FinCEN AVISO

FIN-2020-A003

7 de julio de 2020

Aviso sobre estafas de impostores y esquemas de "mulas de dinero" relacionados con la enfermedad por coronavirus 2019 (COVID-19)

Detectar, prevenir y notificar el fraude a los consumidores y otras actividades ilícitas relacionadas con el COVID-19 es vital para nuestra seguridad nacional, así como para preservar iniciativas y esfuerzos legítimos de ayuda y proteger a personas inocentes de todo daño.

Este aviso debería comunicarse a:

- *Directores ejecutivos*
- *Directores de operaciones*
- *Directores de cumplimiento*
- *Directores de riesgos*
- *Departamentos de ALD/BSA*
- *Departamentos jurídicos*
- *Departamentos de ciberseguridad*
- *Agentes de servicio al cliente*
- *Cajeros de banco*

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

La FinCEN solicita a las instituciones financieras que citen este aviso en el campo 2 del SAR (Nota de la institución depositaria a la FinCEN) y la narrativa introduciendo la siguiente expresión clave: "**COVID19 MM FIN-2020-A003**" y que seleccionen el campo 34(z) del SAR (Fraude-otro). Hacia el final del presente aviso figuran orientaciones adicionales para completar los SAR.

Introducción

La Red contra los Delitos Financieros (FinCEN, por sus siglas en inglés) emite este aviso para alertar a las instituciones financieras sobre un mayor número de estafas médicas observadas durante la pandemia de COVID-19. Este aviso contiene descripciones de estafas de impostores y esquemas de "mulas de dinero", estudios de casos, indicadores financieros y señales de alerta en ambos casos e información sobre la notificación de actividades sospechosas.

Este aviso tiene por objeto ayudar a las instituciones financieras a detectar, prevenir y notificar posibles actividades ilícitas relacionadas con el COVID-19. Se basa en el análisis que realiza la FinCEN de la información relacionada con elCOVID-19 obtenida de datos proporcionados en virtud de la Ley de Secreto Bancario (BSA, por sus siglas en inglés), informes de dominio público y colaboradores de agencias de ley y orden. La FinCEN publicará información relativa al COVID-19 para ayudar a las instituciones financieras a mejorar sus esfuerzos para detectar, prevenir y notificar actividades ilícitas sospechosas en su sitio web, https://www.fincen.gov/coronavirus (en inglés), que también contiene información sobre la manera de inscribirse para recibir información actualizada de la FinCEN (en inglés).

Señales de alerta de estafas de impostores y esquemas de "mulas de dinero" relacionados con el COVID-19

Entre los fraudes a los consumidores se encuentran las estafas de impostores y los esquemas de "mulas de dinero", en los que las partes intervinientes engañan a las víctimas haciéndose pasar por organismos del gobierno federal, organizaciones internacionales o entidades de beneficencia. La FinCEN ha definido las señales de alerta que se describen a continuación, para advertir a las instituciones financieras sobre esos fraudes y ayudarlas a detectar, prevenir y notificar transacciones sospechosas asociadas a la pandemia del COVID-19.

Dado que ningún indicador financiero o señal de alerta es por sí solo necesariamente un indicio de actividad ilícita o sospechosa, antes de determinar si una transacción es sospechosa o indicativa de actividad posiblemente fraudulenta relacionada con el COVID-19 las instituciones financieras deberían tener en cuenta otras informaciones contextuales y los hechos y circunstancias conexos, como el historial de actividad financiera del cliente, si las transacciones se ajustan a las prácticas comerciales imperantes y si el cliente presenta múltiples indicadores. En consonancia con el enfoque basado en el riesgo para el cumplimiento de la BSA, también se alienta a las instituciones financieras a realizar indagaciones e investigaciones adicionales cuando proceda. Además, algunas de las señales de alerta que se describen a continuación pueden aplicarse a múltiples actividades fraudulentas relacionadas con el COVID-19.

Estafas de impostores

En esta clase de estafas los delincuentes se hacen pasar por organizaciones, como organismos gubernamentales, grupos sin fines de lucro, universidades o entidades de beneficencia para ofrecer servicios fraudulentos o estafar de otra manera a las víctimas. Si bien las estafas de impostores pueden adoptar múltiples formas, la metodología básica implica a una persona 1) que contacta a un blanco con el falso pretexto de representar a una organización oficial, y (2) lo coacciona o convence para que proporcione fondos o información valiosa, realice una acción que cause la infección de su computadora con un programa maligno, o difunda información falsa[1]. En el caso de los esquemas vinculados al COVID-19, los impostores pueden fingir ser funcionarios o representantes del Servicio de Impuestos Internos (IRS, por sus siglas en inglés)[2], los Centros para el Control y la Prevención de Enfermedades (CDC, por sus siglas en inglés)[3], la Organización Mundial de la Salud (OMS o WHO, por sus siglas en inglés), otros grupos de atención médica o sin fines de lucro e instituciones académicas.[4]

1. *Véase* el Blog de actividades de la Comisión Federal del Comercio (FTC, por sus siglas en inglés), "Seven Coronavirus Scams Targeting Your Business", (25 de marzo de 2020).
2. Para obtener información sobre estafas de impostores de IRS en general, *véase* el artículo de la FTC "Estafas de impostores del IRS", (enero de 2020).
3. *Véase* el Anuncio de servicio público del Centro de Denuncias de Delitos por Internet (IC3) del Buró Federal de Investigaciones (FBI, por sus siglas en inglés), "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic", (20 de marzo de 2020).
4. La FTC mantiene enlaces a recursos relacionados con estafas y las tendencias actuales que ha observado. *Véase* "Las estafas relacionadas con el Coronavirus" de la FTC.

Los agentes ilícitos pueden servirse de estafas de impostores para defraudar o engañar a las personas vulnerables, entre ellas los ancianos y las personas desempleadas, solicitándoles pagos (como pagos digitales y monedas virtuales), donaciones o información personal por correo electrónico, llamadas automáticas, mensajes de texto[5] u otros métodos de comunicación. Por ejemplo, un impostor puede contactar a las posibles víctimas por teléfono, correo electrónico o mensaje de texto y dar a entender a la víctima que debe verificar datos personales o enviar pagos a estafadores a cambio de prestaciones o pagos de estímulo relacionados con el COVID-19, incluidos pagos de impacto económico[6] en el marco de la Ley de Ayuda, Alivio y Seguridad Económica por Coronavirus (Ley CARES, por sus siglas en inglés)[7]. Otro caso es el de impostores que contactan a sus víctimas fingiendo ser representantes del gobierno o del sector de atención médica que participan en actividades de rastreo de contactos relacionadas con el COVID-19 y dan a entender que la víctima debe compartir datos personales o financieros en el marco de esa labor[8]. Se pueden citar múltiples ejemplos, entre ellos esquemas de *phishing* (ataque por suplantación de identidad), en los que los impostores envían comunicaciones que parecen provenir de fuentes legítimas para obtener datos personales y financieros de las víctimas y posiblemente infectar sus dispositivos, para lo cual convencen al blanco de descargar un archivo adjunto malicioso o hacer clic en enlaces fraudulentos.[9]

5. Para obtener información sobre las estafas de impostores relacionadas con el COVID-19 realizadas por mensajes de texto o llamadas telefónicas, véase el artículo página de la Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés), "Estafas relacionadas con el coronavirus - Recursos para el consumidor", (20 de mayo de 2020). La FTC y la FCC han enviado cartas de advertencia a múltiples proveedores de servicios de Protocolo de Transmisión de Voz por Internet (VoIP) por presuntamente encaminar llamadas de venta telefónica o llamadas automáticas fraudulentas relacionadas con la pandemia. *Véase* el comunicado de prensa de la FTC, "FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls", (20 de mayo de 2020).

6. Los pagos de impacto económico pueden administrarse en forma de depósitos por cámara de compensación automática (ACH), cheques Departamento del Tesoro de los Estados Unidos o tarjetas de débito prepagada. *Véase* el comunicado de prensa del Departamento del Tesoro de los Estados Unidos (el Tesoro) "Treasury is Delivering Millions of Economic Impact Payments by Prepaid Debit Card", (18 de mayo de 2020).

7. La FTC, el IRS y el Inspector General del Departamento del Tesoro para la Administración Tributaria publicaron por separado información sobre estafas de impostores, en particular las relacionadas con los pagos de impacto económico. *Véase* el blog de la FTC, "¿Quieres recibir tu cheque de ayuda para aliviar el impacto económico causado por el coronavirus? Los estafadores también", (1 de abril de 2020) y "Cheques por el coronavirus: aplanemos la curva de las estafas:", (8 de abril de 2020); el boletín informativo del IRS, "IRS emite advertencia de estafas relacionadas con el Coronavirus; cuidado con esquemas atados a pagos de impacto económico", (2 de abril de 2020) y del Centro de Información de Pago de Impacto Económico del IRS, (8 de abril de 2020); así como el comunicado de prensa del Inspector General del Departamento del Tesoro para la Administración Tributaria, "TIGTA Urges Taxpayers to "Be On High Alert" For Coronavirus Relief Payment Scams", (7 de abril de 2020).

8. *Véase* el comunicado de prensa del Departamento de Justicia (DOJ, por sus siglas en inglés) "U.S. Attorney Warns Public of COVID-19 Contact Tracing Frauds", (28 de mayo de 2020).

9. *Véase* la alerta de la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA, por sus siglas en inglés) del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) y del Centro Nacional de Ciberseguridad (NCSC, por sus siglas en inglés) del Reino Unido, "COVID-19 Exploited by Malicious Cyber Actors" (8 de abril de 2020); y el artículo del DHS, "Common Scams: Know How to Spot a Fake". Además, *véase* el artículo sobre seguridad cibernética de la OMS, "Beware of Criminals Pretending to be WHO" (abril de 2020). *Véase también* el blog de la FTC, "Estafas relacionadas con el COVID-19 dirigidas contra estudiantes universitarios," (27 de mayo de 2020); y el comunicado de prensa del DOJ, "Federal Law Enforcement Encourages the Public to Remain Vigilant to Covid-19 Scams", (22 de abril de 2020).

Los estafadores también pueden hacerse pasar por obras de beneficencia legítimas o crear falsas entidades de caridad, aprovechar la generosidad del público y malversar donaciones destinadas a las actividades de respuesta al COVID-19.[10] Para engañar al público, con frecuencia los delincuentes utilizan modalidades como cuentas de medios sociales, recaudación puerta a puerta, folletos, envíos, teléfono y llamadas automáticas, mensajes de texto, sitios web y correos electrónicos que simulan obras benéficas y organizaciones sin fines de lucro legítimas. Esas operaciones pueden incluir en sus títulos términos como "socorro", "fondo", "donación" y "fundación", para dar la impresión de que se trata de una organización legítima.[11]

Dado que muchos estafadores pueden dirigirse a clientes y no a las instituciones financieras directamente, estas deberían estar alerta a posibles actividades sospechosas en el momento de interactuar con sus clientes. A continuación, se presentan algunas señales de alerta de estafas de impostores:

1. Un cliente que indica que una persona que pretendía ser representante de un organismo gubernamental le contactó por teléfono, correo electrónico, mensaje de texto o medios sociales para solicitarle datos personales o de su cuenta bancaria con miras a verificar, tramitar o acelerar el pago de impacto económico, el seguro de desempleo u otras prestaciones[12]. En particular, esté alerta a las comunicaciones en las que se hace hincapié en el "cheque de estímulo" o el "pago de estímulo" en solicitudes al público, a veces argumentando que la entidad fraudulenta puede acelerar el proceso de obtención del "cheque de estímulo" u otro pago gubernamental en nombre del beneficiario por una comisión que ha de pagarse mediante tarjeta de regalo o tarjeta prepagada.

2. El recibo de un documento que parece ser un cheque o una tarjeta de débito prepagada del Departamento del Tesoro de los Estados Unidos, a menudo por un monto inferior al previsto en el pago de impacto económico, con instrucciones para contactar al organismo gubernamental fraudulento por teléfono o en línea, para verificar datos personales con miras a recibir la totalidad de la prestación.

10. Múltiples Oficinas de Fiscales de los Estados Unidos advierten sobre la actividad de delincuentes que pueden pretender explotar de las iniciativas de socorro legítimas para su propio beneficio ilícito, solicitando donaciones para entidades de caridad falsas o sitios de financiación participativa. *Véanse* la Oficina del Fiscal de los Estados Unidos para el Distrito Sur de Georgia, "U.S. Attorney Warns of Coronavirus Scams Targeting Vulnerable Victims", (25 de marzo de 2020); la Oficina del Fiscal de los Estados Unidos para el Distrito Este de Oklahoma, "Department of Justice Requests Citizens be Aware of And Report COVID-19 Fraud", (24 de marzo de 2020); y la Oficina del Fiscal de los Estados Unidos para el Distrito Central de Tennessee, "U.S. Attorney and FBI Urge the Public to Report Suspected Fraud Related to Tornado Destruction and COVID-19", (23 de marzo de 2020). Además, la Comisión de Bolsa y Valores (SEC, por sus siglas en inglés) señaló las posibilidades de que surjan fraudes de inversión benéfica, en los que las partes intervinientes alegan falsamente que las inversiones otorgarán apoyo financiero o tratamiento médico a personas necesitadas, pero en lugar de ello el dinero es robado. *Véanse* los boletines y las alertas de la SEC para inversionistas, "Frauds Targeting Main Street Investors -- Investor Alert" (10 de abril de 2020). *Véase también* la información de la FTC para evitar estafas en nombre de obras benéficas, "Haz valer tus donaciones para la crisis por coronavirus", (5 de mayo de 2020).

11. *Véase* el artículo de la FTC, "Cómo donar sabiamente y evitar estafas de caridad".

12. Para obtener más información sobre los pagos de impacto económico, consulte el sitio del IRS, "Centro de Información de Pago de Impacto Económico" (30 de junio de 2020).

3. Comunicaciones no solicitadas de supuestas fuentes fiables o de programas gubernamentales relacionados con el COVID-19, en las que se indica a los lectores que abran hipervínculos o archivos adjuntos o que proporcionen datos personales o financieros, incluidas las credenciales de la cuenta (es decir, nombres de usuario y contraseñas).

4. Direcciones de correo electrónico en la correspondencia sobre el COVID-19 que no corresponden al nombre del remitente, contienen errores ortográficos o no terminan en el dominio correspondiente de la organización de la que presuntamente proviene el mensaje. Por ejemplo, los organismos gubernamentales utilizan los dominios ".gov" o ".mil". Muchas obras benéficas legítimas utilizan la extensión ".org". Los correos electrónicos de la OMS contienen la extensión "@who.int". En cambio, es posible que los estafadores utilicen ".com" o ".biz" en vez del dominio esperado.

5. La correspondencia de correo electrónico que contiene un asunto identificado por el gobierno o la industria como vinculado a empresas de phishing o contiene hipervínculos o direcciones de páginas web hacia supuestos recursos para el COVID-19 que tienen URL irregulares (por ejemplo, variaciones mínimas en las extensiones de dominios como ".com," ".org," y ".us"). Algunos ejemplos de asuntos de correos electrónicos identificados por el Gobierno de los Estados Unidos como phishing relacionado con el COVID-19 son "2020 Coronavirus Updates" (información actualizada sobre el coronavirus 2020), "Coronavirus updates" (información actualizada sobre el coronavirus), "2019-nCov: New confirmed cases in your City" (2019-nCov: nuevos casos confirmados en su ciudad) y "2019-nCov: Coronavirus outbreak in your city (Emergency)" (2019-nCov: brote de coronavirus en su cuidad (Emergencia))."[13]

6. Solicitudes en las que la persona, el correo electrónico o la publicidad en medios sociales pide donaciones en nombre de una organización prestigiosa, pero no está asociada a esa organización (es decir, el solicitante no es reconocido ni avalado por la organización como empleado o voluntario, la dirección de correo electrónico contiene errores ortográficos o no está vinculada a la organización o la publicidad en los medios sociales dirige a las personas a un sitio web no asociado).

7. Una organización de beneficencia que solicita donaciones: (1) que no tiene una historia pormenorizada, informes financieros, declaraciones anuales al IRS, ni documentación de su estatuto de exención impositiva; o (2) cuya existencia no puede verificarse utilizando diversos recursos en línea que permitan confirmar la presencia del grupo y su condición de entidad sin fines de lucro.

13. *Véase* la alerta de la CISA del DHS CISA y de la NCSC del Reino Unido, "COVID-19 Exploited by Malicious Cyber Actors," (8 de abril de 2020).

Esquemas de "mulas de dinero"

Una "mula de dinero" es una persona que transfiere dinero obtenido de manera ilegal en nombre de otra persona o bajo su dirección[14]. Los esquemas de "mulas de dinero", incluidos los relacionados con la pandemia del COVID-19, abarcan el espectro de utilización de "mulas de dinero" involuntarias, conocedoras o cómplices[15]. Una "mula de dinero" **involuntaria** o **no conocedora** es una persona que desconoce que forma parte de un esquema delictivo más amplio. La persona está motivada por la confianza que deposita en un verdadero romance, puesto de trabajo o propuesta[16]. Una "mula de dinero" **conocedora** es una persona que escoge ignorar las alertas evidentes o actúa cerrando deliberadamente los ojos a su actividad de movimiento de dinero. La persona está motivada por la obtención de un beneficio financiero o por la reticencia a reconocer el papel que desempeña[17]. Una "mula de dinero" **cómplice** es una persona que tiene conocimiento de su papel como "mula de dinero" y es cómplice en el esquema delictivo más amplio. La persona está motivada por la obtención de un beneficio financiero o por su lealtad al grupo delictivo[18]. Durante la pandemia de COVID-19 las autoridades de los Estados Unidos detectaron a reclutadores que utilizaban esquemas de "mulas de dinero", como el del buen samaritano, el romance o el trabajo a domicilio[19]. Las autoridades de los Estados Unidos también identificaron a delincuentes que se utilizan a "mulas de dinero" para explotar programas de seguro de desempleo durante la pandemia de COVID-19.[20]

14. *Véase* el documento del FBI, "Money Mule Awareness", (julio de 2019). Para obtener más información sobre las "mulas de dinero" en general, *consulte* el artículo de la FinCEN, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes", (16 de julio de 2019); "FinCEN Analysis: Bank Secrecy Act Reports Filed by Financial Institutions Help Protect Elders from Fraud and Theft of Their Assets" (4 de diciembre de 2019); y del DOJ, "Justice Department Announces Landmark Money Mule Initiative" (4 de diciembre de 2019).
15. Para obtener más información sobre las personas involuntarias, conocedoras o cómplices que participan en esquemas de "mulas de dinero", *consulte* el documento del FBI, "Money Mule Awareness" (julio de 2019).
16. Para consultar ejemplos de la manera en que se recluta y se utiliza a una "mula de dinero" involuntaria, *véase ídem*, pág. 4.
17. Para consultar ejemplos de la manera en que se recluta y se utiliza a una "mula de dinero" conocedora, *véase ídem*, pág. 5.
18. Para consultar ejemplos de la manera en que se recluta y se utiliza a una "mula de dinero" cómplice, *véase ídem*.
19. El FBI ha publicado información sobre la manera en que los delincuentes se están aprovechando de la pandemia de COVID-19 para robar dinero, acceder a datos personales y financieros y utilizar a personas como "mulas de dinero". *Véase* el comunicado de prensa del FBI, "FBI Warns of Money Mule Schemes Exploiting the COVID-19 Pandemic" (6 de abril de 2020). En los esquemas de trabajo a domicilio, por ejemplo, los encargados de reclutar a "mulas de dinero" para el COVID-19 pueden acercarse a los blancos, con una identidad falsa de entidad de beneficencia o empresa, con una oferta legítima de empleo y el pretexto de proporcionarle trabajo a domicilio. Esto se realiza a menudo por medio de publicidades en internet o en los medios sociales, correos electrónicos o mensajes de texto. Cuando acepta el "empleo", el blanco recibe instrucciones de movilizar fondos a través de cuentas bancarias o de crear una nueva cuenta a su nombre para la "empresa". El blanco (es decir, la "mula de dinero") gana dinero recibiendo un porcentaje de los fondos que ayudó a transferir siguiendo las instrucciones del "empleador". Para obtener más información sobre ofertas de trabajo fraudulentas, *véase* el blog de la FTC, "¿Estás buscando trabajo después de los despidos causados por el coronavirus?" (13 de abril de 2020).
20. *Véanse* los artículos del Departamento para la Seguridad del Empleo del Estado de Washington, "Statement from Commissioner Suzi LeVine on the rise in unemployment imposter fraud attempts" (14 de mayo de 2020) y "Update on imposter fraud from Commissioner Suzi LeVine" (18 de mayo de 2020).

Entre las señales de alerta de los esquemas de "mulas de dinero" para el COVID-19 se encuentran las siguientes:

8. El cliente comienza a recibir en su cuenta bancaria personal transacciones que no se ajustan a su historial de transacciones, incluidas operaciones en el exterior, la compra de grandes sumas de monedas virtuales convertibles o transacciones en grandes cantidades, o la cuenta solía tener saldo bajo hasta que el cliente comenzó a participar en un esquema de "mulas de dinero". Cuando se le interroga acerca de los cambios en las transacciones, el cliente se niega a llenar documentos de "conozca a su cliente" o a responder preguntas con respecto a las fuentes de los fondos, y tal vez cite como fuente de ingresos actividades de socorro para el COVID-19 o una oportunidad de "trabajo a domicilio".

9. El cliente abre una nueva cuenta bancaria a nombre de una empresa y, poco después, una persona transfiere los fondos fuera de la cuenta. Esta persona podría ser el titular de la cuenta registrado u otra persona, y tal vez conserve una parte del dinero que ha transferido (por orden del estafador). Si bien esa actividad en sí puede no resultar sospechosa, podría serlo si la persona responde de manera insatisfactoria a las preguntas formuladas por la institución financiera, se niega a proporcionar documentos fundamentales sobre "conozca a su cliente", cita como fuente de los fondos actividades de socorro para el COVID-19 u oportunidades de "trabajo a domicilio".

10. El cliente abre cuentas a su nombre en múltiples bancos de modo de poder recibir dinero de diversas personas o empresas. Después transfiere el dinero a otras cuentas por orden de su presunto empleador.

11. El cliente recibe en su cuenta o en múltiples cuentas de la misma institución financiera varios pagos del seguro estatal de desempleo, con los mismos intervalos de desembolso (por ejemplo, pagos semanales o quincenales), efectuados por uno o varios estados.

12. El cliente recibe en su cuenta un depósito de desempleo de otro estado en el que presuntamente reside o ha trabajado previamente.

13. El cliente recibe en su cuenta pagos de un seguro de desempleo por numerosos empleados, o el nombre del titular de la cuenta y el nombre que figura en el campo "enviar a" del pago ACH no concuerdan.

14. Los fondos depositados son rápidamente desviados mediante giro bancario a cuentas en el extranjero ubicadas en países conocidos por tener controles deficientes en materia de lavado de dinero.

15. El cliente hace una o más transacciones atípicas que involucran cuentas en el extranjero, especialmente mediante métodos de pago inusuales para el cliente. Cuando se le interroga acerca de la transacción, el cliente indica que está destinada a una persona que vive en el extranjero, que necesita asistencia financiera debido a la pandemia del COVID-19.

16 La documentación de cliente muestra que el supuesto empleador o encargado de la contratación utiliza un servicio de correo electrónico común, gratuito y basado en la web en vez de un correo electrónico específico de una empresa. Por ejemplo, en vez de contar con una dirección de correo electrónico específica de una empresa u organización, como first.lastname@ABCcompany.com o lastname@XYZ_NGO.org, la dirección pertenece a un proveedor de direcciones de correo electrónico común y gratuito.

17 El cliente informa de que su presunto empleador le solicitó que recibiera fondos en su cuenta bancaria personal, de modo que ese empleador pudiera posteriormente tramitar o transferir los fondos fuera de la cuenta personal del cliente mediante un giro bancario, ACH, un correo electrónico o empresas de servicios de dinero.

18 El cliente declara, o la información muestra, que una persona, tal vez desconocida por el cliente hasta el momento, solicitó asistencia financiera para enviar o recibir fondos por intermedio de la cuenta personal del cliente. Esto incluye solicitudes realizadas por personas que dicen ser:

a. Un miembro del servicio militar de los Estados Unidos que presuntamente está destinado en el extranjero;

b. Un ciudadano estadounidense que trabaja o viaja en el extranjero; o

c. Un ciudadano estadounidense que está cumpliendo cuarentena en el exterior.

Información sobre la notificación de actividades sospechosas

Instrucciones para presentar informes de actividades sospechosas (SAR)

La presentación de informes de actividades sospechosas (SAR, por sus siglas en inglés), junto con la instauración eficaz de los requisitos de debida diligencia por parte de las instituciones financieras, es crucial para identificar y poner fin a delitos financieros, incluidos los relacionados con la pandemia del COVID-19. Las instituciones financieras deberían proporcionar todos los datos pertinentes y disponibles en el SAR y en la descripción. La observancia de las instrucciones que figuran a continuación mejorará la capacidad de la FinCEN y de las agencias de ley y orden para identificar adecuadamente los SAR procesables utilizando el sistema Query de la FinCEN y extraer información para respaldar las investigaciones relacionadas con el COVID-19.

- La FinCEN solicita a las instituciones financieras que citen este aviso incluyendo la expresión clave: "COVID19 MM FIN-2020-A003" en el campo 2 del SAR (nota de la institución depositaria a la FinCEN) y la narrativa para indicar el vínculo entre la actividad sospechosa que se está notificando y las actividades destacadas en el presente aviso.

- Las instituciones financieras también deberían seleccionar el campo 34(z) (Fraude-otro) del SAR como el tipo de actividad sospechosa conexo para indicar un vínculo entre la actividad sospechosa que se está notificando y el COVID-19. Dichas instituciones deberían incluir en el campo 34(z) del SAR el tipo de fraude o el nombre de la estafa o producto (por ejemplo, estafas de impostores o esquemas de "mulas de dinero"). Además, la FinCEN alienta a las instituciones financieras a denunciar ciertos tipos de estafas de impostores y de esquemas de "mulas de dinero" en los campos 34(1) (Fraude-comercialización masiva) o 38(d) (Otras actividades sospechosas —Explotación financiera de ancianos) del SAR, según corresponda en función de la actividad sospechosa.
- Consulte el anuncio denominadoFinCEN's "Notice Related to the Coronavirus Disease 2019" (COVID-19), que contiene información sobre la notificación de delitos relacionados con el COVID-19 y recuerda a las instituciones financieras ciertas obligaciones estipuladas en la BSA.

Para obtener más información

Las instituciones financieras deberían enviar sus preguntas o comentarios relativos al contenido del presente Aviso a la Oficina de Apoyo Regulatorio (Regulatory Support Section) de la FinCEN, escribiendo a frc@fincen.gov.

FinCEN tiene como misión proteger el sistema financiero de un uso ilícito, así como combatir el lavado de dinero y contribuir a la seguridad nacional mediante la recopilación, el análisis y la difusión de información de inteligencia financiera y el uso estratégico de sus facultades financieras.