Esta publicación ha sido traducida al español solo para su conveniencia. Aunque FinCEN ha tomado medidas razonables para proporcionar la traducción más precisa posible, la versión en inglés es la única versión oficial de la Alerta de FinCEN sobre el surgimiento nacional de estafas de fraude con cheques en relación con robos postales que apuntan al correo de EE. UU. Si tiene alguna pregunta sobre el significado o la precisión de la información contenida en la alerta traducida, por favor consulte la versión en inglés del documento.

ALERTA DE FinCEN

FIN-2023-Alert003 **27 de febrero de 2023**

Alerta de FinCEN sobre el surgimiento nacional de estafas de fraude con cheques en relación con robos postales que apuntan al correo de EE. UU.

Solicitud de presentación de Informe de actividad sospechosa (SAR, por sus siglas en inglés)

FinCEN solicita que las instituciones financieras consulten esta alerta en el campo 2 del SAR (Nota de la institución de presentación a FinCEN) y en la narrativa incluyendo el término clave "**FIN-2023-MAILTHEFT**" y marcando la casilla de fraude por cheque **(SAR campo 34(d))**.

A la luz de un aumento a escala nacional de los fraudes con cheques dirigidos al correo de EE.UU.[1] (a continuación, "fraude con cheques relacionado con el robo de correo"), la Red de Control de Delitos Financieros (FinCEN) emite esta alerta a instituciones financieras[2] para que estén atentas a la hora de identificar y denunciar dicha actividad. El fraude con cheques relacionados con robos postales en general tiene que ver con la negociación fraudulenta de cheques robados del sistema de correo de EE.UU. El fraude, incluyendo el fraude con cheques, es la fuente más grande de ganancias ilícitas en los Estados Unidos y representa una de las amenazas de lavado de dinero más considerables en los Estados Unidos, según se distingue en la Evaluación Nacional de Riesgos de Lavado de Dinero más reciente y la Estrategia Nacional para Combatir Terroristas y otras Actividades de Financiamiento Ilícitas del Departamento del Tesoro.[3]

1. "Correo de EE.UU." es una marca registrada del Servicio Postal de Estados Unidos (USPS, por sus siglas en inglés) e incluye todo el correo distribuido y entregado mediante el Servicio Postal. Esto incluye el correo de primera clase como las cartas, tarjetas y otras correspondencias enviadas por correo, que pueden contener giros postales, información personal identificable y tarjetas de débito y crédito.
2. *Véase* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
3. *Véase* Departamento del Tesoro de EE. UU., "Evaluación de Riesgo de Lavado de Dinero" (febrero de 2022), en las págs. 6-7; Departamento del Tesoro de EE. UU., "Estrategia Nacional para Combatir el Terrorismo y Otras Actividades de Financiamiento Ilícitas " (mayo de 2022), en la pág. 27.

El fraude también es una de las prioridades nacionales contra el lavado de dinero y contrarrestar el financiamiento del terrorismo (AML/CFT).[4]

FinCEN emite esta alerta en colaboración estrecha con el Servicio de Inspección Postal de Estados Unidos (USPIS)[5] para asegurar que las instituciones financieras presenten SARs que identifiquen y reporten de forma apropiada las sospechas de fraudes con cheques que pueden asociarse con el robo de correo en Estados Unidos. Esta alerta proporciona un resumen de un aumento reciente de los fraudes con cheques relacionados con el robo de correo, destaca las señales de alerta para ayudar a las instituciones financieras al identificar y reportar actividades sospechosas y recuerda a las instituciones financieras sus requisitos de reporte según la Ley de Secreto Bancario (BSA, por sus siglas en inglés).

La información contenida en esta alerta se deriva del análisis de los datos de BSA realizado por FinCEN, reportes de fuente abierta e información reportada por las agencias de ley y orden.

Tendencias crecientes de fraudes con cheques relacionados con el robo de correo

A pesar de la disminución del uso de cheques en los Estados Unidos,[6] los delincuentes han apuntado cada vez más al correo de EE. UU. desde la pandemia de COVID-19 para cometer fraude con cheques.[7] El Servicio Postal de los Estados Unidos (USPS, por sus siglas en inglés) entrega casi 130 mil millones de piezas de correo nacional cada año a más de 160 millones de direcciones residenciales y comerciales en todo Estados Unidos.[8] Desde marzo de 2020 hasta febrero 2021, USPIS recibió 299,020 denuncias de robo de correo, lo cual fue un incremento de 161 por ciento

4. *Véase* FinCEN, "Prioridades nacionales de antilavado de dinero y contra el financiamiento del terrorismo" (30 de junio de 2021).
5. USPIS es la rama de aplicación de la ley, prevención de delitos y seguridad de USPS. Los inspectores postales son agentes federales de fuerzas de seguridad que tienen autoridad general para investigar las violaciones de la ley federal en conexión con el correo de EE. UU. y USPS, incluyendo el robo de correo y los delitos financieros asociados. USPIS es una de varias agencias federales con autoridad para investigar las ganancias por lavado de dinero. Para obtener más información, visite Servicio de Inspección Postal de EE.UU.(uspis.gov). *También véase* USPIS, "Reporte anual 2021" (12 de julio de 2022).
6. Según los analistas del Banco de la Reserva Federal de Atlanta, "de 2015 a 2018, la proporción de clientes que declaran que los cheques son su medio de pago preferido ha disminuido en un 23 por ciento para las cuentas y 8 por ciento para las compras." *Véase* Claire Greene, Marcin Hitczenko, Brian Prescott, y Oz Shy, reportes de información de investigación, "Uso de cheques personales de clientes de EE.UU. cheques personales: evidencia de una encuesta diaria" Reserva Bancaria Federal de Atlanta (febrero de 2020), en pág. 1. Actualmente, las estimaciones del Consejo de Gobernadores de la Reserva Federal muestran que, en promedio, la cantidad en dólares por cheque comercial incrementa cada año. *Véase* el Consejo de Gobernadores del Sistema de Reserva Federal, Cheques comerciales cobrados mediante la reserva federal - información trimestral.
7. Anteriormente, FinCEN emitió una advertencia para alertar a las instituciones financieras que controlen el fraude y otros delitos financieros que implican pagos de impacto económico autorizados por la Ley de Ayuda, Alivio y Seguridad Económica por Coronavirus (CARES, por sus siglas en inglés) y la Ley de Apropiaciones Complementarias de Respuesta y Alivio por Coronavirus de 2021. *Véase* FinCEN," Asesoría sobre delitos financieros que apuntan a pagos de impacto económico de COVID-19" (24 de febrero de 2021).
8. *Véase* USPIS, "Reporte anual de 2021," *supra* nota al pie 5, en pág. 19.

comparado con el mismo periodo un año antes.[9] Los informes de BSA por fraude de cheque también han incrementado en los últimos tres años. En 2021, las instituciones financieras presentaron más de 350,000 SARs a FinCEN para reportar posibles fraudes de cheques, un incremento del 23 por ciento por sobre la cantidad de SARs presentados en relación con el fraude de cheques en 2020. Esta tendencia en alza continuó hasta 2022, cuando la cantidad de SARs relacionados con el fraude de cheques alcanzó más de 680,000, casi el doble que la cantidad de presentaciones del año anterior.[10]

Riesgos y vulnerabilidades de robo de correo

Los delincuentes que cometen fraude de cheques relacionado con el robo de correo, en general, apuntan al correo de EE. UU. para robar cheques personales, comerciales, cheques de reembolso tributario y cheques relacionados con los programas de asistencia de gobierno, como los pagos de seguridad social y beneficios de desempleo. En general, los delincuentes roban todo tipo de cheques en el correo de EE. UU. como parte del robo de correo, pero los cheques comerciales pueden tener más valor porque las cuentas comerciales suelen tener buenos fondos y puede llevar más tiempo que la víctima note el fraude. Ha habido casos de empleados postales que robaron cheques en las instalaciones de separación y distribución de USPS.[11] Sin embargo, según USPIS, los fraudes con cheques relacionados con el robo de correo han incrementado entre otros empleados relacionados con USPS, que van desde los estafadores individuales hasta los grupos de crimen organizado compuestos por los organizadores de la estafa, los reclutadores, lavadores de cheques y mulas de dinero.

Lavadores de cheques: El lavado de cheques implica utilizar químicos para eliminar la tinta original en un cheque para reemplazar el pago y a menudo el importe. Los estafadores también pueden copiar e imprimir múltiples cheques lavados para su uso en el futuro o para venderlos a otros delincuentes.[12]

Mulas de dinero: Una mula de dinero es una persona (ya sea a sabiendas o involuntariamente) que transfiere o traslada fondos ilícitos según las indicaciones o en nombre de otro.[13]

9. *Véase* Oficina del Inspector General de USPS, informe de auditoría "Respuesta de pandemia al fraude por correo y robo por correo del servicio de inspección postal de EE. UU." (20 de mayo de 2021), en la pág. 5.
10. *Véase* las estadísticas de SAR de FinCEN. Esta estadística incluye todos los SAR con el recuadro 34(d), *fraude con cheques*, marcados y que no indican específicamente fraude de correo con cheques relacionados con el robo.
11. *Véase* Departamento de Justicia de EE. UU. (DOJ, por sus siglas en inglés), comunicado de prensa, "Múltiples empleados del servicio postal de EE. UU. y otras personas arrestadas por fraudes y estafas de robo de identidad por $1,3 millones" (29 de septiembre de 2022); DOJ, comunicado de prensa, "Trabajadores postales de Queens procesados por fraude de soborno y robo de correo en relación con el fraude de beneficios por COVID-19" (12 de agosto de 2022).
12. *Véase* USPIS, artículo sobre estafas, Lavado de cheques (22 de septiembre de 2022).
13. *Véase* USPIS, artículo sobre estafas, Mulas de dinero (1 de junio de 2022); DOJ, Iniciativa contra mulas de dinero; Buró Federal de Investigación (FBI), Centro de Denuncias de Delitos por Internet, anuncio de servicio público, "Mulas de dinero: una crisis financiera" (3 de diciembre de 2021); FBI, Mulas de dinero; *también véase* el comunicado de prensa del Servicio Secreto de Estados Unidos, "Hombre de Georgia sentenciado por fraude bancario que explotaba a personas sin hogar en Rhode Island" (16 de febrero de 2022).

Estos delincuentes que se encuentran en todo el condado se enfocan en los buzones azules de USPS, buzones residenciales y, unidades de correo de propiedades en complejos de departamentos, vecindarios cerrados y edificios con alta densidad comercial. El robo de correo puede ocurrir mediante el uso o dispositivos caseros de pesca de buzones[14] e implica de forma progresiva el uso auténtico o falso de llaves maestras de USPS, conocidas como las llaves *arrow*. Las llaves *arrow* abren los buzones azules de recolección de USPS y las unidades de buzones dentro de un área geográfica, y varios casos recientes involucran a delincuentes organizados que atacan violentamente a los carteros de USPS con la intención de robar las llaves *arrow*.[15] También ha habido casos de empleados corruptos del servicio postal que proporcionan de forma ilegal las llaves *arrow* para facilitar el robo de correo.[16] Los actores ilícitos también pueden copiar y vender las llaves *arrow* a terceros estafadores en redes ilegales y mediante redes sociales encriptadas a cambio de monedas virtuales convertibles.

Tipologías de fraudes con cheques relacionados con el robo de correo y asociados con el lavado de dinero

Tras robar cheques del correo de EE. UU., los estafadores y los grupos delictivos organizados pueden modificar o "lavar" los cheques, reemplazando la información del receptor o las cuentas de la empresa que controlan los delincuentes. Durante el lavado de cheques, esos actores ilícitos también suelen incrementar el importe de los cheques, a veces por cientos o miles de dólares. Los cheques lavados también pueden copiarse, imprimirse y venderse a otros estafadores en sitios ilegales y redes sociales encriptadas a cambio de moneda virtual convertible. En algunos casos, los cheques de víctimas también se falsifican utilizando información de ruteo y cuenta del cheque original robado.[17] Los delincuentes pueden cambiar o depositar los cheques en instituciones financieras mediante cajeros automáticos (ATM) o por depósito remoto en cuentas que controlan que suelen abrir específicamente para las estafas de fraude con cheques. Los delincuentes también pueden depender de las mulas de dinero y sus cuentas preexistentes para depositar cheques fraudulentos.[18]

14. Los dispositivos de pesca son artículos improvisados, generalmente con una sustancia adhesiva aplicada, cuyo propósito es adherirse al correo de EE.UU. para facilitar la extracción oculta del correo de un buzón de recolección azul.
15. *Véase* DOJ, comunicado de prensa, "Se condena a un hombre de Tampa por asalto con armas a un cartero" (27 de enero de 2023); DOJ, comunicado de prensa, "Se condena a tres hombres del área de Filadelfia en conexión con las llaves *arrow* de USPS, robo de buzones de correo" (3 de octubre de 2022); DOJ, comunicado de prensa, "Cuatro demandados enfrentan cargos por robo de cartas y posesión de llaves del servicio postal de Estados Unidos" (29 de julio de 2022); DOJ, comunicado de prensa, "Se arresta a tres hombres del área de Filadelfia en conexión con una estafa para lavar y alterar cheques robados de los buzones de USPS" (25 de julio de 2020); DOJ, comunicado de prensa, "Hombre de Nicaragua sentenciado a más de 11 años en prisión por una serie de robos durante dos semanas de los carteros del correo postal de EE. UU." (14 de julio de 2022); DOJ, comunicado de prensa, "Hombre del condado de Sacramento sentenciado a 10 años de prisión por robos armados a un cartero del correo postal de EE. UU. y por fraude bancario" (1 de marzo de 2022); DOJ, comunicado de prensa, "Hombre del condado de Passaic sentenciado por robo a dos empleados del servicio postal de EE.UU." (9 de febrero de 2022).
16. *Véase* el DOJ, comunicado de prensa, "Trabajador postal se declara culpable de ayudar ejecutar el robo de correo en Liverpool" (26 de enero de 2021).
17. *Véase* USPIS, artículo sobre estafas, Fraude con cheques (1 de mayo de 2019).
18. En el caso de los fraudes con cheques relacionados con el robo de correo, las mulas de dinero suelen ser jóvenes y son cómplices del fraude. En ciertos casos, las organizaciones delictivas buscan personas sin hogar y adictos solicitándoles que sean mulas de dinero y dándole una parte de los cheques cambiados.

En todo caso, una vez depositado el cheque, los delincuentes suelen retirar rápidamente los fondos mediante un ATM o realizar un giro postal que controlan para cubrir más sus ganancias ilícitas. Los delincuentes también pueden explotar a las víctimas utilizando información de identificación personal que se encuentra en el correo robado para futuras estafas como el fraude de tarjeta de crédito o fraude de cuentas de crédito.[19]

Señales de alerta financiera en relación con el fraude con cheques relacionado con el robo de correo

FinCEN, en coordinación con USPIS, ha identificado las señales de alerta para ayudar a las instituciones financieras a detectar, evitar y reportar la actividad sospechosa en relación con el fraude con cheques relacionados con el robo de correo, muchos de los cuales se solapan con las señales de alerta de fraudes con cheques en general. Dado que ninguna señal de alerta única es determinante de actividad ilícita o actividad sospechosa, las instituciones financieras deben considerar los hechos y circunstancias circundantes, como la actividad financiera histórica de un cliente, si las transacciones están en línea con las prácticas comerciales predominantes, y si el cliente exhibe múltiples alertas rojas antes de determinar si un comportamiento o transacción es sospechoso o de otra manera indicativo de fraude con cheques relacionados con el robo de correo. Junto con el abordaje basado en riesgos para el cumplimiento de BSA, también se anima a las instituciones financieras a realizar debida diligencia adicional cuando proceda.

1. Retiros de grandes importes poco característicos de la cuenta de un cliente mediante cheques para nuevos beneficiarios.
2. Denuncias de clientes de cheques robados del correo y luego depositado en cuentas desconocidas.
3. Denuncias de clientes de que un cheque que enviaron por correo nunca fue recibido por el beneficiario.
4. Los cheques utilizados para retirar fondos de la cuenta de un cliente parecen ser de un tipo de cheque o papel de cheque notablemente diferente al de los cheques utilizados por el banco emisor y al de los cheques utilizados para transacciones conocidas y legítimas.
5. Un cliente existente sin antecedentes de depósitos tiene nuevos depósitos repentinos de cheques y retiro o transferencia de fondos.
6. Hay depósitos de cheques no característicos, repentinos y anormales, a menudo electrónicos, seguidos de retiros o transferencias de fondos rápidos.

19. *Véase de forma general* DOJ, comunicado de prensa, "Delincuente reincidente con libertad supervisada admite el robo de correo y se declara culpable de fraude de giros bancarios" (7 de junio de 2022).

7. La evaluación de cheques sospechosos revela escritura borrada debajo de escritura más oscura, lo cual da la apariencia de que se ha sobrescrito el texto original.

8. Las cuentas sospechosas pueden tener indicadores de otras actividades sospechosas, como fraudes relacionados con la pandemia.[20]

9. Un cliente nuevo abre una cuenta que parece utilizar solo para el depósito de cheques, seguido de retiros y transferencias de fondos frecuentes.

10. Alguien que no es cliente que intenta cambiar un cheque de importe alto o varios cheques de importe alto en persona y, cuando una institución financiera los interroga, proporciona una explicación sospechosa o que posiblemente indica la actividad de una mula de dinero.

Línea directa para víctimas que quieran reportar fraudes con cheques relacionados con el robo de correo.

Además de presentar un SAR, según corresponda, las instituciones financieras deberían dirigir a los clientes que puedan ser víctimas de fraude con cheques relacionados con el robo de correo a USPIS al 1-877-876-2455 o https://www. uspis.gov/report para reportar el incidente.

Consejos de USPIS para evitar el robo de correo

FinCEN recomienda como buena práctica que las instituciones financieras dirijan a sus clientes a www.uspis.gov/tips-prevention/mail-theft para ver consejos de USPIS sobre cómo protegerse contra el robo de correo.

Si los clientes parecen ser víctimas de un robo que implica giros postales de USPS, pueden dirigirse a https://www.usps.com/shop/money-orders.htm para ver una guía sobre cómo reemplazar un giro postal robado.

20. *Véase* FinCEN, "Asesoría sobre delitos financieros dirigidos a pagos de impacto económico por COVID-19" (24 de febrero de 2021); DOJ, comunicado de prensa, "Trabajadores postales de Queens acusados de sobornos y robo de correo relacionado con el fraude de beneficios de COVID-19" (12 de agosto de 2022); DOJ, comunicado de prensa, "Acusado sentenciado por robo de correo y posesión de correo robado, incluyendo estímulos con cheques" (28 de junio de 2021).

Recordatorio de obligaciones y herramientas de BSA pertinentes para instituciones financieras de EE. UU.

Informe de actividad sospechosa
Otro informe pertinente de BSA
LEY PATRIOTA DE EE.UU. Artículo 314(b) Autoridad para compartir información

Informe de actividad sospechosa

Una institución financiera está obligada a presentar un SAR si sabe, sospecha o tiene razones para sospechar que una transacción realizada o que se intentó a través de la institución financiera involucra fondos derivados de actividades ilegales; está destinada o realizada para disfrazar fondos derivados de actividades ilegales; está diseñada para evadir las regulaciones promulgadas conforme la BSA; carece de un propósito comercial o aparentemente legal; o involucra el uso de la institución financiera para facilitar la actividad criminal.[21] Todas las instituciones financieras definidas por estatuto pueden reportar voluntariamente transacciones sospechosas bajo el actual refugio seguro de informes de actividad sospechosa.[22]

Cuando una institución financiera presenta un SAR, se requiere que mantenga una copia del SAR y el original o el equivalente en registros comerciales de cualquier documentación de respaldo durante un período de cinco años a partir de la fecha de presentación del SAR.[23] Las instituciones financieras deben proporcionar cualquier documentación solicitada que respalde la presentación de un SAR a petición de FinCEN o una agencia de supervisión o las agencias de ley y orden.[24] Cuando se solicite proporcionar documentación de respaldo, las instituciones financieras deben tener especial cuidado para verificar que el solicitante de información es, de hecho, un representante de FinCEN o una agencia de supervisión o las agencias de ley y orden. Una institución financiera debe incorporar procedimientos para dicha verificación en su programa de cumplimiento de la BSA o programa de AML. Estos procedimientos pueden incluir, por ejemplo, la verificación independiente de empleo con la oficina de campo del solicitante o la revisión cara a cara de las credenciales del solicitante.

Instrucciones para presentar un SAR

FinCEN solicita que las instituciones financieras indiquen una conexión entre la actividad sospechosa que se reporta y las actividades destacadas en esta alerta, incluyendo el término clave "**FIN-2023-MAILTHEFT**" en el campo 2 del SAR (Nota de la presentación de archivo

21. *Véase* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, y 1030.320.
22. *Véase* 31 USC § 5318(g)(3). Las instituciones financieras pueden reportar transacciones sospechosas independientemente de la cantidad involucrada y aun así aprovechar el refugio seguro.
23. *Véase* 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).
24. *Id. Véase también* FinCEN, "Documentación de respaldo para el informe de actividad sospechosa" (13 de junio de 2007).

a FinCEN), así como en la narrativa y seleccionando **el campo 34(d) en un SAR (fraude con cheque)**. Las instituciones financieras pueden resaltar palabras clave adicionales de asesoramiento o alerta en la narrativa, si corresponde.

Las instituciones financieras que quieren acelerar su informe de transacciones sospechosas que pueden estar relacionadas con la actividad indicada en esta alerta debería llamar a la línea gratuita para instituciones financieras al (866) 556-3974 (7 días a la semana, 24 horas al día).[25]

Las instituciones financieras deben incluir toda la información disponible relacionada con la(s) cuenta(s) y ubicación(es) involucradas en la actividad reportada, información de identificación y descripciones de cualquier entidad legal o acuerdos involucrados y los propietarios beneficiarios asociados, y cualquier información sobre personas o entidades relacionadas involucradas en la actividad. Las instituciones financieras también deben proporcionar toda la información disponible sobre otras instituciones financieras nacionales y extranjeras involucradas en la actividad; cuando sea apropiado, las instituciones financieras deberían considerar presentar un SAR conjuntamente sobre actividad sospechosa compartida.[26]

Otros requisitos de informes pertinentes de BSA

Las instituciones financieras y otras entidades o personas también pueden tener otros requisitos de informes pertinentes de la BSA para proporcionar información en relación con el tema de esta alerta. Estos incluyen obligaciones relacionadas con el Informe de transacciones en efectivo (CTR, por sus siglas en inglés),[27] Informe de pagos en efectivo de más de $10,000 recibidos en un comercio o negocio (Formulario 8300),[28] Informe de cuentas bancarias y financieras extranjeras (FBAR, por sus siglas en inglés),[29] Informe de transporte internacional de moneda o instrumentos monetarios (CMIR, por sus siglas en inglés),[30] Registro de negocios de servicios monetarios (RMSB, por sus siglas en inglés),[31] y Designación de persona exenta (DOEP, por sus siglas en

25. El propósito de la línea de emergencia es acelerar la presentación de información a las fuerzas de seguridad. Las instituciones financieras deberían reportar de inmediato cualquier amenaza inminente a los oficiales locales de las agencias del orden.
26. *Véase* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A) (2).
27. Un informe de cada depósito, retiro, cambio de moneda, u otro pago o transferencia, por, a través, o a una institución financiera que involucra una transacción en moneda de más de $10,000. Se pueden agregar varias transacciones al determinar si se ha alcanzado el umbral de informe. *Véase* 31 CFR §§ 1010.310-313, 1020.310¬313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, y 1026.310-313.
28. Un informe presentado por un comercio o negocio que recibe divisas por más de $10,000 en una transacción o dos o más transacciones relacionadas. Las transacciones deben ser reportadas en un formulario conjunto de FinCEN/ Servicio de Impuestos Internos cuando no se requiere que se informen en un CTR. *Véase* 31 CFR § 1010.330; 31 CFR § 1010.331. Un formulario 8300 también puede ser presentado voluntariamente para cualquier transacción sospechosa, incluso si el monto total no supera los $10,000.
29. Un informe presentado por una persona de EE. UU. que tiene un interés financiero, o firma u otra autoridad sobre cuentas financieras extranjeras con un valor agregado que supera los $10,000 en cualquier momento durante el año calendario. *Véase* 31 CFR § 1010.350; formulario 114 de FinCEN.
30. Un formulario presentado para reportar sobre el transporte de más de $10,000 en divisas u otros instrumentos monetarios hacia o desde los Estados Unidos. *Véase* 31 CFR § 1010.340.
31. Un formulario presentado para registrar un negocio de servicios monetarios (MSB) con FinCEN, o para renovar dicho registro. *Véase* 31 CFR § 1022.380.

inglés).[32] Estos requisitos de informes estándar pueden no tener una conexión obvia con la financiación ilícita, pero finalmente pueden resultar muy útiles para las agencias de ley y orden.

Instrucciones para presentar el Formulario 8300

Al presentar un formulario 8300 que involucra una transacción sospechosa relevante para esta alerta, FinCEN solicita que el presentador seleccione ***Caja 1b*** ("transacción sospechosa") e incluya el término clave "**FIN-2023-MAILTHEFT**" en la sección de "**Comentarios**" del informe.

Compartir información

Compartir información con instituciones financieras es crucial para identificar, reportar y prevenir los fraudes con cheques relacionados con el robo de correo u otras actividades financieras ilícitas. Se recuerda a las instituciones financieras y asociaciones de instituciones financieras que comparten información según el puerto seguro autorizado por el artículo 314(b) de la Ley PATRIOTA DE EE.UU. que pueden compartir información entre sí con respecto a personas, entidades, organizaciones y países que sean sospechosos de posible financiación del terrorismo y lavado de dinero.[33] FinCEN recomienda compartir dicha información de forma voluntaria.

Para más información

Las preguntas sobre el contenido de esta alerta deben dirigirse a la Sección de Apoyo Regulatorio de FinCEN en frc@fincen.gov.

32. Un informe presentado por los bancos para eximir a ciertos clientes de los requisitos de informes de transacciones de divisas. *Véase* 31 CFR § 1010.311.
33. *Véase* FinCEN, "La hoja informativa del artículo 324(b)" (diciembre de 2020).