

07 DE AGOSTO, 2020

BOLETÍN DE FINTRAC SOBRE TENDENCIAS EN LAVADO DE DINERO Y FRAUDES RELACIONADOS AL COVID-19

La Unidad de Inteligencia Financiera de Costa Rica, desea compartir un extracto del Boletín **20/21-SIRA-006** de la UIF homóloga en Canadá FINTRAC, en donde se advierte sobre fraudes y tendencias de lavado relacionadas al COVID-19. Esta información tiene como base primaria el análisis hecho por FINTRAC de transacciones reportadas relacionadas a COVID-19. La Alerta completa se puede acceder en el siguiente enlace:

<https://www.fintrac-canafe.gc.ca/intel/operation/covid-eng>

EXTRACTO DE LA ALERTA 20/21-SIRA-006:

La pandemia COVID-19 está teniendo un impacto significativo en la economía mundial. Aunque todavía es demasiado pronto para determinar si (o cómo) esta pandemia alterará el panorama del blanqueo de dinero, la crisis COVID-19 tiene importantes implicaciones para la delincuencia organizada al crear oportunidades nuevas o ampliadas significativas para la perpetración del fraude.

Por ejemplo, ha creado nuevas oportunidades para los delincuentes en el espacio de monedas virtuales en Canadá e internacionalmente. Los falsificadores se han centrado en la venta de kits de pruebas caseras y productos farmacéuticos COVID-19 falsos, y ofreciendo consejos no confirmados y a menudo falsos tratamientos de COVID-19 en la Internet y la red oscura, con transacciones realizadas utilizando monedas virtuales.

El mayor uso de los servicios en línea durante la pandemia también aumenta el riesgo de ciberdelincuencia. Los delincuentes cibernéticos están explotando la situación actual para dirigirse a individuos, empresas y entidades con COVID-19 con variedad de estafas populares de phishing y chantaje, que están llevando cada vez más a las víctimas a enviar moneda virtual para donaciones y pagos de rescate.

Las tendencias generales observadas en el lavado de dinero y el fraude, incluido el uso cada vez mayor de monedas virtuales, el aprovechamiento de las mulas (a menudo las propias víctimas) y el uso de productos y servicios ofrecidos por las instituciones financieras, probablemente continuarán para el lavado de los ganancias por fraudes de COVID-19.

Resumen de COVID-19 Reportes de Fraude

COVID-19 ha dado lugar a un aumento de categorías específicas de fraude, que los delincuentes han adaptado de los regímenes existentes. La presentación de informes al CAFC (Centro Anti Fraude de Canadá) indica una mayor dependencia de monedas virtuales y de los métodos de pago tradicionales ofrecidos por las instituciones financieras (es decir, pagos con tarjeta de crédito, transferencias electrónicas (eTransfers) y transferencias bancarias). Los informes relacionados con esquemas de phishing, fraude de identidad y estafas de mercancías, representan el 80% del fraude de mercancías relacionados al COVID-19 que ha sido reportado al CAFC, los cuales se describen a continuación.

Estafas de mercancías por COVID-19 incluyen ofertas para el suministro de máscaras faciales y otros equipos de protección personal y kits de prueba para COVID-19, curas y tratamientos no probados. De las estafas de mercancías reportadas por las víctimas a la CAFC, el 62% se refieren a individuos que compran máscaras faciales y no reciben el producto o reciben un producto inferior o falsificado; 18% se refieren a proveedores que venden todo tipo de equipos de protección personal (por ejemplo, batas, máscaras, guantes, desinfectantes, etc.) y personas que no reciben nada en absoluto o reciben productos inferiores o falsificados.

Indicadores de COVID-19. Fraude de Mercancías

- Comerciantes que venden kits de prueba COVID-19, curas y tratamientos, y servicios de descontaminación del hogar.
- Transacciones que implican la venta o adquisición de equipos de protección personal u otros suministros médicos o de higiene que están en alta demanda debido a la pandemia COVID-19, a precios significativamente rebajados.
- Clientes que proporcionan pagos a través de monedas virtuales, o dirigen fondos a un tercero no relacionado, especialmente aquellos en una jurisdicción de alto riesgo.
- Aparición repentina y alto volumen de eTransfers en cuentas bancarias de clientes que dicen estar involucrados en el ecommerce (también conocido como comercio electrónico o comercio por Internet). Los fondos se agotan inmediatamente o se reenvían a otra cuenta al recibirlos.
- El uso de cuentas bancarias personales con fines comerciales, en particular las vinculadas a plataformas de comercio electrónico.

Las estafas de phishing incluyen llamadas telefónicas, correos electrónicos y mensajes de texto de delincuentes que pretenden estar vinculados a Beneficios de Seguro de Empleo, Beneficio de Respuesta a Emergencias de Canadá (Canada Emergency Response Benefit - CERB), la Agencia de Salud Pública de Canadá u otras empresas. Las víctimas son dirigidas a hacer clic en un enlace o abrir un archivo adjunto, que puede contener malware o puede dirigirlos a sitios web falsos solicitándoles información personal y financiera. La mayoría de los informes presentados a la CAFC vinculados a la categoría de fraude de identidad, se relaciona al uso de la información personal de la víctima para aplicar a los pagos del CERB.

Indicadores de COVID-19. Fraude de Identidad y Beneficios de Emergencia

- El aumento repentino de las grandes transacciones que implican cuentas de clientes, donde había un saldo bajo y/o una actividad financiera previa limitada, o ese pago directo a un beneficiario con el que el cliente no tiene historial de pagos o relación comercial, puede indicar la victimización del fraude o el lavado de procedencias por actividades de fraude.
- Cuentas de receptoras para CERB (Canada Emergency Response Benefit/Beneficio de Respuesta a Emergencias de Canadá) recientemente abiertas, que carecen de las transacciones comerciales usuales asociadas con los gastos de la vida diaria.
- Cuentas bancarias abiertas durante la pandemia en un lugar que no es el lugar de residencia del cliente.
- El cliente retira totalmente los pagos del CERB depositados en la cuenta o reenvía los beneficios a otra cuenta, inmediatamente después de recibir los beneficios o después de un período de inactividad.

A medida que continúa la pandemia, la CAFC espera que es probable que las dificultades financieras a las que se enfrentan los ciudadanos y las empresas canadienses resulten en una mayor victimización. Las estafas de préstamos, los fraudes de consolidación de deudas y el fraude de inversión probablemente aumentarán. Además, los fraudes cibernéticos dependientes como el phishing de lanza, ransomware y campañas de phishing que están aprovechando el aumento de las actividades en línea (por ejemplo trabajando desde casa) de los canadienses, también es probable que aumenten.

Nota importante:

La información presentada en este boletín debe ser utilizada como inteligencia y de absoluta confidencialidad, su uso es reservado únicamente para fines de Cumplimiento, no puede ser puesta en conocimiento de terceras personas bajo ninguna circunstancia, lo cual será considerado una fuga de información y será denunciado a las autoridades competentes. La información puede ser utilizada para en la definición de parámetros de riesgo y la generación de alertas en sistemas, manteniendo la confidencialidad absoluta de la fuente. Queda a entera responsabilidad del Oficial de Cumplimiento y el Oficial Adjunto, como únicos destinatarios de la misma, sobre el uso que se dé a esta información diferente a los fines indicados por esta Unidad.