REPORTE DE ACTIVIDAD SOSPECHOSA (SAR)

J&A Global Compliance

DEFINICIÓN

Es un reporte que se presenta a las autoridades competentes cuando una entidad financiera o una persona sospecha que una transacción o actividad puede estar relacionada con el lavado de activos, el financiamiento del terrorismo u otras actividades ilícitas.

Directores, oficiales, empleados, agentes y contratistas actuales y anteriores tienen prohibido divulgar SAR.

No revele información sobre la existencia (o inexistencia) de un SAR.

Se pueden imponer sanciones civiles y penales

NUNCA informe o "avise" a ningún individuo en la transacción que es sospechoso. El Informe de actividad (SAR) no debe ser archivado o divulgado fuera del Banco

Sanciones civiles de hasta $ 100K por violación. Penas criminales de hasta $ 250K y / o encarcelamiento que no exceda 5 años.

TARJETA DE DÉBITO, CRÉDITO, PREPAGADAS EN EL MUNDO CRYPTO

J&A Global Compliance

Tumblers
herramienta que permite a los usuarios mezclar sus fondos de criptomonedas con los de otros usuarios para ocultar el origen y el destino de los fondos

Mercados no regulados

Tarjetas prepagadas

P2P

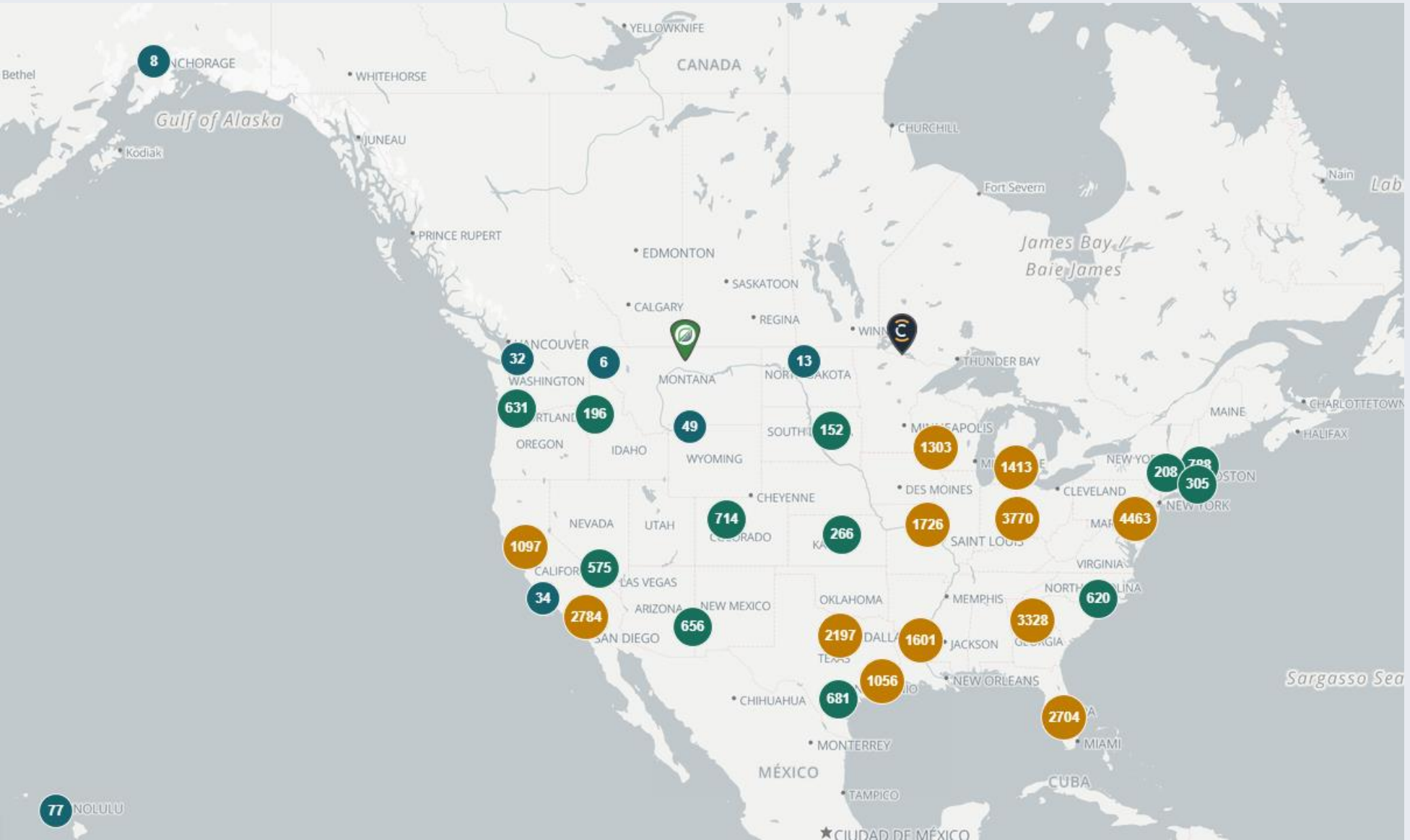
Sitios web de juegos

ATMs

Prácticas habituales de blanqueo de criptomonedas.

CRYPTO ATM´S ACTIVOS EN ESTADOS UNIDOS

J&A Global Compliance

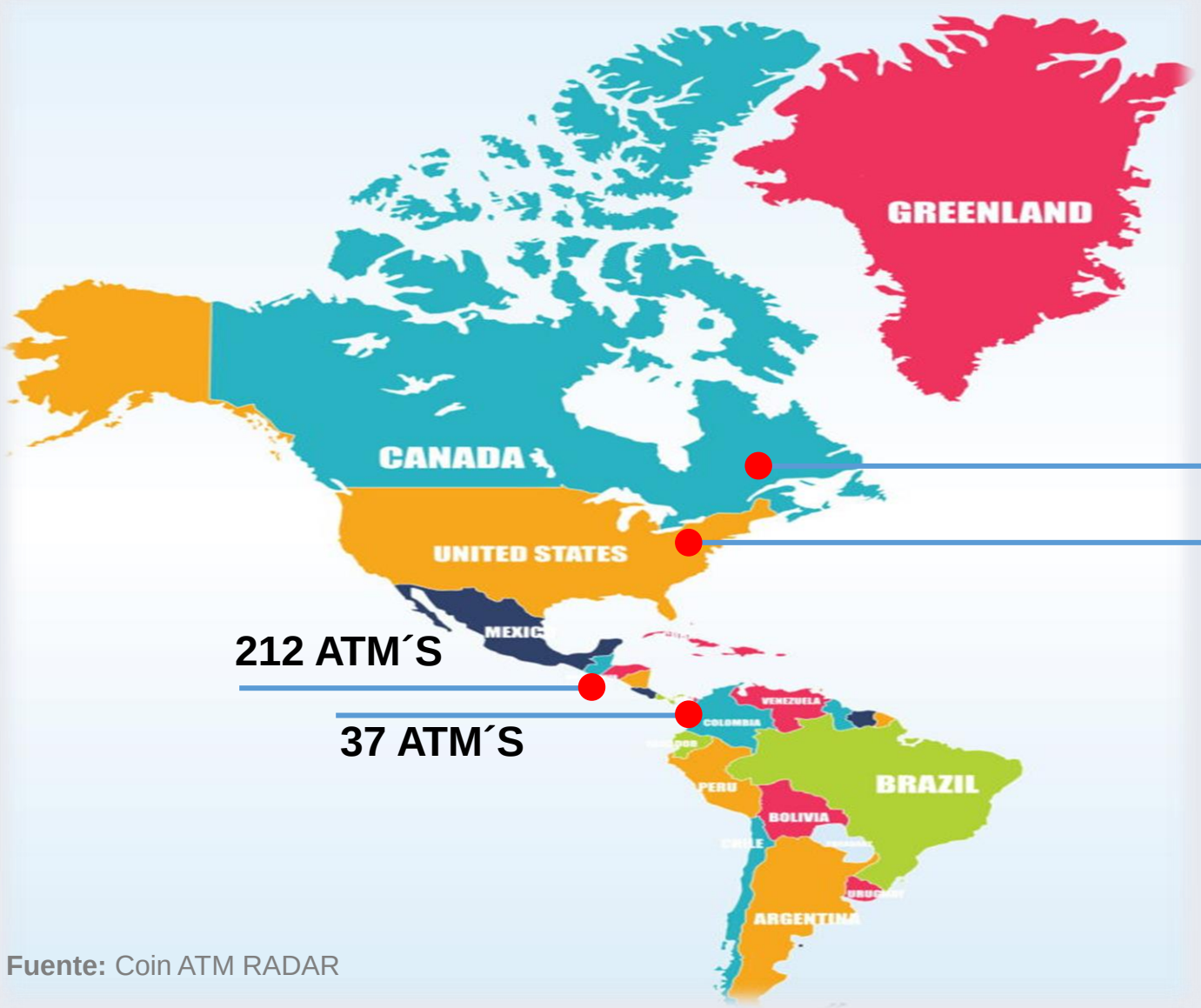


AL MENOS 33,462 CAJEROS AUTOMÁTICOS DE CRIPTOMONEDAS ACTIVOS EN EL 2023.

Fuente: Coin ATM RADAR

CRYPTO ATM´S ACTIVOS EN EL CONTINENTE AMERICANO

J&A Global Compliance



ATM CRYPO EN AMERICA	
PAIS	**Cantidad de ATM´S**
USA	33462
CANADA	2661
EL SALVADOR	212
COLOMBIA	37
PANAMA	30
PUERTO RICO	28
BRAZIL	25
REPUBLICA DOMINICANA	16
ARGENTINA	13
PERU	7
GUATEMALA	7
COSTA RICA	7
CHILE	3
PARAGUAY	3
MEXICO	1
URUGUAY	1
VENEZUELA	1
SAN MARTIN	1
BARBADOS	1
ECUADOR	1
HONDURAS	1
SAN CRISTOBAL Y NIEVES	1

Fuente: Coin ATM RADAR

¿CÓMO FUNCIONAN LOS ATM´S DE CRIPTOMONEDAS?

J&A Global Compliance

Es un ATM que se diferencia de los ATM convencionales, ya que este conecta a los usuarios a un exchange de criptomonedas, que les permite realizar una orden de compra o venta”

Paso 4: Una vez realizada la operación, el cajero automático te va a pedir que confirmes la transacción.
Debes confirmar todos los detalles de la compra y pulsar el botón de enviar.
Una vez confirmado, el cajero te dará la cantidad correspondiente de la criptomoneda a tu billetera.

Paso 1: Se debe configurar una cuenta con el operador del cajero automático. Por lo general, el ATM te va a solicitar crear una cuenta con el operador.

Paso 3: Una vez que ya esté introducida la información de tu billetera, puedes insertar todo el dinero efectivo que te gustaría convertir en criptomonedas

Paso 2: Introduce la información requerida del Wallet (Billetera). Por lo general esto, se realiza escanenado con el ATM el código QR de la Wallet.

PRINCIPALES PROVEEDORES DE TARJETAS Y SU RELACIÓN CON LOS EXCHANGES CRYPTO MÁS RELEVANTES

J&A Global Compliance

MASTERCARD: Programa Crypto Tarjetas.

BINANCE

Crypto Tarjeta de Débito y Tarjeta prepagada

nexo

Tarjeta de Crédito Crypto

tap

Tarjeta Prepagada

GEMINI

Tarjeta de Crédito

VISA: Programa Crypto Tarjetas.

Tarjeta Prepagada

eToro

Tarjeta Prepagada

coinbase

Tarjeta de Débito

xapo

Tarjeta Prepasgada

CÓDIGOS MCC ASOCIADOS A LAS TRANSACCIONES DE CRIPTOMONEDAS CON LOS PRODUCTOS DE TARJETAS

J&A Global Compliance

MCC

- **MCC 6012**

  "FINANCIAL INSTITUTIONS - MERCHANDISE & SERVICES"

- **MCC 6051**

  "QUASI CASH"

Se señala que estos códigos deben ser utilizado cuando se realizan compras de criptomonedas con los productos de tarjetas

ALGUNAS SEÑALES DE ALERTA ASOCIADAS A LOS ATM´S CRYPTO

J&A Global Compliance

- Depósitos de billetes de gran denominación, utilizados para realizar depósitos fiat en cajeros automáticos Crypto por los mismos usuarios, posiblemente reutilizando sólo un pequeño número de monederos de criptoactivos.
- Los cajeros automáticos de criptomonedas utilizados por los delincuentes están situados en regiones o barrios asociados con altas concentraciones de actividad delictiva y de bandas.
- Los fondos se envían a cajeros automáticos de criptoactivos o se recogen en ellos en jurisdicciones con poca o ninguna regulación en materia de criptoactivos, y, o con proveedores de cajeros automáticos de criptoactivos que no exigen información KYC/CDD
- Los cajeros automáticos de criptodivisas se encuentran en direcciones físicas asociadas a lo que parecen ser empresas de fachada, y que a su vez pueden ser propiedad de delincuentes cómplices de la actividad ilegal.
- En algunos casos, una única empresa fachada puede operar numerosos cajeros automáticos de crypto, todos ellos con niveles de facturación inverosímilmente altos
- Un solo ATM utilizado para procesar múltiples operaciones al mes en zonas o regiones que no tienen una adopción excepcionalmente alta de criptoactivos.

SEÑALES DE ALERTA ASOCIADAS A LOS PRODUCTOS DE TARJETA VINCULADAS A CRIPTOMONEDAS

J&A Global Compliance

- Mover fondos directamente desde una fuente ilícita a un proveedor de tarjetas prepago de criptoactivos para utilizarlos en una rápida conversión a fiat, o para comprar bienes y servicios físicos.
- Utilizar grandes transferencias entrantes desde cuentas bancarias para recargar rápidamente los saldos en la tarjeta prepago de criptoactivos y gastar en artículos de alto valor en comercios asociados con artículos de lujo, entre otros.
- Las tarjetas pueden presentar rachas repentinas de gran volumen y gasto de alto valor en un único comercio sin un propósito obvio.
- "Mulas" que sean utilizados para abrir numerosas cuentas y obtener tarjetas de prepago utilizando identificaciones auténticas o falsas, direcciones comunes, dispositivos móviles o direcciones IP.
- Delincuentes que pueden abrir cuentas en proveedores de tarjetas de prepago que no están regulados o no cumplen las normas, o con medidas débiles KYC/EDD
- Los fondos fiat transferidos a proveedores de tarjetas prepago de criptoactivos proceden de cuentas bancarias en países de alto riesgo.
- Los delincuentes abren numerosas cuentas en un único proveedor de tarjetas prepagadas e intentan utilizar múltiples tarjetas por debajo de los límites de transacción autorizados para evitar ser detectados en cada cuenta.
- Grandes volúmenes de transferencias bancarias entrantes de fiat pueden estar asociadas a fraudes de ingeniería social que utilizan plataformas de redes sociales para obtener fondos de las víctimas y luego convertirlos en criptomonedas para su posterior proceso de lavado de dinero

¿CÓMO UTILIZAN LOS DELINCUENTES UBER Y AIRBNB PARA LAVAR DINERO ROBADO CON TU TARJETA DE CRÉDITO?

J&A Global Compliance

Según los expertos, los ciberdelincuentes están recurriendo a nuevas tecnologías para lavar sus ganancias ilícitas, como el reclutamiento de falsos conductores de Uber, anfitriones sospechosos de Airbnb y especialistas en conversión de criptomonedas a través de la Dark Web

Los titulares de delitos cibernéticos tienden a centrarse en nuevas variantes de malware o negligencia grave que resultan en grandes filtraciones de datos. Es un juego proverbial del gato y el ratón, con sombreros blancos que fortalecen las defensas y sombreros negros que se ajustan para pasar por alto", dijo. "Sin embargo, lo que falta en estas historias e igual de importante para comprender cómo operan los ciberdelincuentes es lo que ocurre después de la filtración o cuando los fondos se adquieren ilegalmente".

Los delincuentes utilizan un esquema similar con los anfitriones de Airbnb, explicó Mador. Los anfitriones responden a anuncios, generalmente publicados en la dark web. Pero en lugar de alojar a un huésped real, con todo el trabajo y las molestias que ello puede implicar, aceptan el pago de un huésped falso que nunca tiene intención de presentarse. Una vez procesado el dinero a través del sistema de Airbnb, el anfitrión reembolsa una parte de la factura al ciberdelincuente.

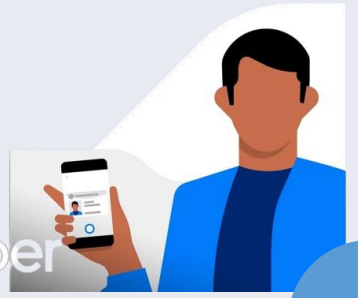
01

02

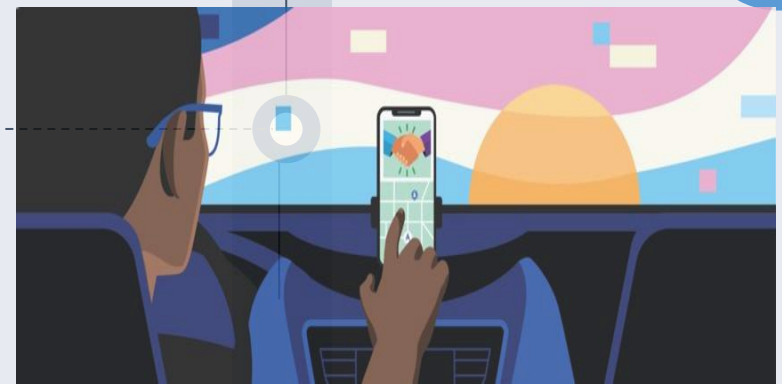
03

04

05



airbnb



Ziv Mador, que dirige el equipo de investigación SpiderLabs de la empresa de ciberseguridad Trustwave, afirma que el lavado de dinero es esencial para que prolifere la ciberdelincuencia. De hecho, si alguna vez le han robado dinero en una estafa cibernética o de una tarjeta de crédito o débito pirateada, puede que esta sea la última etapa del delito.

En una estafa habitual, los delincuentes reclutan a conductores de Uber para que simulen llevarlos a dar una vuelta. El delincuente nunca aparece, pero utiliza dinero ilícito de una tarjeta de crédito robada para pagar el viaje. A continuación, el conductor transfiere una parte del pago del viaje al delincuente. Esto es común verse en la dark web, una red de sitios web fuera de la Internet establecida a la que sólo se puede acceder a través de aplicaciones especiales, dijo Mador

NOTICIA RELEVANTE:

J&A Global Compliance

OFAC Multa a Tango Card, Inc. Por 116.048,60 Dólares en Relación con Aparentes Infracciones de Múltiples Programas de Sanciones.

Tango Card, Inc. (Tango Card), una empresa con sede en Seattle, Washington, que suministra y distribuye recompensas electrónicas, ha acordado pagar 116.048,60 dólares para saldar su posible responsabilidad civil por aparentes violaciones de múltiples programas de sanciones de Estados Unidos.

Como resultado de procesos deficientes de identificación de geolocalización, Tango Card transmitió al menos 27.720 productos de valor almacenado a personas con direcciones de protocolo de Internet (IP) y de correo electrónico asociadas a Cuba, Irán, Siria, Corea del Norte y la Región Ucraniana de Crimea. El importe del acuerdo refleja la determinación de la Oficina de Activos Extranjeros del Departamento del Tesoro de los Estados Unidos (OFAC) de que las aparentes infracciones de Tango Card no eran graves y se habían realizado una declaración voluntaria y refleja además la cooperación de Tango Card con la OFAC y las medidas correctivas aplicadas tras el acuerdo.

En febrero de 2021, uno de los clientes de Tango Card descubrió que varias direcciones de correo electrónico de destinatarios de recompensas que había proporcionado previamente a Tango Card (y a las que Tango Card había enviado recompensas) tenían dominios de primer nivel (TLD) asociados a jurisdicciones sancionadas. Posteriormente, Tango Card revisó su base de datos en busca de casos similares relacionados con direcciones de correo electrónico facilitadas anteriormente por otros clientes. Tango Card también identificó casos en los que un beneficiario canjeó una recompensa emitida por Tango Card desde una dirección IP ubicada en una jurisdicción sancionada.

En total, entre septiembre de 2016 y septiembre de 2021, Tango Card transmitió 27.720 tarjetas regalo comerciales y tarjetas de débito promocionales, por un total de 386.828,65 dólares, a personas con direcciones de correo electrónico o IP asociadas a Cuba, Irán, Siria, Corea del Norte o la Región Ucraniana de Crimea.

NOTICIA RELEVANTE:

J&A Global Compliance

Mastercard prohíbe las transacciones de cannabis con sus tarjetas de débito aún en lugares donde es legal. **27 de julio 2023**

La empresa dio instrucciones a los procesadores de pagos y a los bancos para que no acepten transacciones del sector en sus tarjetas de débito. Mastercard ha solicitado a las instituciones financieras que dejen de aceptar transacciones de marihuana a través de tarjetas de débito con PIN de la empresa.

Esto llega en un momento en que la industria del cannabis se ha vuelto legal en casi la mitad de los estados de EE.UU., pero aún carece de regulación federal. Mastercard ha dado instrucciones a los procesadores de pagos y a los bancos para que no acepten transacciones del sector en sus tarjetas de débito.

“De acuerdo con nuestras políticas, instruimos a las instituciones financieras que ofrecen servicios de pago a los comerciantes de cannabis y los conectan a Mastercard para que terminen la actividad”, dijo un portavoz de Mastercard, según informó Bloomberg, que cubrió la noticia por primera vez.

El movimiento de Mastercard llega después de que Visa enviara un memorando a los bancos en 2021, aclarando su postura sobre los cajeros automáticos sin efectivo utilizados por las empresas de marihuana y afirmando que violan las reglas de la compañía. Debido a la política de Visa contra la marihuana, el método de cajero automático sin efectivo está prohibido.

Aunque la marihuana para uso de adultos se ha legalizado en más de 23 estados de EE.UU., sigue siendo ilegal a nivel federal, lo que crea implicaciones desafiantes tanto para los consumidores de marihuana como para las empresas legales estatales que son difíciles de superar. Si bien los bancos regionales más pequeños aún pueden prestar servicios a las empresas de marihuana, las principales instituciones y redes de tarjetas de crédito como Visa y Mastercard evitan facilitar las transacciones de marihuana en sus redes debido a la ilegalidad federal.

Fuente:https://es-us.finanzas.yahoo.com/noticias/mastercard-proh%C3%ADbe-transacciones-cannabis-tarjetas-165700254.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMLs0ROjlyrQElLN507WWFbjr8HMKGZ_rzVRSW9fdf6R_qAKCsUl8h4GhL61ylo2Fd5UcTSVi6bZob73xp

NOTICIA RELEVANTE:

J&A Global Compliance

Mastercard prohíbe las compras de cannabis con sus tarjetas de débito y crédito.

27 de julio 2023

Mastercard ha emitido cartas de cese y desistimiento a los procesadores de pagos, poniendo fin a la posibilidad de usar sus tarjetas para comprar marihuana.

Aunque la marihuana recreativa es legal en muchos estados, su estatus ilegal a nivel federal lleva a que las transacciones de cannabis aún se mantengan al margen de la economía.

RAZONES

Aunque los dispensarios de marihuana operan legalmente en algunos estados, muchos bancos no están dispuestos a trabajar con ellos, lo que dificulta su acceso a servicios financieros básicos. Ahora, Mastercard ha dejado en claro que no aprueba que sus productos estén vinculados con compras de marihuana.

Visa también ha emitido un edicto

Mastercard no es la única compañía que toma esta medida, ya que Visa también ha emitido un edicto similar para bloquear transacciones en dispensarios y distribuidores legales de marihuana.

Esta postura de las compañías de tarjetas de crédito representa un obstáculo adicional para los distribuidores de marihuana, quienes ya han tenido dificultades para encontrar métodos de pago alternativos al efectivo.

En el pasado, algunos dispensarios utilizaron cajeros automáticos sin efectivo para sortear las restricciones financieras, haciendo que las transacciones parecieran simplemente retiros de cuentas en lugar de compras de productos.

Sin embargo, tras la intervención de los reguladores, esta opción ya no es viable, lo que llevó a más personas a optar por el débito con PIN al comprar marihuana legalmente.

Fuente: https://mundoejecutivo.com.mx/economia-finanzas/mastercard-prohibe-las-compras-de-cannabis-con-sus-tarjetas-de-debito-y-credito/

LAS CRIPTO MONEDAS Y LAS TARJETAS DE CRÉDITO

J&A Global Compliance

Las criptomonedas están llegando a las tarjetas de crédito. **21 de julio 2022**

Los clientes ahora pueden realizar pagos con criptomonedas vinculadas a tarjetas Visa y Mastercard, que son proporcionadas principalmente por empresas fintech. Sin embargo, todavía se trata de un nicho de mercado y las transacciones dependen generalmente de que terceros conviertan esas criptomonedas en dinero local.

Visa y Mastercard, las redes de tarjetas más grandes de Estados Unidos, dicen que están trabajando para realizar los pagos en criptomonedas por su cuenta. Estos esfuerzos, si tienen éxito, marcarían un punto de inflexión importante. Sería la primera vez que estas redes permitirían liquidar pagos en activos diferentes a los considerados como monedas principales.

Un impulso hacia las criptomonedas

En los últimos cinco años, las criptomonedas han pasado de ser un activo –en gran medida– reservado a inversionistas adinerados y millennials, a uno que podría convertirse en el rival de los pagos cotidianos. A las redes de tarjetas de crédito más grandes de EE UU les preocupa quedar excluidos si no habilitan los pagos con criptomonedas, un método que se encuentra en constante crecimiento y que posiblemente, algún día, domine la escena, según personas familiarizadas con el asunto.

También creen que los consumidores van a querer usar ese método de pago. “Realmente no vemos demanda para eso en la actualidad, pero puede llegar, y esa es también una razón por la que estamos invirtiendo”, dijo el año pasado Jorn Lambert, director digital de Mastercard.

Otras grandes empresas de pagos están ampliando sus capacidades cripto. Desde el año pasado PayPal Holdings Inc. comenzó a permitir que los usuarios estadounidenses paguen con criptomonedas. En lugar de pagarles a los comerciantes con una tarjeta que recargaron en PayPal, los consumidores pueden elegir criptomonedas que almacenan en cuentas de esa plataforma. Las criptos se convierten en moneda local gracias a una asociación con Paxos, una plataforma con infraestructura blockchain, y luego PayPal envía el pago al comerciante. En junio, PayPal informó que les permitirá a sus clientes (que tienen criptomonedas en la plataforma) pagarles con ellas a otros usuarios de PayPal.

Fuente: https://eldiario.com/2022/07/21/las-criptomonedas-estan-llegando-a-las-tarjetas-de-credito/

LAS CRIPTO MONEDAS Y LAS TARJETAS DE CRÉDITO

J&A Global Compliance

Cómo comprar criptomonedas con tarjeta de crédito. **23 de noviembre 2022**

1. Elija una plataforma. Hay muchas plataformas digitales que ofrecen el servicio de compra de criptomonedas con tarjeta. Estas plataformas reciben el nombre de casas de cambio digitales o exchanges.
2. Cree una cuenta. Este es un procedimiento fácil donde le van a pedir datos básicos de identidad como nombre completo, número de cédula o pasaporte, dirección y teléfono celular.
3. Verifique su cuenta. Este proceso es obligatorio para comprar y vender criptomonedas en cualquier casa de cambio digital. Es muy fácil: Luego de crear una cuenta, debe verificar que todos sus datos sean correctos. Cada plataforma le irá indicando paso a paso qué debe hacer. Básicamente, consiste en adjuntar la foto de un documento como el pasaporte.
4. Introduzca su método de pago. En general, las tarjetas, así como la cuenta bancaria, deben estar a su nombre. Seleccione la opción de pagar con tarjeta de crédito y complete los campos requeridos con la información de la tarjeta. Le pedirán: nombre del titular, número de tarjeta, fecha de vencimiento, código de seguridad.
5. Ingrese los detalles de compra. A continuación, ya puede comprar criptomonedas en la plataforma.
6. Pros: Es un método de pago rápido y fácil de usar. La mayoría de los exchanges permiten pagar con tarjeta. Es una forma rápida de comprar Bitcoin y otras criptomonedas. Es ideal para personas que recién se inician en el mundo cripto.
7. Contras: Es una opción cara debido a sus altas comisiones. La compra de criptomonedas puede verse restringida por los montos máximos de su tarjeta de crédito. Las compras con tarjeta de crédito suelen estar habilitadas sólo para las criptomonedas más populares. Facilita su identidad, por lo cual no es una buena opción si desea conservar un mayor grado de privacidad.

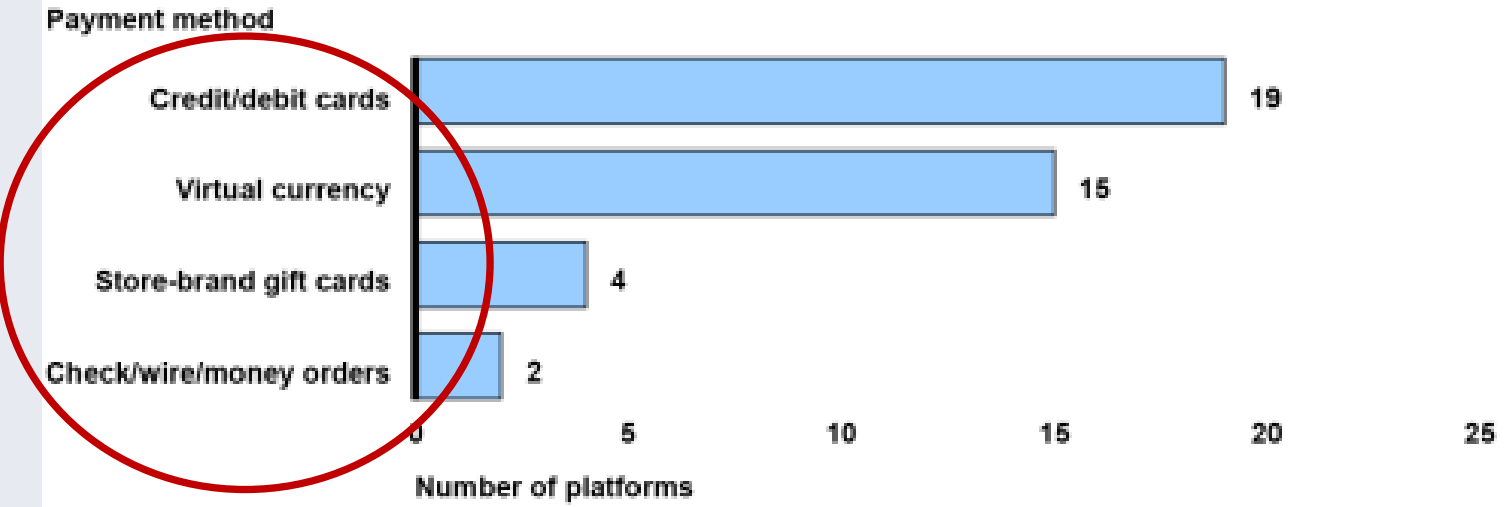
Fuente: https://saberespoder.com/articles/finance/como-comprar-criptomonedas-con-tarjeta-de-credito

MEDIOS DE PAGO EN EL TRÁFICO SEXUAL EN LÍNEA.

J&A Global Compliance

Se ilustra el uso de tarjetas de crédito como uno de los medios de pago utilizados en el tráfico sexual en línea.

Figure 4: Payment Methods Accepted by 27 Platforms in the Online Commercial Sex Market, as of November 2020



Source: GAO analysis. | GAO-21-385

Accessible Data for Figure 4: Payment Methods Accepted by 27 Platforms in the Online Commercial Sex Market, as of November 2020

Payment method	Number of platforms
Credit/debit cards	19
Virtual currency	15

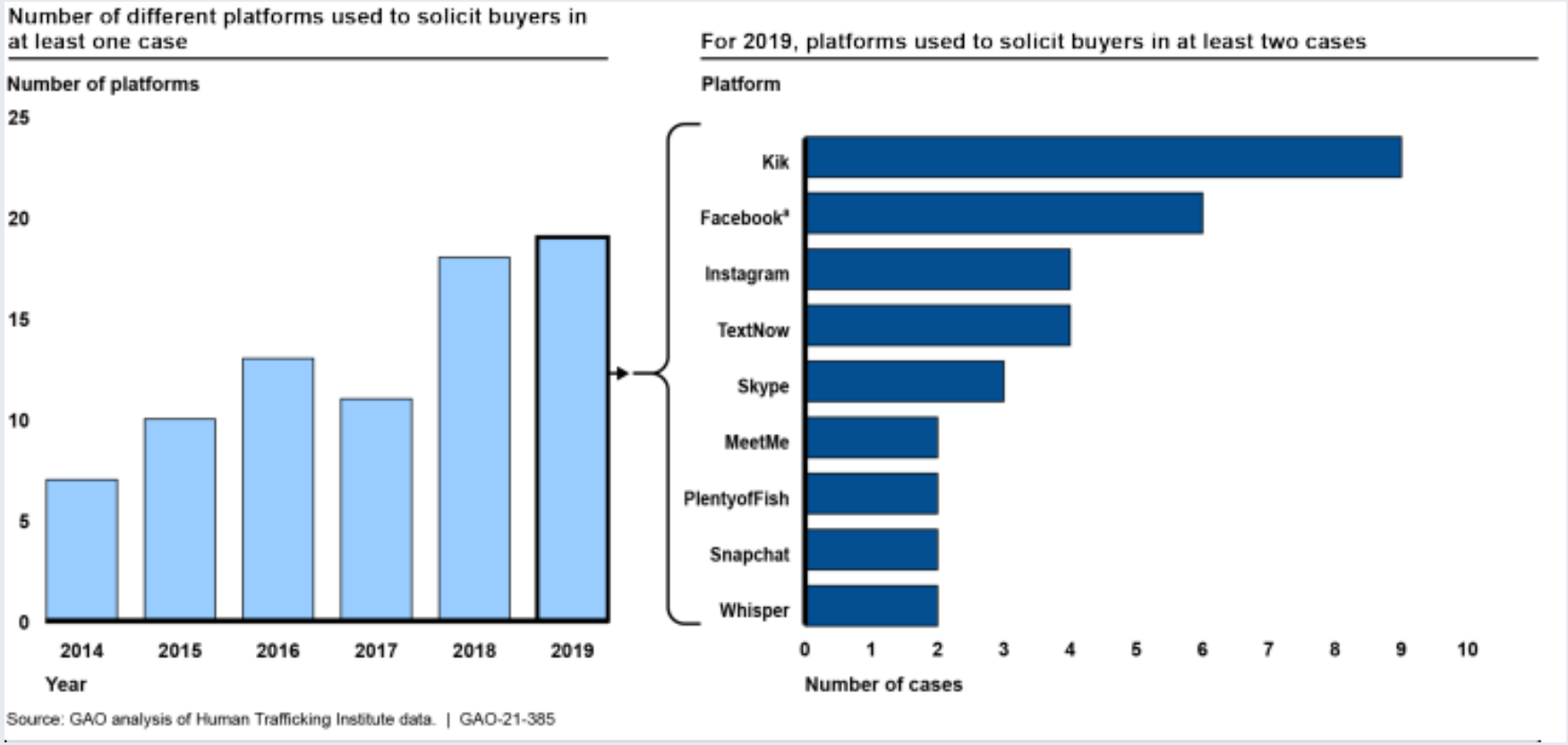
Si una cuenta de comerciante mantiene una tasa de contracargo demasiado alta durante demasiado tiempo, a menudo el banco emisor la cerrará. Por lo tanto, para evitar una interrupción de los pagos, un operador exitoso tendrá múltiples cuentas comerciales para procesar y ajustará su flujo de transacciones entre ellas para evitar que una cuenta acumule demasiado fraude.

1. Una de las razones por las que las plataformas podrían aceptar métodos de pago más allá de las tarjetas de crédito y débito puede ser la dificultad que tienen para mantener sistemas de pago confiables con tarjetas de crédito y débito, según los informes de Polaris de julio de 2020 y childsafe.ai de abril de 2019. El informe de childsafe.ai de abril de 2019 afirma que gran parte de las operaciones de backpage.com se centraron en la "gimnasia financiera" necesaria para aceptar tarjetas de crédito con fines publicitarios. Específicamente, el informe establece que solicitar constantemente nuevas cuentas comerciales, cambiar los descriptores de facturación y equilibrar la carga de los pagos entre cuentas para mantener las tasas de fraude/devolución de cargo dentro de límites aceptables requiere experiencia y tiempo significativos

COMPLEJIDAD DE LOS SISTEMAS DE PAGO EN PLATAFORMAS DE TRÁFICO SEXUAL.

J&A Global Compliance

Uso de las redes sociales, las citas, el enganche y las plataformas de mensajería/comunicación para captar compradores en los nuevos casos federales de tráfico sexual criminal (2014 a 2019)



1. La información del FBI también indica que el aumento del uso de estas plataformas dificulta la capacidad de las fuerzas del orden para recabar pistas y pruebas relacionadas con el tráfico sexual, es difícil porque: las plataformas emplean distintos niveles de encriptación de los mensajes compartidos entre los usuarios; permiten a los usuarios el pseudoanonimato mediante el uso de identidades falsas; y algunas plataformas borran automáticamente el contenido poco después de que los destinatarios lo vean.

CASO REAL:

Carbanak y el Sindicato Cibercriminal COBALT

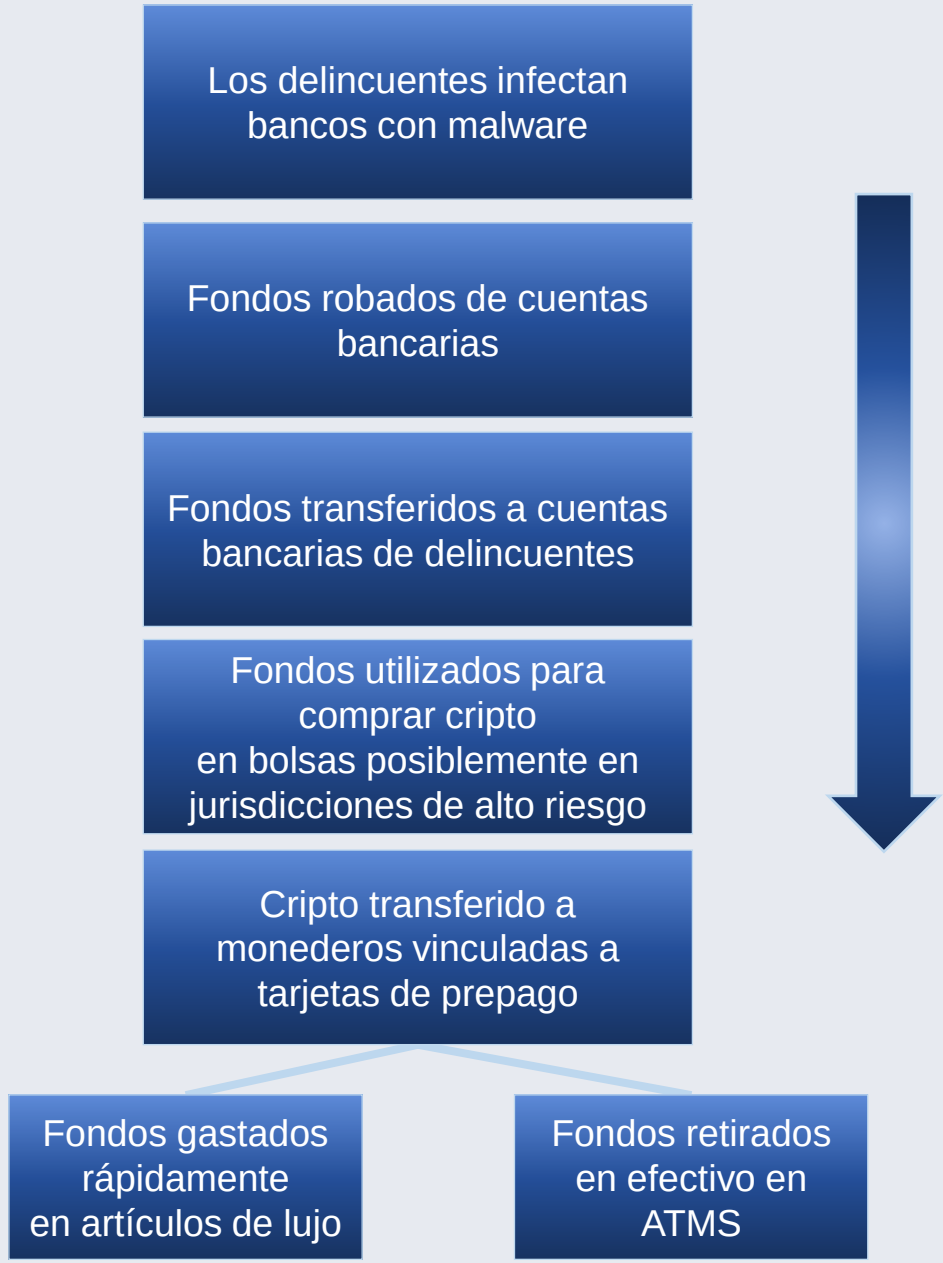
J&A Global Compliance

En marzo de 2018, Europol detuvo al jefe del grupo de ciberdelincuentes que desarrolló las cepas de malware Carbanak y las cepas de malware Cobalt utilizadas para atacar a decenas de bancos mundiales.

Este grupo criminal lavó hasta 1.000 millones de dólares y dependía en gran medida de los criptoactivos. Las cepas de malware que desplegaron les permitieron comprometer cuentas bancarias y transferir fondos a sus propias cuentas bancarias en el extranjero. El malware también permitía a los ladrones comprometer los cajeros automáticos de los bancos y vaciarlos de efectivo.

La red criminal movía estos fondos robados a través de numerosas cuentas bancarias utilizando mulas de dinero en países como Taiwán, España y Bielorrusia .

Finalmente, convertían los fondos en criptoactivos a través de bolsas y proveedores de servicios de monedero que ofrecían servicios de tarjetas de prepago. Según Europol, las tarjetas de prepago se utilizaban para comprar artículos de lujo, como casas y coches.

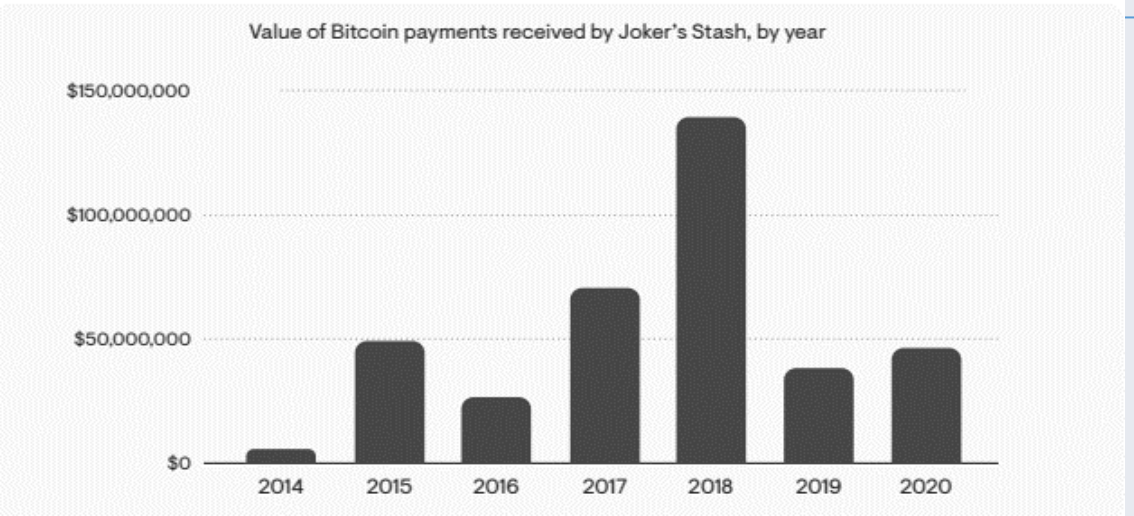


CASO REAL:

Joker's Stash: Se Retira el Mayor Mercado de Tarjetas

J&A Global Compliance

- Durante varios años, el sitio web más popular para que los delincuentes compraran datos robados de tarjetas de crédito y débito utilizando criptoactivos era Joker's Stash.
- Creado en 2014, Joker's Stash era un emporio masivo en línea, donde los delincuentes podían comprar datos de tarjetas robadas por entre 1 y 150 dólares por tarjeta utilizando Bitcoin.
- Aunque estas cantidades pueden parecer pequeñas, el comercio total de tarjetas robadas que tuvo lugar en Joker's Stash era asombroso: La investigación de Elliptic indica que recibió más de 400 millones de dólares en pagos de Bitcoin entre 2014 y 2020, como se indica en el siguiente gráfico.
- En febrero de 2021, los operadores de Joker's Stash anunciaron su retirada y cerraron el sitio. Su negocio ilícito les reportó enormes beneficios; el Bitcoin que adquirieron habría tenido un valor de aproximadamente 2.500 millones de dólares a principios de 2021.



CASO REAL:

Uso de Tarjetas FIAT para Comprar Criptoactivos con Fines Ilícitos

J&A Global Compliance

- Las agencias de ley de los Estados Unidos detectaron casos de traficantes de seres humanos y partidarios del terrorismo que utilizaban tarjetas fiat para comprar criptomonedas y utilizarlas en sus delitos.
- Según FinCEN, durante un caso en 2018, las agencias de ley estadounidenses arrestaron en Texas a William Harris y Dean Hall, que estaban involucrados en la trata de mujeres para la prostitución. Al recuperar las armas de fuego las agencias de ley se enteraron de que Harris había comprado tarjetas de crédito prepagadas Vanilla Visa.
- El utilizó estas tarjetas para comprar Bitcoin en un popular sitio web P2P, y luego utilizó el Bitcoin para comprar anuncios en el sitio de prostitución Backpage.com.
- En otro caso estadounidense, una mujer de Nueva York fue condenada a 13 años de prisión por su participación en una campaña de financiación de la organización terrorista ISIS.
- Según el Departamento de Justicia, Zoobia Shanaz obtuvo fraudulentamente un préstamo de 22.500 dólares.
- También utilizó más de una docena de tarjetas de débito y crédito obtenidas fraudulentamente para comprar criptomonedas por un total de 62.500 dólares. Shanaz transfirió finalmente fondos a entidades de fachada del ISIS en Pakistán, China y Turquía

EJEMPLO

Actividad Sospechosa

J&A Global Compliance

Cliente X lavador de dinero, quien posee cuenta banco XYZ

Producto

Al tener fondos depositados en su cuenta de procedencia irregular, decide prepagar este producto

Reembolso

Los fondos reembolsados los usa para adquirir productos o pagar servicios ocultando el origen primario.

Cliente

También posee tarjeta de crédito asignada a su nombre.

Uso de fondos

Luego solicita al banco, el reembolso del monto prepagado

Compras

EJEMPLO

Actividad Sospechosa

J&A Global Compliance

Posteriormente coloca este dinero en los bancos offshore para continuar haciendo uso de sus TDC/TDD.

Posterior, accede a estos fondos a través de Tarjetas de Crédito / Débito.

Coloca fondos ilícitos en cuentas en bancos extraterritoriales.

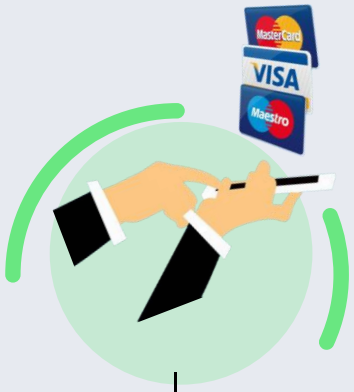
Realiza contrabando de efectivo de un país a otro con controles laxos

Cliente X lavador de dinero, quien posee cuenta banco XYZ

EJEMPLO

Actividad Sospechosa

J&A Global Compliance



01

Se adquiere una tarjeta de una institución financiera internacional

La persona viaja a la línea fronteriza y se dirige a una gasolinera a realizar avances de efectivo por ATM

02

03

Ese dinero es luego utilizado para facilitar operaciones fraudulentas o delictivas.

EJEMPLO:

J&A Global Compliance

En este escenario, los delincuentes utilizan las redes sociales para recopilar información sobre las personas, como nombres, fechas de nacimiento. Una vez que los delincuentes recopilan suficiente información, pueden utilizarla para realizar estafas o actividades de carding. Por ejemplo, pueden realizar compras en línea utilizando los datos de la tarjeta de crédito de la víctima sin su conocimiento o consentimiento.

PROGRAMA DE MONITOREO: FRAUDE

A través del monitoreo de transacciones relacionadas a TDD o TDC, mayormente, se analizan tipologías como las siguientes:

- Transacciones que excedan cierta cantidad diariamente.
- Transacciones con múltiples rechazos.
- Transacciones que exceden varios intentos en el mismo comercio en un período de tiempo determinado.

Robo de Tarjetas

Utilizan tarjetas perdidas y encontradas

"Account Takeover".

Tarjetas falsificadas – Interceptan tarjetas por correo.

Aplicaciones fraudulentas.

FRAUDE. CLONACIÓN DE TARJETAS

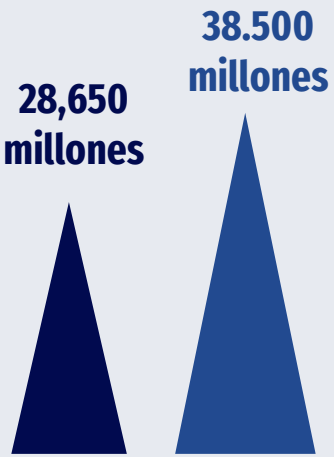
J&A Global Compliance

¿Qué es la clonación de tarjetas?

La clonación de tarjetas de crédito o skimming es el acto ilegal de hacer copias no autorizadas de tarjetas de crédito o débito.

Esto permite a los delincuentes utilizarlas para realizar pagos, robando efectivamente el dinero del titular de la tarjeta y/o endeudándolo, La clonación de tarjetas ha sido históricamente uno de los tipos de fraude relacionados con las tarjetas más comunes en todo el mundo,

La clonación de tarjetas ha sido históricamente uno de los tipos de fraude relacionados con las tarjetas más comunes en todo el mundo, por el que se pierden 28.650 millones de dólares al año en todo el mundo, cifra que se prevé que aumente a 38.500 millones de dólares en 2023, según Nilson Report,



¿Como evitar la clonación de tarjetas de crédito

Microchips EMV en lugar de bandas magnéticas

Estos contienen valores iCVV más avanzados que los de las bandas magnéticas, y no pueden ser copiados mediante skimmers.

Perfiles de clientes

Mediante la creación de perfiles de clientes, a menudo utilizando el machine learning y algoritmos avanzados, los gestores de pagos y los emisores de tarjetas adquieren una valiosa información sobre lo que se consideraría un comportamiento «normal» para cada titular de la tarjeta, señalando cualquier movimiento sospechoso para realizar un seguimiento con el cliente

Educar al público

Convertir al público en general en un aliado en la lucha contra el fraude de las tarjetas de crédito y débito puede redundar en beneficio de todos

Responsabilidad, leyes y reglamentos

Debido a la normativa y la legislación gubernamentales, los proveedores de tarjetas tienen un gran interés en prevenir el fraude, ya que son ellos quienes deben pagar la factura del dinero perdido en la mayoría de las situaciones. La legislación actual varía según el país, pero en la mayoría de los lugares se puede recurrir a los servicios del defensor del pueblo para cualquier transacción controvertida

¿CÓMO SE HACE LA CLONACIÓN DE TARJETAS?

J&A Global Compliance

1. Se recluta a un cómplice, alguien con acceso físico a las tarjetas de crédito, por ejemplo, un cajero, un camarero de restaurante, etc.

2. Se le entrega un skimmer, una máquina compacta que se utiliza para capturar los datos de las tarjetas. Puede ser una máquina independiente o un complemento del lector de tarjetas

3. El cliente entrega su tarjeta al cómplice, como pago.
El cómplice pasa la tarjeta por el skimmer, además de la máquina de TPV utilizada para el pago normal.

4. El cómplice devuelve la tarjeta al cliente desprevenido

5. El ladrón transfiere los datos capturados por el skimmer a la banda magnética de una tarjeta falsificada, que podría ser una tarjeta robada

6. La tarjeta falsificada puede utilizarse ahora de la misma manera que una tarjeta legítima, o para cometer otros fraudes, como el uso de tarjetas de regalo y otras tarjetas

¿QUÉ ES EL CARDING?

J&A Global Compliance

DEFINICIÓN

Es un término general para referirse a la utilización de los datos de las tarjetas de crédito y débito robadas para beneficio personal, que puede consistir en la venta de los datos, en su utilización para comprar bienes o para alimentar otros fraudes

EJEMPLOS DE CARDING

- En la industria del iGaming: Estafas de juego y apuestas online dirigidas a los proveedores de iGaming.
- En el sector de la hostelería: Huéspedes de hoteles que intentan pagar con varias tarjetas.
- En el comercio y el mercado de divisas: Estafadores que compran criptomonedas con tarjetas robadas

¿Cómo funciona el robo de tarjetas?

- Clonación de tarjetas/skimming
- Robo por RFID / Phishing / Wi-Fi público / Software espía / Filtración de datos / Ataques BIN

Tras adquirir los datos, el ladrón suele recopilar largas listas y proceder a:

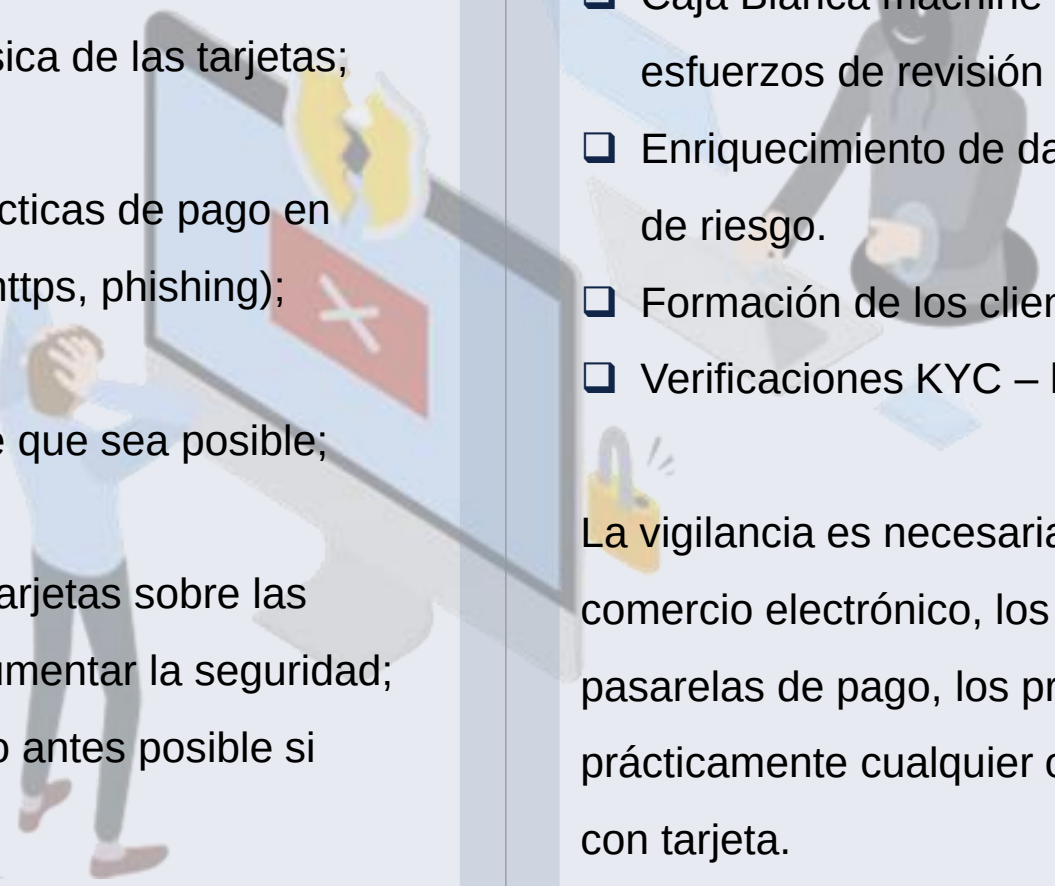
- Venderlos en la dark web o en plataformas cifradas como Telegram, para obtener beneficios.
- Utilizarlos para comprar artículos costosos para luego revenderlos.
- Utilizarlos para comprar criptomonedas para revenderlas, como inversión o como pago no rastreable para financiar más fraudes.
- Utilizarlos para comprar tarjetas de prepago o tarjetas de regalo para venderlas.
- Utilizarlos para financiar otras actividades nefastas, incluyendo otras estafas.

¿CÓMO EVITAR EL CARDING?

J&A Global Compliance

¿Cómo pueden los consumidores evitar el carding?

- Supervisar todos los extractos de la tarjeta y hacer un seguimiento de cualquier cargo sospechoso;
- Ser consciente de la ubicación física de las tarjetas;
- Informarse sobre las mejores prácticas de pago en línea y los riesgos (por ejemplo, https, phishing);
- Activar la MFA y/o la 2FA siempre que sea posible;
- Preguntar a los emisores de las tarjetas sobre las salvaguardias opcionales para aumentar la seguridad;
- Congelar o cancelar una tarjeta lo antes posible si surgen problemas.



¿Cómo pueden las empresas detectar el carding?

- Análisis de la huella digital para señalar las cuentas sospechosas.
- Caja Blanca machine learning para ayudar a los esfuerzos de revisión manual.
- Enriquecimiento de datos para informar de los modelos de riesgo.
- Formación de los clientes y del personal.
- Verificaciones KYC – ligeras o pesadas (o combinadas).

La vigilancia es necesaria por parte de las empresas de comercio electrónico, los bancos, los operadores de pasarelas de pago, los proveedores de servicios y prácticamente cualquier organización que gestione pagos con tarjeta.

FRAUDE. ¿QUÉ SON LAS PRUEBAS DE TARJETAS?

J&A Global Compliance

La prueba de tarjetas es cuando un estafador comprueba si una tarjeta de crédito robada sigue activa («viva») antes de pasar a utilizarla, así como si le quedan fondos.
La prueba consiste en llevar a cabo una actividad con la tarjeta con menos probabilidades de ser señalada como sospechosa, y a menudo se realiza con largas listas de credenciales de tarjetas adquiridas ilegalmente, para separar las que sirven de las que no.

MÉTODO: PAGOS PEQUEÑOS

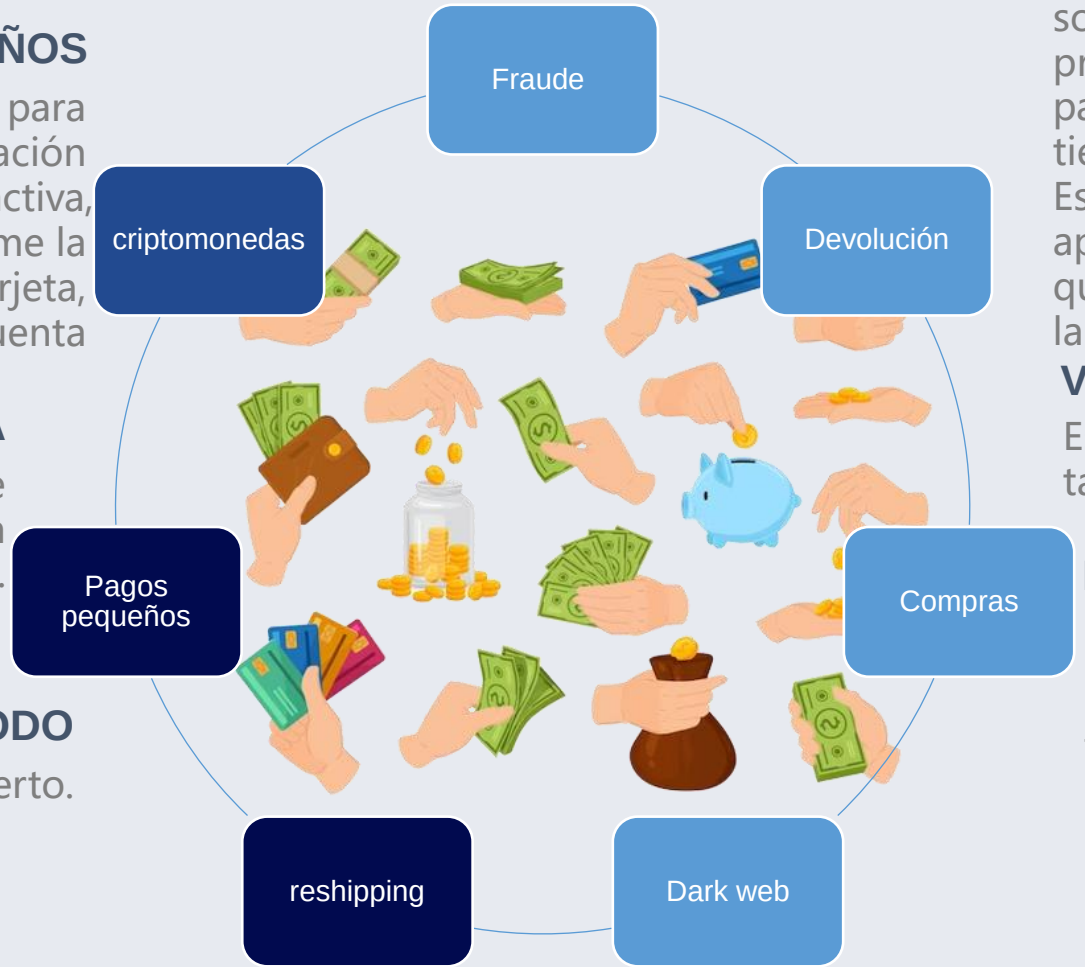
El estafador intenta utilizar una tarjeta para realizar un pequeño pago. La aceptación del pago le mostrará si la tarjeta está activa, pero también es probable que llame la atención del titular legítimo de la tarjeta, ya que aparecerá en su estado de cuenta

VENTAJA

Es fácil encontrar lugares donde utilizarlo; los rechazos pueden ayudar a los delincuentes.

RIESGO DEL MÉTODO

Mayor probabilidad de ser descubierto.



MÉTODO: AUTORIZACIONES

A diferencia de los pagos, las autorizaciones son una consulta enviada a través del procesador de pagos al emisor como primer paso de un pago, preguntando si el cliente tiene los fondos para cubrir la transacción. Estas autorizaciones tardan mucho más en aparecer en los extractos de las tarjetas, lo que da al estafador más tiempo para utilizar la tarjeta activa.

VENTAJA

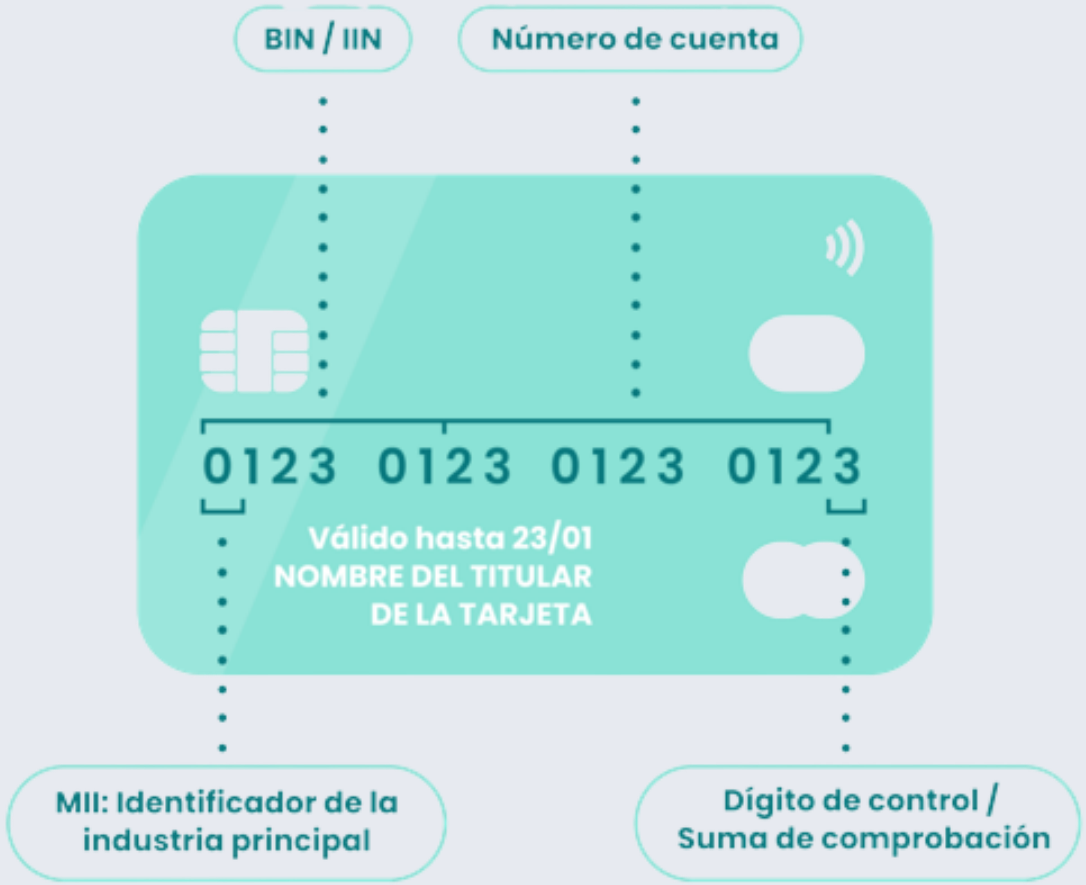
Es poco probable que el titular de la tarjeta se entere; método más sutil.

RIESGOS DEL MÉTODO

Los métodos antifraude avanzados seguirán detectándolos.
En este punto, el propietario legítimo de la tarjeta podría darse cuenta y ponerse en contacto con el emisor de ella. Esto es una mala noticia para el delincuente, pero también es desafortunado para el comerciante, que se enfrentará a solicitudes de contracargos.

CÓMO DETENER EL FRAUDE DE PRUEBAS DE TARJETAS

J&A Global Compliance



- ❑ Enrequecimiento de datos
- ❑ CI-DSS
- ❑ Análisis de huellas digitales
- ❑ Análisis de riesgos
- ❑ Protocolos SCA
- ❑ Reglas de velocidad
- ❑ Indicadores de riesgo

La idea general es recopilar toda la información posible sobre el cliente que intenta realizar un pago, manteniendo la fricción al mínimo, para no disuadir a los consumidores legítimos.

FRAUDE.

J&A Global Compliance

¿PARA QUÉ SE UTILIZAN LAS PRUEBAS DE TARJETAS?

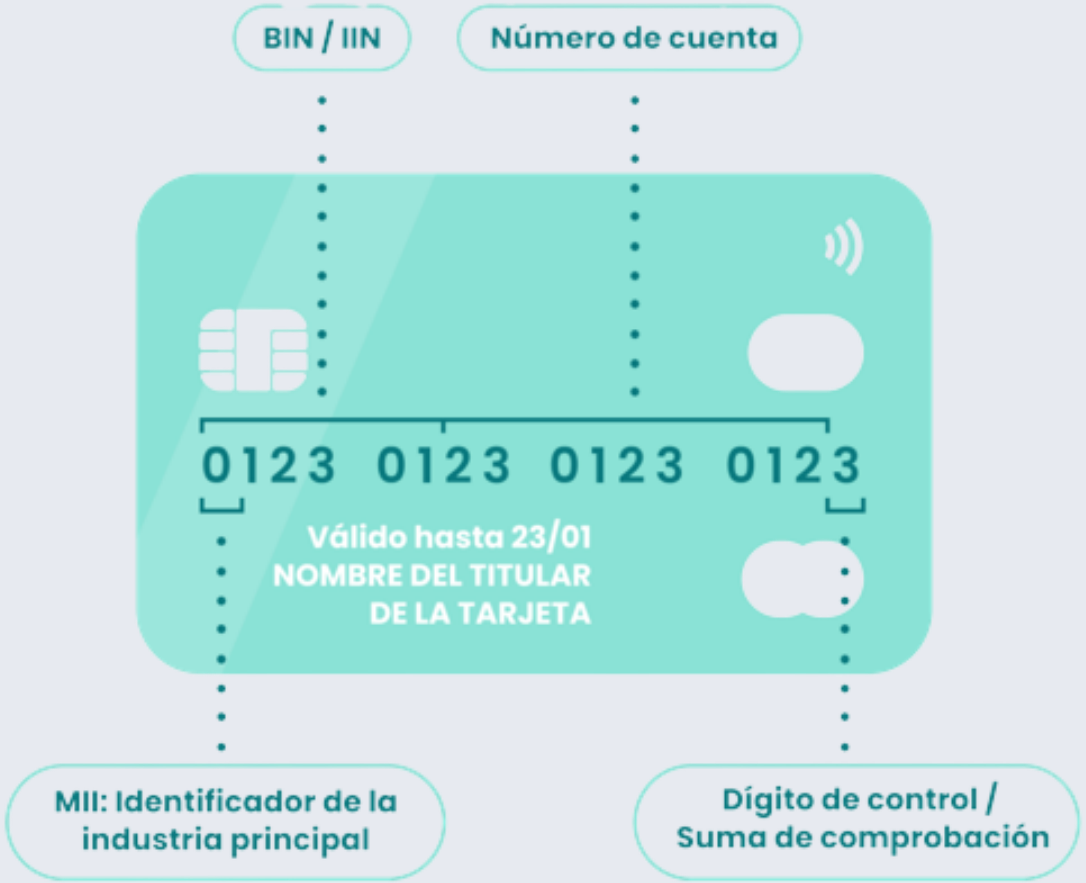
- Revenden las tarjetas activas para obtener un beneficio (las tarjetas verificadas se venden por más dinero que las no verificadas);
- Las utilizan para realizar fraudes, incluidos los de devolución de cargos
- Las utilizan para comprar tarjetas de regalo o criptomonedas;
- Las utilizan para comprar productos para el reshipping;
- Las utilizan para comprar servicios delictivos o ilegales en la dark web;
- Así como cualquier otro acto que implique pagos con tarjeta.

¿Cómo perjudica el fraude de pruebas de tarjetas al comercio electrónico?

- Pueden provocar solicitudes de devolución de cargos y, por lo tanto, puede afectar la tasa de devoluciones de cargos, lo que en última instancia puede llevar incluso a ser prohibido como comerciante
- El comerciante puede ser marcado como de alto riesgo, viéndose así obligado a pagar tasas más altas a los procesadores de pago.
- El éxito de las pruebas indica a los delincuentes que los protocolos antifraude son bajos, lo que abre la caja de Pandora de los posteriores ataques de fraude.
- Costes adicionales: tasas de disputa, tasas de intercambio, horas de trabajo empleadas, tasas de resolución.
- Caída de la moral de los empleados, así como daños a la reputación.

¿QUÉ SON LOS ATAQUES DE BINEROS?

J&A Global Compliance



- El BIN, o Número de Identificación del Banco (BIN), son los seis primeros dígitos en una tarjeta de crédito. Estos siempre están relacionados a su institución emisora, usualmente un banco. En un ataque de binero, los estafadores utilizan estos seis dígitos para intentar generar algorítmicamente los otros números legítimos, con la esperanza de generar un número de tarjeta de crédito utilizable.

- Luego las utilizan con varios comerciantes para filtrar esa lista y detallarla, esencialmente, con lo que funcione. Un tipo de ataque de fuerza bruta, que típicamente involucra un gran número de transacciones pequeñas, cómo un típico testeo de tarjeta.

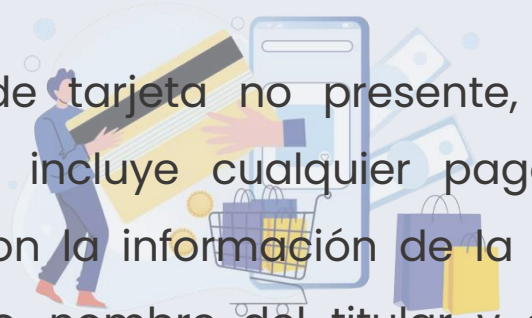
- Debido a que solamente se utilizan números de tarjetas de crédito, los ataques bineros constituyen un fraude de tarjeta no presente.

¿QUÉ ES EL FRAUDE CON TARJETA NO PRESENTE (CNP)?

J&A Global Compliance

Definición

El fraude CNP se describe como un pago fraudulento o una estafa sin el consentimiento del propietario correcto de la tarjeta.



Un escenario de tarjeta no presente, como su nombre indica, incluye cualquier pago que se procesa solo con la información de la tarjeta de crédito (número, nombre del titular y código de seguridad). La tarjeta física está en otro lugar. Así es como funcionan todos los pagos en línea, y también los pagos por teléfono.

¿Cómo funciona el fraude con tarjeta no presente?

- El fraude CNP tiene lugar siempre que un estafador adquiere algún tipo de información de pago, como el número de una tarjeta de crédito, el nombre de una persona, los detalles de su dirección o el número de seguridad de 3 dígitos que aparece en el reverso, para luego comprar productos.
- Hoy en día, los estafadores pueden adquirir fácilmente «fullz», es decir, perfiles completos robados que se descubren a través de filtraciones de datos o ataques de phishing y que pueden comprarse a través de la dark web.
- En la mayoría de los casos, la responsabilidad de las transacciones CNP fraudulentas recae en el comerciante, por lo que las devoluciones de cargos son habituales, ya que la víctima a menudo sólo reacciona una vez que descubre el fraude.

CONSEJOS PARA REDUCIR EL FRAUDE CON TARJETA NO PRESENTE

J&A Global Compliance

Cuanto más se sepa de un usuario, más fácil será rechazar pagos sospechosos que podrían ser claros casos de fraude con tarjeta no presente.

Recopilar información sin crear demasiada fricción para el usuario, lo que puede perjudicar las conversiones y las ventas.

Recopila toda la información de los clientes que puedas

El enriquecimiento de datos puede ser invisible para el titular de la tarjeta, lo que le ayuda a reducir el peligro sin crear demasiados obstáculos para los clientes adecuados

Enriquecer los datos a partir de fuentes que tengan sentido y de conjuntos de datos frescos y de código abierto.

Enriquecimiento de datos

Los datos encriptados y protegidos tienen menos probabilidades de caer en manos equivocadas, lo que reduce el fraude en su conjunto.

La gestión de las copias de seguridad y la configuración del software y el hardware de protección pueden ser costosas debido al rápido crecimiento

Mejores prácticas de protección de datos

Cuidado con transacciones muy pequeñas

Identificar las pruebas de la tarjeta lo antes posible puede ayudar a evitar que los estafadores utilicen los datos de la tarjeta robada para transacciones más grandes.

Vigilar las pequeñas transacciones que, de otro modo, pasarían desapercibidas.

Reglas de velocidad

Alto número de transacciones en la misma tarjeta; alto valor del pedido y método de envío más rápido; pedidos de artículos de alto precio durante el día

El número de combinaciones de reglas de velocidad es prácticamente infinito, por lo que hay que afinar la búsqueda (o dejar que un sistema de IA ayude)

Comportamiento inusual

Número inusual de solicitudes de contracargo; transferencias de gran cantidad de puntos de recompense; solicitudes masivas de restablecimiento de contraseña; compras muy grandes

Los estafadores suelen intentar trabajar con rapidez y utilizan varios datos de tarjetas robadas seguidos para maximizar la cantidad que pueden extraer.

J&A Global Compliance

¿PREGUNTAS?

J&A Global Compliance

GRACIAS POR SU ATENCIÓN

www.linkedin.com/in/juanmedranocastro

www.jaglobalcompliance.com

info@jaglobalcompliance.com / juan.medrano@jaglobalcompliance.com

Estados Unidos, Puerto Rico, Argentina, Panamá, República Dominicana y Venezuela.

001-305-335-1666