales preciosos," (4 de diciembre de 2024) https://www.justice.gov/usao-ma/pr/supervisor-luxury-jewelry-company-sentenced-stealing-selling-millions dólares por valor de dólares.

381 DOJ, "Propietario de depósito de metales preciosos condenado a 65 años de prisión federal por esquema de fraude de 76 millones de dólares," (20 de junio de 2025) https:// www.justice.gov/usao-de/pr/precious-metals-depository-owner-sentenced-65-years-federal-prison-76-million-fraud. 382 DOJ, "Joyero con sede en India y Nueva Jersey condenado a 30 meses de prisión por esquema de fraude comercial internacional multimillonario y transmisión de dinero sin licencia," (23 de enero de 2025) https://www.justice.gov/usao-nj/pr/india-and-new-jersey-based joyero condenado a 30 meses de prisión multimillonaria.

383 *Ver, por ejemplo,* Tesorería, "Treasury sanciona a empresas vinculadas al Grupo Wagner en la República Centroafricana," (30 de mayo de 2024) https://home. treasury.gov/news/press-releases/jy2384.

384 Treasury, "Estudio sobre la facilitación del blanqueo de capitales y la financiación del terrorismo a través del comercio de obras de arte" (febrero de 2022) https:// home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf.

385 GAFI, "Complejos Sistemas de Financiación de la Proliferación y Evasión de Sanciones" (junio de 2025)

https://www.fatf-gafi.org/content/dam/fatf-gafi/ informes/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.

Esquemas de evasión de sanciones porque el uso de intermediarios, como asesores o consultores, y empresas pantalla son prácticas comerciales comúnmente aceptadas en el mercado del arte de alto valor, incluso para transacciones legítimas dominadas por individuos de alto patrimonio que buscan mantener sus operaciones protegidas del escrutinio por motivos legítimos.

En un caso, una mujer que actuaba como intermediaria fue acusada de un cargo de conspiración para violar la Ley de Poderes Económicos de Emergencia Internacional (IEEPA), un cargo de violación de la IEEPA y un cargo de conspiración para cometer blanqueo internacional de capitales. Como alega en la acusación, desde al menos febrero de 2023 hasta el presente, la mujer y otras personas supuestamente participaron en un plan para violar la IEEPA comprando arte y antigüedades para beneficio de oligarcas sancionados en galerías y casas de subastas en Estados Unidos y Europa, y enviando los objetos a su residencia en Huntly, Virginia, donde se almacenaron para su envío posterior a Rusia. A cambio, la mujer fue reembolsada y recibió una tarifa por servicios. La acusación alega que la mujer también participó en un esquema para blanquear dinero, sabiendo que las transacciones tenían como objetivo ocultar los ingresos de las violaciones de la IEEPA. [386]

Aunque el mercado del arte de alto valor tiene algunas cualidades que lo hacen vulnerable al abuso por parte de actores ilícitos, existen varios factores atenuantes que reducen el riesgo residual en el sector. Primero, el tamaño relativamente pequeño del mercado del arte, en comparación con otros sectores, no es lo suficientemente grande como para que los actores amenazantes más importantes generen o blanqueen volúmenes significativos de ingresos ilícitos. En segundo lugar, los participantes en el mercado del arte tienen incentivos económicos para realizar verificaciones mejoradas de contraparte y fuente de fondos, como el riesgo reputacional en un mercado cerrado y basado en la confianza o el riesgo crediticio de impago. En tercer lugar, las transacciones en el mercado del arte pueden llevar un tiempo considerable debido a la naturaleza de la obtención, la realización de la debida diligencia y los procedimientos de cierre. Esto puede convertir el mercado en un entorno inhóspito para los delincuentes que buscan blanquear rápidamente grandes cantidades de ingresos ilícitos. [387]

Bienes de lujo y electrónica

Varios casos durante el periodo de evaluación demuestran cómo los blanqueadores profesionales, incluidos los CMLN, continúan comprando bienes de lujo y electrónicos para blanquear ingresos ilícitos, como se destacó en la NMLRA de 2024.[388] Como ocurre con otros métodos profesionales de blanqueo de capitales, la fuente de los ingresos ilícitos puede provenir de diferentes delitos subyacentes, incluyendo el tráfico de drogas, varios tipos de esquemas de fraude y ciberdelitos. Los blanqueadores de dinero generalmente utilizan los ingresos ilícitos para comprar los bienes en minoristas (en persona o en línea), consolidar los bienes en almacenes y exportar los productos a jurisdicciones extranjeras para su reventa.

En un caso, dos hombres fueron arrestados y acusados de dirigir una empresa que exportaba cientos de millones de dólares en electrónica de consumo y tarjetas regalo, casi todas derivadas de actividades delictivas como robo de identidad, robo de tarjetas de crédito y fraude. Según una declaración jurada presentada junto con la denuncia, los hombres poseían y operaban una empresa que utilizaba almacenes para agregar electrónica antes de enviarlos fuera de Estados Unidos. Desde 2019, la empresa ha exportado más de 611 millones de dólares en electrónica desde Estados Unidos, casi todos los cuales las fuerzas del orden consideran ingresos por delitos. Los hombres consiguieron aparatos electrónicos y tarjetas regalo de muchas fuentes ilícitas. También adquirieron electrónica directamente mediante fraude. Compraron productos electrónicos en Best Buy, The Home Depot y otros minoristas utilizando tarjetas regalo cargadas con el dinero del fraude, principalmente a través de tarjetas de crédito robadas. Esos

386 DOJ, "Presentador de televisión que trabajó para Channel One Rusia acusado de violar las sanciones estadounidenses impuestas a Rusia," (5 de septiembre de 2024) https://www.justice.gov/archives/opa/pr/tv-presenter-who-worked-channel-one-russia-charged-violating-us-sanctions-imposed-Rusia.

387 Véase Tesorería, "Estudio sobre la facilitación del blanqueo de capitales y la financiación del terrorismo a través del comercio de obras de arte" (febrero de 2022) https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf; GAFI, "Blanqueo de Dinero y Financiación del Terrorismo en el Mercado del Arte y las Antigüedades" (febrero de 2023) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.pdf.coredownload.pdf.

388 *véase, por ejemplo,* DOJ, "Ciudadanos chinos condenados a prisión federal por participar en una conspiración fraudulenta de tarjetas regalo que implica la compra y exportación de productos Apple a China," (22 de abril de 2025) https://www.justice.gov/usao-nh/pr/chinese-nationals-sentenced- conspiración de tarjetas regalo fraudulentas que participan en prisiones federales; DOJ, "Tres miembros de una organización internacional de blanqueo de dinero acusados de blanquear millones de dólares en ingresos por drogas," (24 de abril de 2025) https://www.justice.gov/opa/pr/three-members- organización internacional de blanqueo de capitales acusada de millones.

La electrónica a menudo se enviaba directamente al almacén de la empresa o a buzones que controlaban los hombres. [389]

Como se describe en el Análisis de Tendencias Financieras CMLN de FinCEN de agosto de 2025, es probable que las CMLN con sede en EE. UU. recluten a individuos conscientes o inconscientes, especialmente estudiantes chinos, en Estados Unidos para comprar productos electrónicos y de lujo de alto valor para exportar a China y otras regiones, como parte de esquemas de blanqueo de capitales. Las personas reclutadas creen que trabajan como *compradores de daigou*, un acuerdo informal en el que los compradores, principalmente utilizando plataformas de mensajería populares en China, conectan a consumidores con base en China con productos extranjeros. Esto puede incluir comprar artículos en tiendas o online usando tarjetas de crédito y obtener fondos de CMLNs en efectivo, P2P o ACH para realizar pagos sobre los saldos de las cuentas. [390]

Bienes Raíces

La mayoría de las transferencias de bienes raíces residenciales están bien reguladas porque están asociadas a un préstamo hipotecario u otra financiación proporcionada por instituciones financieras cubiertas sujetas a los requisitos del programa integral AML/CFT. Las transferencias no financiadas (o "totalmente en efectivo") de bienes inmuebles residenciales, que representan entre el 20 y el 30 por ciento del mercado, no implican a dichas instituciones financieras y pueden ser explotadas para blanquear ingresos ilícitos. El Tesoro ha reconocido desde hace tiempo los riesgos financieros ilícitos que representan los delincuentes y funcionarios corruptos que abusan de entidades legales opacas y fideicomisos para blanquear ganancias mal habidas mediante transferencias de bienes inmuebles residenciales.[391] Este uso ilícito del mercado inmobiliario residencial amenaza la seguridad económica y nacional de EE. UU. y puede perjudicar a individuos y pequeñas empresas que buscan competir de manera justa en la economía estadounidense.

Actores ilícitos de todo tipo, incluidos aquellos que suponen amenazas internas, como personas involucradas en fraudes o crimen organizado, y amenazas extranjeras, como cárteles internacionales de droga, traficantes de personas y figuras políticas o empresariales corruptas, participan en el blanqueo de capitales a través del sector inmobiliario. En un caso, una mujer se declaró culpable de cargos federales de conspiración para poseer con intención de distribuir metanfetamina y conspiración para blanquear dinero. Como parte de la operación criminal, la mujer y sus asociados compraron bienes inmuebles por valor de millones de dólares, vehículos y bienes de lujo, todo diseñado para ocultar la fuente ilícita de su riqueza. La investigación reveló que la mujer compró cinco viviendas distintas, incluyendo una casa de siete dormitorios frente al mar en Jonesboro, Georgia. Tres de estas residencias fueron adquiridas con dinero en efectivo aportado directamente a la transacción. [392]

En otros casos, el sector inmobiliario residencial estadounidense ha sido un vehículo para que exfuncionarios del gobierno venezolano en el régimen de Nicolás Maduro y numerosos rusos sancionados oculten sus ganancias ilícitas de la corrupción. Por ejemplo, en enero de 2025, un agente inmobiliario de Miami se declaró culpable de participar en un plan para violar las sanciones estadounidenses y blanquear dinero mediante transacciones que involucraban propiedades bloqueadas propiedad de oligarcas rusos sancionados. Según se describe en documentos judiciales, desde enero de 2018 o alrededor de marzo de 2023, el corredor conspiró con otros para violar la IEEPA y cometer blanqueo de capitales manteniendo, transfiriendo, vendiendo y arrendando varios condominios de lujo en el área de Miami que poseían los oligarcas y recaudando, compartiendo y utilizando los ingresos para mantener las propiedades. [393]

---

389 DOJ, "Dos hombres del Valle de San Fernando arrestados por denuncia federal que alegan haber exportado 611 millones de dólares en electrónica obtenida mediante fraude," (16 de septiembre de 2025) https://www.justice.gov/usao-cdca/pr/two-san-fernando-valley-men-arrested-federal-complaint- alegando-haber-exportado-611.

390 FinCEN, "Redes chinas de blanqueo de capitales: 2020 – 2024 Patrón de amenazas e información sobre tendencias," (agosto de 2025), pp. 11-12, https://www. fincen.gov/system/files/2025-08/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf.

391 Tesoro, "Evaluación Nacional de Riesgo de Blanqueo de Dinero 2024," febrero de 2024, pp. 75-78, https://home.treasury.gov/system/ archivos/136/2024-National-Money-Laundering-Risk-Assessment.pdf; Tesoro, "Evaluación Nacional del Riesgo de Blanqueo de Dinero 2022," febrero de 2024, pp. 57-60, https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf 392 DOJ, "Líder de una red internacional multimillonaria de blanqueo de dinero y tráfico de drogas condenado," (16 de junio de 2025) https://www. justice.gov/usao-ndga/pr/leader-multi-million-dollar-international-money-laundering-and-drug-trafficking-ring. 393 DOJ, "Corredor inmobiliario con sede en Miami se declara culpable de conspiración para violar las sanciones Rusia-Ucrania y para cometer blanqueo de capitales," (16 de enero de 2026) https://www.justice.gov/archives/opa/pr/miami-based-real-estate-broker-pleads-guilty-conspiracy-violar-Rusia-Ucrania-sanciones-y; OFAC, "Family International Realty LLC y su propietario llegan a un acuerdo con OFAC por 1.076.923 dólares relacionados con aparentes violaciones de sanciones relacionadas con Ucrania y Rusia," (16 de enero de 2025) https://ofac.treasury.gov/media/933941/ descargar en línea.

En agosto de 2024, el Tesoro finalizó una norma que impondría requisitos de información y conservación de registros a una categoría limitada de transferencias de bienes inmuebles residenciales de mayor riesgo.[394] La norma final se centra en menos del 20 al 30 por ciento de las transferencias que no son financiadas y que involucran a ciertas entidades jurídicas y fideicomisos, e incluye múltiples excepciones significativas para transferencias comunes y de bajo riesgo. La norma final abordará los riesgos derivados de numerosas tipologías de blanqueo de capitales que implican la compra de bienes inmuebles residenciales, incluyendo el uso de entidades jurídicas nacionales y extranjeras, acuerdos legales y cuentas agrupadas como las IOLTAs; el uso de candidatos y guardianes; el uso de pagos totalmente en efectivo para evitar el escrutinio AML/CFT que conlleva la financiación; pagar por encima o por debajo de los bienes inmuebles; y la sucesiva transferencia de bienes inmuebles a un valor superior . Para ser declarable, la transferencia debe ser no financiada (es decir, totalmente en efectivo) y el nuevo propietario de la propiedad debe ser una persona jurídica o fideicomiso. La norma final se desarrolló basándose en las lecciones aprendidas de las muy efectivas Órdenes de Segmentación Geográfica (GTOs) en bienes raíces residenciales, que están vigentes desde 2016 y que ahora cubren más de 66 condados en Estados Unidos.[395] Estas GTO han exigido informes similares de ventas no financiadas de bienes inmuebles residenciales a entidades jurídicas, pero de forma geográficamente limitada.

La norma final entrará en vigor el 1 de marzo de 2026. Por primera vez, Estados Unidos contará con un mecanismo uniforme y nacional para que la industria inmobiliaria informe sobre riesgos financieros ilícitos generalizados asociados en igual medida a entidades y acuerdos legales nacionales y extranjeros en el mercado inmobiliario residencial estadounidense no financiado. [396]

Los informes presentados según los requisitos de la norma definitiva harán que las investigaciones policiales sobre actividades ilícitas y blanqueo de capitales a través de bienes raíces residenciales sean menos costosas, menos extensas y más eficaces; reducir los costes sociales asociados a esta actividad ilícita, como los precios de las viviendas artificialmente inflados; crear igualdad de condiciones para las pequeñas empresas que operan en el mercado inmobiliario asegurando que existan requisitos uniformes de informes y registro a nivel nacional; y fortalecer la seguridad nacional de EE. UU. y ayudar a proteger la integridad del sistema financiero estadounidense asegurando que los actores ilícitos no se beneficien financieramente al utilizar nuestro mercado inmobiliario para desplazar los beneficios del delito.

Bienes raíces comerciales

Las transacciones inmobiliarias comerciales pueden servir como conductos para fondos ilícitos, incluidos aquellos relacionados con el tráfico de drogas y otras formas de actividad delictiva. En enero de 2023, FinCEN emitió una alerta destacando que el sector inmobiliario comercial está expuesto al riesgo de blanqueo de capitales porque normalmente utiliza entidades legales diseñadas específicamente, cadenas de propiedad indirecta, múltiples tipos de propiedad y financiación, y diversas partes involucradas en cada transacción, factores que pueden ocultar la titularidad beneficiaria y el origen de los fondos.[397] Por ejemplo, en abril de 2024 se publicó una acusación formal de ocho cargos que acusaba a dos hombres por su papel en facilitar el mercado negro de la industria de la marihuana en Oklahoma. La acusación alega que los dos hombres, un agente inmobiliario y un abogado, conspiraron para ayudar y complicar a traficantes de marihuana en Oklahoma haciendo declaraciones falsas y fraudulentas en solicitudes de licencias estatales para operar granjas de marihuana, todo en nombre de sus clientes traficantes de marihuana en el mercado negro. El corredor inmobiliario también fue encargado de utilizar su firma de corretaje y su red de empresas de gestión e inversión inmobiliaria para atender las necesidades de vivienda y/o inmuebles de los traficantes de marihuana del mercado negro, mediante ventas de terrenos por todo Oklahoma, alquilándoles terrenos para operar sus cultivos de marihuana en el mercado negro y alquilándoles viviendas que servían como depósitos de marihuana y residencias personales de los propietarios de cultivos del mercado negro. [398]

Se necesitan investigaciones más exhaustivas, recopilación de datos y escrutinio regulatorio para determinar si estos riesgos de blanqueo de capitales en bienes raíces comerciales son generalizados, sistémicos o concentrados en segmentos específicos.

394 Regulaciones contra el Blanqueo de Capitales para Transferencias de Bienes Raíces Residenciales, 31 CFR Capítulo X RIN 1506-AB54 https://www.federalregister. gov/documents/2024/08/29/2024-19198/anti-blanqueo de dinero-para transferencias inmobiliarias residenciales.

395 FinCEN, "FinCEN renueva órdenes geográficas de segmentación de bienes raíces residenciales," (9 de octubre de 2025), https://www.fincen.gov/news/news- publica/fincen-renieva-inmobiliaria-geográfica-órdenes-0.

396 Ver Informe Inmobiliario, OMB No. 1506-0080 https://www.fincen.gov/system/files/2025-09/RER-Form-508C.pdf.

397 FinCEN, "Alerta FinCEN sobre posibles inversiones inmobiliarias comerciales en EE. UU. por parte de élites rusas sancionadas, oligarcas y sus proxies," (enero de 2023) https://www.fincen.gov/system/files/shared/FinCEN%20Alert%20Real%20Estate%20FINAL%20508_1-25-23%20FINAL%20FINAL.pdf.

398 DOJ, "Abogado Metro y Corredor Inmobiliario Metropolitano acusados en esquema de licencias fantasma para facilitar operaciones de marihuana en el mercado negro," (10 de abril de 2024) https://www.justice.gov/usao-wdok/pr/metro-attorney-and-metro-real-estate-broker-charged-ghost-esquema_de_licencias-facilitar.

CONCLUSIÓN

Las principales amenazas y vulnerabilidades de blanqueo de capitales se han mantenido en gran medida constantes durante la última década, pero el carácter y la manera en que el sistema financiero estadounidense es explotado por actores ilícitos sigue evolucionando. Los avances tecnológicos en finanzas y comunicación han amplificado las amenazas que suponen todo tipo de delitos subyacentes.

Aunque todos los países deben adaptarse a estos cambios, Estados Unidos en particular ha sido cada vez más objetivo de actores extranjeros debido al tamaño y la apertura de la economía estadounidense. Los sectores público y privado de EE. UU. deben seguir evolucionando para combatir la amenaza que supone la financiación ilícita, al tiempo que protegen y fomentan la financiación legítima sin una carga excesiva.

PARTICIPANTES

Departamento del Tesoro

Servicio de Impuestos Internos - Investigación Criminal (IRS-CI), Terrorismo e Inteligencia Financiera (TFI)

- y Red de Aplicación de Delitos Financieros (FinCEN)
- y Oficina de Control de Activos Extranjeros (OFAC)
- y Oficina de Inteligencia y Análisis (OIA)
- y de Financiación del Terrorismo y Delitos Financieros (TFFC)

Departamento de Justicia (DOJ)

División Penal

- y Sección de Delitos Informáticos y Propiedad Intelectual (CCIPS)
- y Sección de Fraude

y Sección de Blanqueo de Capitales, Narcóticos y Decomiso (MNF) Oficina Ejecutiva de los Fiscales de los Estados Unidos (DEA) de la Oficina Federal de Investigación (FBI)

Departamento de Seguridad Nacional

Aduanas y Protección Fronteriza (CBP) Investigaciones de Seguridad Nacional (HSI) Servicio Secreto de los Estados Unidos (USSS)

Departamento de Estado del Servicio de Inspección Postal de los EE. UU. (USPIS) Personal de los reguladores funcionales federales 399

399 Esto incluye al personal de la Comisión de Comercio de Futuros de Materias Primas (CFTC), la Corporación Federal de Seguros de Depósitos (FDIC), la Junta de Gobernadores del Sistema de la Reserva Federal (FRB), la Administración Nacional de Cooperativas de Crédito (NCUA), la Oficina del Contralor de la Moneda (OCC) y la Comisión de Bolsa y Valores (SEC). El personal de la SEC también solicitó la opinión del personal de la Autoridad Reguladora de la Industria Financiera (FINRA), que regula a los miembros de corredores de bolsa que hacen negocios con el público en Estados Unidos.

METODOLOGÍA

La Oficina de Financiación del Terrorismo y Delitos Financieros (TFFC) del Tesoro, por ley, es la coordinadora de políticas AML/CFT para el Tesoro y interactúa rutinariamente con nuestros socios nacionales. Este informe se basa en una revisión del análisis del sector público federal y estatal, acciones de aplicación, directrices y entrevistas con personal del Tesoro de EE.UU., analistas de inteligencia, agentes de la ley y fiscales. Durante la fase de investigación y análisis, compartimos borradores de trabajo de diferentes secciones con los interesados relevantes para comentarios y coordinamos aportaciones y retroalimentación sobre tres borradores distintos de este documento.

La NMLRA utiliza toda la información disponible para identificar el actual entorno de blanqueo de capitales en Estados Unidos. Esta iniciativa incluye comentarios y aportaciones de diversos participantes del sector privado a través de mecanismos formales e informales y reuniones específicas sobre tendencias de financiación ilícita. Esta acción se realiza generalmente mediante divulgación tras la publicación del NMLRA previamente publicado. Componentes relevantes de agencias, oficinas y oficinas del Tesoro, el Departamento de Justicia de EE. UU. (DOJ), el Departamento de Seguridad Nacional de EE. UU. (DHS) y otros mencionados anteriormente participaron en el desarrollo de la evaluación de riesgos. Los datos recogidos están actualizados a fecha de 15 de enero de 2026.

Hemos identificado casos que demuestran algún tipo de actividad de blanqueo de capitales o muestran cómo actores criminales han utilizado el sistema financiero estadounidense para mover, disfrazar u ocultar los beneficios del delito. Ejemplos de casos pueden implicar cargos penales en una acusación formal, que son meras acusaciones. Todos los acusados se presumen inocentes salvo que, y hasta que se demuestre su culpabilidad más allá de toda duda razonable, en un tribunal de justicia.
También hemos utilizado datos cualitativos, a menudo proporcionados por las fuerzas del orden, cuando no hay fuentes públicas disponibles (por ejemplo, notas de prensa o documentación judicial). Al citar datos cualitativos, la NMLRA deja claro que cierta información es "conforme a las fuerzas del orden".

El Tesoro llevará a cabo una amplia divulgación con nuestros sectores público y privado para entregar los resultados de este informe. Al hacerlo, esperamos recibir comentarios valiosos sobre la utilidad de esta evaluación y cómo podemos seguir mejorando este proceso.

TERMINOLOGÍA

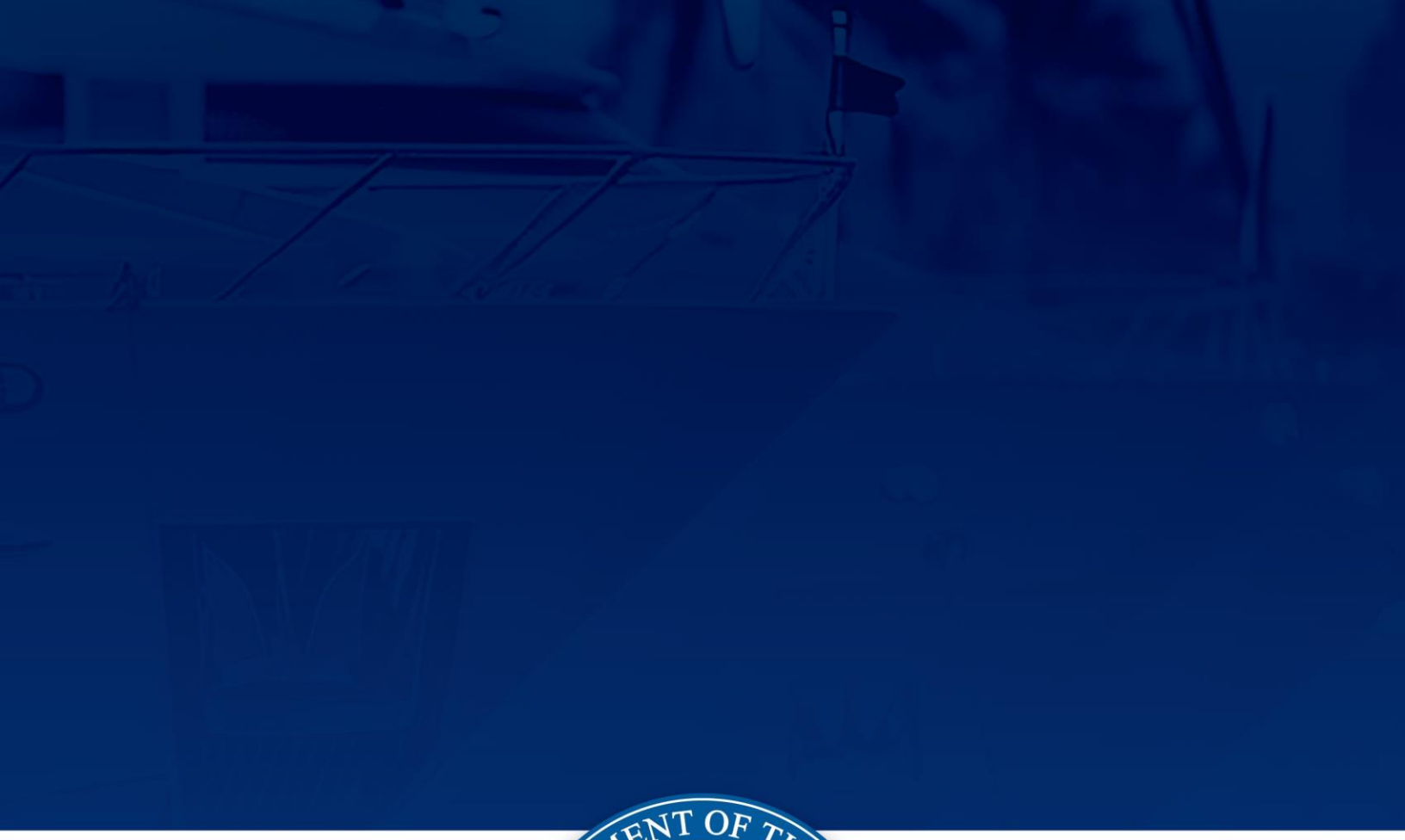
La terminología y metodología de la NMLRA se basan en parte en las directrices del GAFI, el organismo internacional de normalización para las salvaguardas AML/CFT. En esta evaluación de riesgos se utilizan los siguientes conceptos:

Amenazas: A efectos de la NMLRA, las amenazas son los delitos subyacentes asociados al blanqueo de capitales. El entorno en el que se cometen delitos subyacentes y se generan los beneficios del delito es relevante para entender por qué, en algunos casos, delitos específicos están asociados con métodos particulares de blanqueo de capitales.

Vulnerabilidades: Las vulnerabilidades son las que facilitan o crean la oportunidad de blanqueo de capitales. Pueden estar relacionadas con un sector financiero o producto específico, o con una debilidad en la ley, regulación, supervisión o aplicación.

Consecuencias: Las consecuencias incluyen daños o costes infligidos a los ciudadanos estadounidenses y el efecto en la economía estadounidense, lo que proporciona más contexto sobre la naturaleza de las amenazas.

Riesgo: El riesgo es una función de la amenaza, la vulnerabilidad y la consecuencia. Representa una evaluación global, considerando el efecto de las medidas de mitigación, incluyendo regulación, supervisión y aplicación.




THE DEPARTMENT OF THE TREASURY
1789