Instituto Costarricense sobre Drogas

BOLETÍN UIF 76-2020

14 DE JULIO, 2020

AVISO DE FINCEN SOBRE ESTAFAS DE IMPOSTORES Y ESQUEMAS DE MULAS DE DINERO RELACIONADOS CON LA ENFERMEDAD POR CORONAVIRUS 2019 (COVID-19)

La Unidad de Inteligencia Financiera de Costa Rica, desea compartir con el Sistema Antilavado y contra el Financiamiento al Terrorismo del país, un extracto del Aviso FIN-2020-A003 – FinCEN Advisory, emitido por la UIF homóloga de los Estados Unidos FinCEN, el cual esboza una serie de indicadores y banderas rojas detectadas en ese país, mediante el análisis de información obtenida de diversas fuentes por parte de dicha entidad, en donde se previene y se insta a reportar posibles conductas delictivas relacionadas con el COVID-19. El Aviso completo se puede acceder en el siguiente enlace:

https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a003

RESUMEN DEL AVISO FIN-2020-A003:

La Red de Cumplimiento de Delitos Financieros (FinCEN por sus siglas en inglés) está emitiendo este aviso para alertar a las instituciones financieras sobre posibles indicadores de estafas de impostores y esquemas de mulas de dinero, que son dos formas de fraude al consumidor observadas durante la pandemia COVID-19. Muchos actores ilícitos están involucrados en esquemas fraudulentos que explotan las vulnerabilidades creadas por la pandemia. Este aviso contiene descripciones de estafas de impostores y esquemas de mulas de dinero, con indicadores para ambos casos de banderas rojas financieras, e información para el reporte de operaciones sospechosas.

Este aviso está destinado a ayudar a las instituciones financieras a detectar, prevenir y reportar posibles actividades delictivas relacionadas con COVID- 19. Este aviso se basa en el análisis de FinCEN de información relacionada con COVID-19, de datos obtenidos de la Ley de Secreto Bancario (BSA), informes de código abierto y socios encargados de hacer cumplir la ley. FinCEN emitirá información relacionada con COVID-19 a las instituciones financieras para ayudar a mejorar sus esfuerzos para detectar, prevenir e informar de presuntas actividades ilícitas en su sitio web, en la dirección https://www.fincen.gov/coronavirus.

INDICADORES DE BANDERAS ROJAS FINANCIEROS DE COVID-19 ESTAFAS IMPOSTORES Y ESQUEMAS DE MULAS DE DINERO

Los fraudes de los consumidores incluyen estafas de impostores y esquemas de mulas de dinero, donde los actores engañan a las víctimas haciéndose pasar por agencias del gobierno federal, organizaciones internacionales o de caridad. FinCEN identificó los indicadores de bandera roja financiera descritos a continuación para alertar a las instituciones financieras sobre estos fraudes y para ayudar a las instituciones financieras a detectar, prevenir y reportar operaciones sospechosas asociadas con la pandemia COVID-19.

Dado que ningún indicador de bandera roja financiera es necesariamente indicativo de actividades ilícitas o sospechosas, las instituciones financieras deben considerar información contextual adicional y los hechos circundantes y circunstancias, como la actividad financiera histórica de un cliente, si las transacciones están en línea con las prácticas comerciales prevalecientes, y si el cliente exhibe múltiples indicadores, antes de determinar si una transacción es sospechosa o de otro modo indicativo de actividades potencialmente fraudulentas relacionadas con COVID-19. De conformidad con su enfoque basado en riesgo para el cumplimiento de la Ley de Secreto Bancario, también se alienta a las instituciones financieras a realizar consultas adicionales e investigaciones cuando proceda. Adicionalmente, algunos de los indicadores de bandera roja financieros que se describen a continuación pueden aplicarse a múltiples actividades fraudulentas relacionadas con COVID-19.

ESTAFAS DE IMPOSTORES

En las estafas de impostores, los delincuentes se hacen pasar por organizaciones como agencias gubernamentales, grupos sin fines de lucro, universidades u organizaciones benéficas para ofrecer servicios fraudulentos o de otra manera defraudar a las víctimas. Mientras que las estafas de impostores pueden tomar múltiples formas, la metodología básica implica un actor (1) ponerse en contacto con un objetivo bajo el falso pretexto de representar a una organización oficial, y (2) coaccionar o convencer al objetivo para proporcionar fondos o información valiosa, participar en el comportamiento que hace que el equipo del objetivo esté infectado con malware, o propagar la desinformación. En el caso de los esquemas relacionados con COVID-19, los impostores pueden presentarse como funcionarios o representantes del Servicio de Impuestos Internos (IRS), los Centros para el Control y la Prevención de Enfermedades (CDC), la Organización Mundial de la Salud (OMS), otros grupos de salud o sin fines de lucro, e instituciones académicas.

Los actores ilícitos pueden utilizar estafas para defraudar y engañar a los vulnerables, incluidos los ancianos y desempleados, a través de la solicitud de pagos (como pagos digitales y moneda virtual), donaciones, o información personal por correo electrónico, robocalls, mensajes de texto, u otros métodos de comunicación. Por ejemplo, un impostor puede ponerse en contacto con posibles víctimas por teléfono, correo electrónico o texto para dar a entender que la víctima debe verificar la información personal o enviar pagos a los estafadores a cambio de pagos o beneficios de estímulo relacionados con COVID-19, incluidos los pagos o beneficios de impacto económico (EIP) bajo la Ley de Ayuda, Alivio y Seguridad Económica (CARES) de Coronavirus. Otra instancia incluye a los impostores que se comunican con las víctimas y se hacen pasar por representantes gubernamentales o de atención médica en las actividades de rastreo de contactos COVID-19, lo que implica que una víctima debe compartir información personal o financiera como parte de los esfuerzos de rastreo de contactos. Múltiples ejemplos incluyen esquemas de phishing, donde los impostores envían comunicaciones que parecen provenir de fuentes legítimas, para recopilar los datos personales y financieros de las víctimas y potencialmente infectar sus dispositivos convenciendo al objetivo de descargar un adjunto malicioso o hacer clic en enlaces maliciosos.

Los estafadores también pueden hacerse pasar por organizaciones benéficas legítimas o crear falsas organizaciones benéficas, aprovechando la generosidad del público y malversando donaciones destinadas a los esfuerzos de respuesta COVID-19.

Los delincuentes a menudo utilizan cuentas de redes sociales, cobros puerta a puerta, folletos, envíos, y robocalls, mensajes de texto, sitios web y correos electrónicos imitando organizaciones benéficas legítimas y organizaciones sin fines de lucro para defraudar al público. Estas operaciones pueden incluir palabras como "alivio", "fondo", "donación" y "fundación" en sus títulos para dar la ilusión de que son una organización legítima.

Dado que muchos estafadores pueden estar apuntando a los clientes en lugar de las instituciones financieras directamente, las instituciones financieras, al interactuar con sus clientes, deben permanecer alerta para posibles actividades sospechosas. Indicadores de bandera roja financieros por estafas de impostores, pueden incluir:

1. Un cliente que indica que una persona que dice representar a una agencia gubernamental se comunicó con él o ella por teléfono, correo electrónico, mensaje de texto o redes sociales pidiendo información personal o de cuenta bancaria para verificar, procesar o agilizarlos beneficios de impacto económico, seguro de desempleo u otros beneficios. En particular, esté alerta a las comunicaciones que hacen hincapié en el "cheque de estímulo" o "pago de estímulo" en las solicitudes al público, a veces alegando que la entidad fraudulenta puede agilizar el "cheque de estímulo" u otro pago gubernamental en nombre del beneficiario por una comisión pagada con tarjeta de regalo o tarjeta de prepago.

2. Recibo de un documento que parece ser un cheque o una tarjeta de débito prepagada de la Tesorería de los EE. UU., a menudo en una cantidad inferior a los beneficios de impacto económico esperado, con instrucciones para contactar a la agencia gubernamental fraudulenta, a través de un número de teléfono o en línea, para verificar la información personal con el fin de recibir todo el beneficio.

3. Comunicaciones no solicitadas de fuentes de confianza o programas gubernamentales relacionados con COVID-19, indicando a los lectores que abran enlaces o archivos incrustados o que proporcionen información personal o financiera, incluidas las credenciales de la cuenta (por ejemplo, nombres de usuario y contraseñas).

4. Direcciones de correo electrónico en correspondencia COVID-19 que no coinciden con el nombre del remitente, contienen errores ortográficos o no terminan en el dominio correspondiente de la organización desde la que supuestamente se envió el mensaje. Por ejemplo, las agencias gubernamentales usarán ".gov" o ".mil." Muchas organizaciones benéficas legítimas usarán ".org." Los correos electrónicos de la OMS contendrán "@who.int. " Los estafadores, sin embargo, pueden usar ".com" o ".biz" en lugar del dominio esperado.

5. Correspondencia por correo electrónico que contiene líneas de asunto que el gobierno o la industria han identificado como asociadas con campañas de phishing, o que contiene enlaces incrustados o direcciones de páginas web para supuestos recursos COVID-19 que tienen URL irregulares (por ejemplo, ligeras variaciones en las extensiones de dominio como ".com", ".org" y ".us"). Algunos ejemplos identificados por el gobierno de los Estados Unidos de líneas de asunto de correo electrónico de phishing incluyen "2020 actualizaciones de Coronavirus", "actualizaciones de Coronavirus", "2019-ncov: Nuevos casos confirmados en tu ciudad" y "2019-ncov: Brote de coronavirus en tu ciudad (emergencia)"

6. Solicitudes en las que la persona, el correo electrónico o el anuncio en las redes sociales buscan en nombre de una organización de buena reputación, pero no está afiliado a la organización de buena reputación (por ejemplo, el abogado no es reconocido o respaldado como empleado o voluntario por la organización, la dirección de correo electrónico está mal escrita o no está conectada a la organización, o el anuncio de redes sociales dirige a las personas a un sitio web no afiliado).

7. Una organización caritativa que solicita donaciones que (1) no tiene una historia en profundidad, informes financieros, declaraciones anuales del IRS, documentación de su estado exento de impuestos, o (2) no pueden ser verificados mediante el uso de diversos recursos basados en Internet que pueden ayudar a confirmar la existencia del grupo y su estado sin fines de lucro.

ESQUEMAS DE MULAS DE DINERO

Una mula de dinero es "una persona que transfiere dinero adquirido ilegalmente en nombre de o bajo la dirección de otro". Los esquemas de mulas de dinero, incluidos los relacionados con la pandemia COVID-19, abarcan el espectro de usar mulas de dinero involuntarias, ingeniosas o cómplices. Una mula de dinero involuntaria o desconocida es una persona que "no es consciente de que él o ella es parte de un esquema criminal más grande". El individuo está motivado por su confianza en el romance real, puesto de trabajo o propuesta. Una mula de dinero consciente es una persona que "elige ignorar las banderas rojas obvias o actúa deliberadamente ciego a su actividad de movimiento de dinero." El individuo está motivado por ganancias financieras o una falta de voluntad para reconocer su papel. Una mula de dinero cómplice es un individuo que es "consciente de su papel como mula de dinero y es cómplice en el esquema criminal más grande." El individuo está motivado por la ganancia financiera o la lealtad a un grupo criminal. Durante la pandemia COVID-19, las autoridades estadounidenses han detectado reclutadores usando esquemas de mulas de dinero, como el buen samaritano, el romance y los planes de trabajo desde casa. Las autoridades estadounidenses también han identificado criminales que utilizan mulas de dinero para explotar los programas de seguro de desempleo durante la pandemia COVID-19.

Los indicadores de bandera roja financiera de los esquemas de mulas de dinero COVID-19 pueden incluir:

8. La cuenta bancaria personal del cliente comienza a recibir transacciones que no se ajustan a su perfil de historial transaccional, incluidas las transacciones en el extranjero, la compra de grandes sumas de moneda virtual convertible, o transacciones en grandes cantidades fiduciarias, o la cuenta generalmente tenía un saldo bajo hasta que el cliente se involucró en un esquema de mulas de dinero. Cuando se le pregunta sobre los cambios en las transacciones, el cliente rechaza las solicitudes de documentos o consultas de "conozca a su cliente" con respecto a fuentes de fondos, y puede mencionar COVID-19, trabajo de socorro o una oportunidad de "trabajo desde casa" como la fuente de los ingresos.

9. El cliente abre una nueva cuenta bancaria a nombre de una empresa y poco después, alguien transfiere los fondos fuera de la cuenta. La persona que transfiere los fondos podría ser el titular de la cuenta registrada u otra persona, y puede conservar una parte del dinero que transfirió (por instrucción del estafador). Si bien esta actividad, en sí misma, puede no ser sospechosa, puede llegar a serlo si el individuo proporciona respuestas insatisfactorias a las consultas de la institución financiera, se niega a proporcionar documentos esenciales de "conozca a su cliente", o menciona COVID-19, trabajo de socorro, o "trabajo desde casa" oportunidades como la fuente de los fondos.

10. El cliente abre cuentas a su nombre en varios bancos para que pueda recibir dinero de varias personas o empresas, luego mueve el dinero a otras cuentas bajo la dirección del supuesto empleador del cliente.

11. 11. El cliente recibe múltiples pagos de seguro de desempleo estatal a su cuenta, o a varias cuentas en la misma institución financiera, dentro del mismo plazo de desembolso (por ejemplo, pagos semanales o bisemanal) emitidos desde uno o varios estados.

12. La(s) cuenta(s) del cliente recibe un depósito de desempleo de un estado diferente en el que supuestamente reside o ha trabajado previamente.

13. La cuenta del cliente recibe pagos de seguro de desempleo para numerosos empleados o el nombre del titular de la cuenta y el nombre del pago de "remitir a" de la Cámara de Compensación Automatizada (Automated Clearing House - ACH) no coinciden.

14. Los fondos depositados se desvían rápidamente mediante transacciones bancarias a cuentas extranjeras ubicadas dentro de países conocidos por tener controles deficientes contra el lavado de dinero.

15. 15. El cliente realiza una o más transacciones atípicas que involucran una cuenta en el extranjero, especialmente a través de métodos de pago inusuales para el cliente. Cuando se le pregunta sobre la transacción, el cliente indica que es para una persona ubicada en el extranjero que necesita asistencia financiera debido a la pandemia COVID-19.

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

17. El cliente proporciona información que su supuesto empleador le pidió al cliente que recibiera fondos en su cuenta bancaria personal, para que el empleador pueda procesar o transferir fondos a través de transferencia bancaria, ACH, correo o servicios monetarios fuera de la cuenta personal del cliente.

18. El cliente afirma, o la información muestra, que una persona a quien el cliente puede no haber conocido previamente, solicitó asistencia financiera para enviar/recibir fondos a través de la cuenta personal del cliente, incluyen solicitudes de individuos que dicen ser:

    a. Miembro del Servicio de los E.E. UU. que según se informa está en el extranjero;

    b. Ciudadano estadounidense que trabaja o viaja al extranjero; o

    c. Ciudadano estadounidense en cuarentena en el extranjero.