FinCEN AVISO

FIN-2020-A005 **30 de julio de 2020**

Aviso sobre delitos cibernéticos y delitos perpetrados mediante tecnologías cibernéticas que explotan la pandemia de la enfermedad del coronavirus 2019 (COVID-19)

Detectar, prevenir y notificar las transacciones ilícitas y la actividad cibernética asistirá en la protección de las labores legítimas de ayuda para la pandemia del COVID-19 y a proteger las instituciones financieras y a sus clientes contra los cibercriminales malignos y los autores estatales de amenazas.

Este aviso debería comunicarse a:

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

Solicitud de presentación de informes de actividad sospechosa (SAR):

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 descripción introduciendo la siguiente expresión clave: "COVID19-CYBER FIN-2020-A005" y que seleccionen el campo 42 del SAR (Evento cibernético). Hacia el final del presente aviso figuran pautas adicionales para completar el SAR.

Introducción

La Red contra los Delitos Financieros (FinCEN, por sus siglas en inglés) emite este aviso para alertar a las instituciones financieras sobre posibles indicadores de delitos cibernéticos y delitos perpetrados mediante las tecnologías cibernéticas observados durante la pandemia del COVID-19. Un sin número de individuos que cometen actos ilícitos participan en estafas fraudulentas que explotan las vulnerabilidades generadas por la pandemia. Este aviso presenta descripciones de ciberataques y estafas cibernéticas, señales de alerta, así como información sobre como notificar actividades sospechosas, todos en relación con el COVID-19.

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 el COVID-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 la ley y el orden. La FinCEN seguirá publicando información relativa al COVID-19 para las instituciones financieras con el fin de ayudarlas a mejorar sus esfuerzos para detectar, prevenir y

notificar actividades ilícitas sospechosas en su sitio web, https://www.fincen.gov/coronavirus, que también contiene información sobre la manera de inscribirse para recibir información actualizada de la FinCEN.

Señales de alerta de delitos cibernéticos y delitos perpetrados mediante tecnologías cibernéticas que explotan el COVID-19

Este aviso aborda los medios principales por los cuales cibercriminales y los autores estatales de amenazas explotan cada vez más la pandemia del COVID-19 a través de delitos perpetrados mediante las tecnologías cibernéticas por medio de programas malignos (*malware*) y suplantación de la identidad (*phishing*), extorsión, compromiso de correo electrónico de negocios (*business email compromise* o BEC, por sus siglas en inglés) y explotación de aplicaciones remotas, sobre todo contra sistemas financieros y de salud.[1]

La FinCEN ha identificado las siguientes señales de alerta de delitos perpetrados mediante tecnologías cibernéticas que explotan el COVID-19[2] con el propósito de ayudar a las instituciones financieras a detectar, prevenir y notificar operaciones sospechosas relacionadas con la pandemia del COVID-19. Dado que ninguna señal de alerta es por sí sola un indicio de actividad ilícita o sospechosa, 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 antes de determinar si una transacción es sospechosa o indicativa de actividad posiblemente fraudulenta relacionada con el COVID-19. 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. Ya que muchos estafadores pueden tener en su punto de mira a los clientes, las instituciones financieras deberían permanecer en alerta para detectar actividades sospechosas que involucren a sus clientes.

1. Véase el comunicado de prensa del Departamento de Justicia (DOJ), "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams" (22 de abril de 2020); el comunicado de prensa del Centro Nacional de Ciberseguridad (National Cyber Security Centre, NCSC) del Reino Unido, "Public Urged to Flag Coronavirus Related Email Scams as Online Security Campaign Launches" (21 de abril de 2020); la notificación de la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) del Departamento de Seguridad Nacional (DHS), "Defending Against COVID-19 Cyber Scams" (6 de marzo de 2020); el informe de la Europol, "Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis" (27 de marzo de 2020); el anuncio de servicio público de la DHS CISA y el Buró Federal de Investigaciones (FBI), "People's Republic of China (PRC) Targeting of COVID-19 Research Organizations" (13 de mayo de 2020); el anuncio de servicio público del Centro de Denuncias de Delitos por Internet (IC3) del FBI, "Increased Use of Mobile Banking Apps Could Lead to Exploitation" (10 de junio de 2020); y el aviso conjunto de la DHS CISA, la Agencia de Seguridad Nacional, el NCSC y el Centro de la Seguridad de las Telecomunicaciones de Canadá (Canada Communications Security Establishment), "APT29 Targets COVID-19 Vaccine Development" (16 de julio de 2020).
2. Para los fines de este aviso, los delitos perpetrados mediante las tecnologías cibernéticas hacen referencia a las actividades ilícitas (como el fraude, robo de identidad, etc.) que se llevan a cabo, o se facilitan, por medio de sistemas electrónicos y dispositivos como redes y computadoras. Véase el Aviso de la FinCEN, FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime" (25 de octubre de 2016).

Ataque y explotación de las plataformas y procesos remotos

La importante migración hacia el acceso remoto durante la pandemia presenta oportunidades a los criminales para explotar los sistemas remotos de las instituciones financieras y los procesos dirigidos a sus clientes. Los cibercriminales y las amenazas estatales se aprovechan de las vulnerabilidades de las aplicaciones remotas y del entorno virtual para robar información confidencial, poner en peligro la actividad financiera e interrumpir las operaciones comerciales[3]. Los procesos de identificación remota[4] también enfrentan riesgos importantes que pueden incluir:

- *Manipulación digital de documentos de identidad:* Los criminales intentan frecuentemente debilitar los procesos de verificación de identidad en línea valiéndose de documentos de identificación fraudulentos. Estos se pueden generar mediante la manipulación de imágenes digitales de documentos de identidad legítimos emitidos por un gobierno para alterar la información o las fotos que contienen.[5]

- *Aprovechar las credenciales comprometidas para acceder a distintas cuentas:* Los cibercriminales frecuentemente se aprovechan de la debilidad de procesos de autenticación para intentar tomar el control de cuentas, valiéndose de métodos como los llamados ataques con credenciales comprometidas o *credential stuffing*. En estos ataques, los cibercriminales usan listas de credenciales de cuentas robadas, como nombres de usuarios o correos electrónicos y sus contraseñas, para llevar a cabo intentos de acceso automáticos con el fin de obtener acceso no autorizado a las cuentas de las víctimas.

3. Para obtener información relativa a vulnerabilidades y exposiciones de ciberseguridad difundidas al público, véase la "National Vulnerability Database del Instituto Nacional para estándares y tecnología (National Institute for Standards and Technology, NIST) del Departamento de Comercio de los EE. UU.;" MITRE, "Common Vulnerabilities and Exposures: CVE List Home"; y los anuncios de servicio público del FBI IC3, "Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments", (1 de abril de 2020) y "Increased Use of Mobile Banking Apps Could Lead to Exploitation", (10 de junio de 2020). Véase también el discurso preparado de antemano que presentó el director de la FinCEN Kenneth A. Blanco en la "Consensus Blockchain Conference (Virtual)" (13 de mayo de 2020).

4. Para los fines de este aviso, "procesos de identidad remota" incluye los procesos remotos de integración de los clientes y de verificación de identidad, así como la autenticación de los clientes para fines de acceso a cuentas. Para obtener más información sobre los criterios de identidad digital, véase las pautas del NIST, "Digital Identity Guidelines" (1 de diciembre de 2017) y el Grupo de Acción Financiera Internacional (GAFI), "Guidance on Digital Identity" (6 de marzo de 2020).

5. Los criminales que explotan los procesos de verificación de identidad por lo general utilizan información conexa a la identidad de una persona real (conocido como robo de identidad) o fabrican una nueva identidad que por lo general consiste de un identificador real, como un número de seguro social, o de licencia de conducir, junto a otra información falsa (conocido como fraude de identidad sintético). Para más información sobre ejemplos de tipologías e indicadores de alerta financieros que involucren el robo o fraude de identidad, véase el informe de la FinCEN, "Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports" (octubre de 2010).

Las señales de alerta financiera de este tipo de actividad pueden incluir:[6]

1. La ortografía de los nombres en la información de la cuenta no corresponde a los documentos de identidad emitidos por el gobierno que se proporcionan para la apertura de la cuenta en línea.
2. Las fotos en los documentos de identidad están borrosas, tienen baja resolución o muestran aberraciones, sobre todo alrededor de la cara. Las fotos en los documentos de identidad u otras imágenes de personas presentadas en los procesos de verificación de identidad remota[7] muestran indicios visuales que apuntan a una posible manipulación de la imagen (por ejemplo: incongruencias en la coloración cercana a los márgenes de la cara o bordes o líneas dobles en los rasgos faciales).
3. Las imágenes de los documentos de identidad que muestran irregularidades son indicio de manipulación digital de las imágenes, especialmente alrededor de los campos de datos que posiblemente se cambiarían para llevar a cabo un fraude de identidad sintético (por ejemplo, nombre, dirección y otros datos de identificación).
4. La descripción física del cliente en los documentos de identidad que no corresponde a otras imágenes del cliente.
5. Un cliente que se rehúsa a proporcionar documentos de identidad suplementarios o se retrasa al proporcionar documentos adicionales.
6. Inicios de sesión a través de múltiples cuentas aparentemente no relacionadas que se producen desde un solo dispositivo o una sola dirección de protocolo de Internet (dirección IP) y, por lo general, en un periodo corto de tiempo.
7. La dirección IP vinculada con los inicios de sesión no corresponde a la dirección indicada en los documentos de identidad.
8. Los inicios de sesión de los clientes que se producen dentro de un patrón de alto tráfico de la red, conjuntamente con una reducción de accesos con éxito y un aumento del restablecimiento de contraseñas.
9. Un cliente que llama a la institución financiera para cambiar los métodos de comunicación de la cuenta y la información de autenticación, y luego intenta rápidamente llevar a cabo operaciones en una cuenta que nunca antes había recibido pagos de ese cliente.

6. Id. Véanse también las pautas interinstitucionales sobre la detección, prevención y mitigación del robo de identidad (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation), Título 16 del Código de Reglamentos Federales, Parte 681, apéndice A.
7. Las imágenes que se utilizan en la verificación de identidad que no sean documentos de identidad pueden ser fotos o vídeos del cliente (como imágenes tipo selfi) que se toman como parte del proceso de integración de la institución financiera.

Suplantación de la identidad, programas malignos y extorsión

La FinCEN y las agencias de ley y orden de los EE. UU. han observado un considerable aumento en las campañas de suplantación de la identidad extensas y focalizadas que intentan atraer a compañías, sobre todo del sector salud y a proveedores farmacéuticos, con ofertas de información e insumos relacionados con el COVID-19.[8] Las estafas de suplantación de la identidad van dirigidas a las personas por medio de comunicaciones que aparentan venir de fuentes legítimas para recopilar información personal y financiera de las víctimas, así como potencialmente infectar sus dispositivos electrónicos al convencer a la víctima para que descargue programas malignos.[9] Por lo general, los cibercriminales envían las comunicaciones de suplantación de la identidad por correo electrónico, pero también lo podrían hacer por medio de llamadas telefónicas o mensajes de texto.

En estos nuevos esquemas de fraude, los estafadores que suplantan la identidad hacen referencia frecuentemente a temas relacionados con el COVID-19, como los pagos relativos a la Ley de Ayuda, Alivio y Seguridad Económica por Coronavirus (CARES, por sus siglas en inglés),[10] en la línea de asunto y el contenido del mensaje de los correos electrónicos. Algunos correos electrónicos de suplantación de la identidad atraen a las víctimas mediante anuncios sobre métodos para generar dinero, por ejemplo, inversiones en monedas virtuales convertibles (CVC, por sus siglas en inglés) o nombres de dominio que emulan nombres de organizaciones, como las que proporcionan u otorgan capacidades de teletrabajo.[11] Los cibercriminales también distribuyen programas malignos,[12] incluido el secuestro de datos o *ransomware*, a través de correos de suplantación de identidad, descargas y sitios web malignos, secuestro de los sistemas de nombres de dominio (DNS, por sus siglas en inglés) o *spoofing* y aplicaciones móviles fraudulentas. Estas técnicas se pueden aplicar en campañas más amplias que involucran redes sociales, como el reciente ataque que tuvo como blanco a Twitter y a usuarios famosos de esa plataforma.[13] Las instituciones

8. El Servicio Secreto de los Estados Unidos (USSS) y la DHS CISA han observado un aumento en la cantidad de campañas de suplantación de la identidad, programas malignos y extorsión vinculadas al COVID-19. Véase el comunicado de prensa del USSS, "Secret Service Issues COVID-19 (Coronavirus) Phishing Alert" (9 de marzo de 2020).
9. Véase el aviso conjunto de la DHS CISA y del NCSC del Reino Unido (AA20-099A), "COVID-19 Exploited by Malicious Cyber Actors" (8 de abril de 2020); y del DHS, "Common Scams: Know How to Spot a Fake."
10. Ley pública. 116–136, Congreso 116 (2020).
11. Desde enero de 2020, se han registrado docenas de miles de dominios nuevos con términos relacionados con el COVID-19- o con labores de respuesta ante desastres o del sector salud (por ejemplo, "cuarentena", "vacuna" y "CDC"). Muchos de ellos incluyen nombres o imitan nombres de compañías que proporcionan capacidades de teletrabajo o las facilitan. Las agencias de ley y orden de los EE. UU. han desmantelado cientos de dominios con nombres malignos que se utilizaban para explotar la pandemia. Véase el Aviso de la FinCEN,, FIN-2020-A003, "Aviso sobre estafas de impostores y esquemas de "mulas de dinero" relacionados con la enfermedad por coronavirus 2019 (COVID-19)" (7 de julio de 2020). Véase también, el comunicado de prensa del FBI, "FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic" (13 de abril de 2020).
12. Los programas malignos pueden permitir a los criminales acceder a computadoras y sistemas de computadoras comprometidos para robar credenciales, filtrar información confidencial mediante mecanismos como las capturas de pantalla o el registro del tecleo, cambiar la información de cuentas y llevar a cabo transacciones fraudulentas.
13. Véase la alerta de la FinCEN, FIN-2020-Alert001, "FinCEN Alerts Financial Institutions to Convertible Virtual Currency Scam Involving Twitter" (16 de julio de 2020).

financieras que manejan CVC deberían estar especialmente alertas al uso potencial de sus instituciones para el lavado de las ganancias vinculadas a los delitos cibernéticos, las actividades ilícitas en el mercado del *darknet*, también conocida como red oscura, y otras estafas relacionadas con las CVC, y tomar las medidas adecuadas para mitigar el riesgo, de conformidad con sus obligaciones respecto de la BSA.

La FinCEN estima que los casos de extorsión también seguirán en aumento tras la pandemia del COVID-19. En lo que va de 2020, la FinCEN ha recibido numerosos informes de actividad sospechosa (SAR, por sus siglas en inglés) que implican secuestros de datos (*ransomware*)[14] que tienen como blanco a centros médicos y municipios. Gran parte de estos secuestros de datos se transmitieron mediante el uso de señuelos conexos al COVID-19 mencionados anteriormente. Pronosticamos que los criminales seguirán centrándose en entidades vulnerables involucradas en la respuesta a la pandemia, como los investigadores de tratamientos médicos o los fabricantes de equipo de protección personal. En otros casos de extorsión, los criminales amenazan con exponer a las víctimas y a sus familiares al COVID-19 si no pagan la cantidad de dinero que se exige. En casi todos los casos, los criminales exigen que los pagos vinculados a la extorsión se hagan en CVC.[15]

Las señales de alerta financiera de este tipo de actividad pueden incluir, entre otros:

10 La actividad de empresas en tecnología de la información relacionada a los procesos de operaciones o información está vinculada a indicadores cibernéticos relacionados con posibles actividades ilícitas. La actividad cibernética maliciosa podría ser evidente en los archivos de registros del sistema, tráfico de red o información de archivos.[16]

11 Las direcciones de correo que supuestamente están vinculadas al COVID-19 no corresponden al nombre del emisor o al dominio correspondiente de la compañía que presuntamente envía el mensaje.

14. El secuestro de datos o ransomware es un tipo de programa maligno que por lo general encripta datos en sistemas con el fin de extorsionar pagos de rescate de las víctimas a cambio de descifrar la información y devolver acceso a las víctimas a sus sistemas.

15. Las instituciones financieras que manejan CVC deberían prestar especial atención al lavado de ganancias vinculadas con los delitos cibernéticos, la actividad en el mercado de la darknet y otras estafas conexas a las CVC. Véase el Aviso de la FinCEN, FIN-2019-003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (9 de mayo de 2019).

16. Ya que los indicadores cibernéticos son señales de alerta útiles que las instituciones financieras pueden aprovechar para detectar actividad financiera conexa y sospechosa, la FinCEN, la DHS CISA y la Oficina de Ciberseguridad y Protección de la Infraestructura Crítica del Departamento del Tesoro de los EE. UU. (OCCIP, DOT) ofrecen una amplia gama de recursos en materia de indicadores cibernéticos, como: las listas de indicadores cibernéticos de la FinCEN (CILs), las cuales se difunden a través del Sistema de intercambio seguro de información de la FinCEN (FinCEN Secure Information Sharing System); las listas de indicadores cibernéticos y circulares de la OCCIP, que se encuentran disponibles a petición del interesado; y los productos y servicios de análisis cibernético de la DHS CISA, incluida una lista abarcadora de indicadores de ataques vinculados con el COVID-19 en formato CSV o STIX de XML , el Programa de intercambio de información y colaboración cibernética o Cyber Information Sharing and Collaboration Program (CISCP), y el Programa de intercambio de indicadores automático o Automated Indicator Sharing (AIS) program. Las asociaciones público-privadas y de la industria, como el Centro de intercambio de información de servicios financieros (Financial Services Information Sharing and Analysis Center), y los canales de dominio público y comerciales sobre amenazas cibernéticas también pueden ser recursos útiles.

12 Los correos electrónicos no solicitados conexos al COVID-19 de fuentes que no son de confianza animan a los lectores a abrir enlaces o archivos insertados, o a proporcionar información personal o financiera, como nombres de usuario y contraseñas u otras credenciales de las cuentas.

13 Los correos electrónicos de fuentes que no son de confianza o de direcciones similares a cuentas legítimas de proveedores de teletrabajo que ofrecen programas para aplicaciones remotas y que los ofrecen de manera gratuita o a un costo reducido.

14 Los correos que contienen "líneas de asunto" que el gobierno o la industria ha determinado están vinculadas con campañas de suplantación de identidad, como "Coronavirus Updates", "2019-nCov: New confirmed cases in your City", y "2019-nCov: Coronavirus outbreak in your city (Emergency)").

15 Los mensajes de texto con enlaces insertados que alegan provenir de programas de asistencia o pagos del gobierno, o estar vinculados con ellos.

16 Los enlaces insertados o direcciones de páginas web con supuestos recursos vinculados con el COVID-19 cuyos localizadores uniformes de recursos (URL, por sus siglas en inglés) no corresponden al sitio web que debería dirigirse o son similares a sitios web legítimos, pero muestran leves diferencias en el dominio (por ejemplo, cambios en las extensiones de dominio como ".com", ".org," y ".us") o en ortografía de la dirección en la web.

Compromiso de correo electrónico de negocios (BEC, por sus siglas en inglés)

Los cibercriminales explotan la pandemia del COVID-19, cada vez con mayor frecuencia, a través de las estafas BEC y tienen como blanco particular los municipios y la cadena de suministro del sector salud. Una estafa BEC común consiste en criminales que convencen a compañías a redirigir pagos a nuevas cuentas, alegando que el cambio se debe a modificaciones en las operaciones empresariales debido a la pandemia. Los criminales que realizan las estafas BEC tienden a usar cuentas de correo electrónico comprometidas, también conocidas como cuentas de correo electrónico suplantadas o *spoofed accounts*, para comunicar estos cambios de pago de último minuto y urgentes. En el contexto del COVID-19, los criminales se insertan en las comunicaciones y se hacen pasar por una persona crucial en una relación u operación de negocios. Por lo general fingen ser proveedores de suministros sanitarios, para interceptar un pago de insumos que se necesitan urgentemente o inducir de forma fraudulenta un pago de esta índole.[17]

17. Véase el comunicado de prensa del FBI, "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic" (6 de abril de 2020). Véase también el comunicado de prensa de la Europol, "Corona Crimes: Suspect Behind €6 Million Face Masks and Hand Sanitisers Scam Arrested Thanks to International Police Cooperation" (6 de abril de 2020).

Las señales alerta de este tipo de actividad incluyen las siguientes:[18]

17 Las instrucciones de operación de un cliente contienen detalles distintos, como el lenguaje, el plazo de tiempo y las cantidades, en comparación con instrucciones de operaciones previas, sobre todo cuando se trata de operaciones que involucran a proveedores del sector de la salud o de compras de insumos.

18 Las instrucciones de transacciones que, por lo general, involucran a una contraparte del sector de la salud o que hacen referencia a la compra de insumos sanitarios o de respuesta ante emergencias y que provienen de una cuenta de correo electrónico que se asemeja mucho a la cuenta de correo electrónico de un cliente de confianza, pero no es idéntica a ella.

19 Las instrucciones de transacciones enviadas por correo electrónico que indican que se envíe el pago directamente a una cuenta diferente a la de un beneficiario de confianza. El transmisor puede alegar que necesita cambiar la cuenta receptora como parte de la respuesta a la pandemia del COVID-19, como mover la cuenta a una institución financiera en una jurisdicción que se vea menos afectada por la enfermedad, e indicar que es urgente que se realice la transacción debido a la pandemia.

20 Las instrucciones de transacciones enviadas por correo que solicitan que se cambie el método de pago de cheques a transferencia bancaria (o transferencia de la cámara de compensación automatizada, ACH, por sus siglas en inglés) en respuesta a la pandemia.

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.

18. Para obtener señales de alerta generales sobre las estafas BEC, véanse los avisos de la FinCEN, FIN-2016-A003, "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes" (6 de septiembre de 2016), y FIN-2019-A005, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes" (16 de julio de 2019).

- La FinCEN solicita a las instituciones financieras que citen este aviso incluyendo la expresión clave: "**COVID19-CYBER FIN-2020-A005**" en el campo 2 del SAR (nota de la institución depositaria a la FinCEN) y la descripción para indicar el vínculo entre la actividad sospechosa que se está notificando y las actividades destacadas en el presente aviso.
- Las instituciones financieras que sospechen una actividad fraudulenta relacionada con el COVID-19 deberían marcar todas las casillas correspondientes en el formulario de SAR para indicar que existe un vínculo entre el COVID-19 y la actividad sospechosa sobre la que se está informando. Por ejemplo, si la actividad incluye la apropiación de una cuenta que implica una transferencia ACH relacionada con el COVID-19, las instituciones financieras pueden seleccionar los campos SAR 38a y 38z del SAR y anotar en el recuadro "otros", "apropiación por fraude de cuenta COVID-19 – ACH"("*COVID-19 account takeover fraud – ACH*").[19]
- Las instituciones financieras también deberían incluir todos los indicadores cibernéticos técnicos pertinentes relacionados con los eventos cibernéticos y las transacciones conexas sobre los que se informa en el SAR dentro de los campos disponibles de indicadores estructurados de eventos cibernéticos. Por ejemplo, para un evento cibernético relacionado con el COVID-19 contra una institución financiera, las instituciones financieras pueden seleccionar los campos del SAR 42a y 42z (anotando en el recuadro "otro" el evento cibernético relacionado con el COVID-19), y los campos del SAR 44(a)-(j), (z), incluyendo direcciones de correo electrónico o de billetera CVC, dominios o URL malignos, y cualquier otro indicador de evento cibernético conocido.
- En el caso de los delitos cibernéticos que impliquen un fraude conexo al COVID-19, las instituciones financieras deberían seleccionar el campo SAR 34z (Fraude - otros)/(Fraud – other) como el tipo de actividad sospechosa asociada. Además, las instituciones financieras deberían incluir el tipo de delito o fraude cibernético como palabra clave (por ejemplo, "Fraude de COVID 19 BEC", "fraude EAC" o "robo de datos BEC"/"COVID 19 BEC Fraud," "EAC fraud," o "BEC data theft") en el campo 34(z) del SAR.
- Por favor, consulte la notificación del 18 de mayo de 2020 de la FinCEN "Notice Related to the Coronavirus Disease 2019", o en español, el "Aviso sobre estafas médicas relacionadas con la enfermedad del coronavirus de 2019 (COVID-19)" de la misma fecha, que contienen información sobre la denuncia de delitos relacionados con el COVID-19 y el Programa de Respuesta Rápida de la FinCEN, y que recuerda a las instituciones financieras sobre ciertas obligaciones de la BSA.

19. Para obtener pautas adicionales sobre cómo detectar la apropiación de una cuenta y las instrucciones para presentar informes SAR sobre el tema, véase el aviso de la FinCEN, FIN-2011-A016, "Account Takeover Activity" (19 de diciembre de 2011).

Para obtener más información

Las instituciones financieras deberían enviar sus preguntas o comentarios relacionados al contenido del presente aviso a la Oficina de Apoyo Regulatorio 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.