CNP WHITE PAPER

DE IDENTIFICADOR UNIVERSAL A DESTRUCTOR DE FRAUDE

Por qué la evaluación de riesgos por correo electrónico se ha vuelto indispensable para su negocio

CNPCardNotPresent.com®
THE INDEPENDENT SOURCE FOR ORIGINAL CNP NEWS

emailage™
GLOBAL FRAUD PREVENTION

DE IDENTIFICADOR UNIVERSAL A DESTRUCTOR DE FRAUDE

Por qué la evaluación de riesgos por correo electrónico se ha vuelto indispensable para su negocio

"Si tienes la capacidad como compañía de ver realmente la historia y el comportamiento detrás de una dirección de correo electrónico, ese es un gran indicador de fraude". –Brett "Gollumfun" Johnson

¿Por qué un ex hacker y pionero en el fraude tarjeta no presente cree que la evaluación de riesgos del correo electrónico podría ser el arma más importante en el arsenal antifraude de una empresa? Porque es la única pieza de información que identifica y acompaña a cada transacción de comercio electrónico. Y, porque los defraudadores valoran la eficiencia tanto como lo hace cualquier organización.

Hasta donde se puede decir que una sola persona es considerada responsable de la proliferación del fraude con tarjeta inexistente y del desarrollo de muchas de sus técnicas más perniciosas, Brett Johnson es ese individuo. Bajo el nombre de pantalla "Gollumfun", él y otros notorios ciberdelincuentes establecieron Shadow Crew, el primer foro en línea donde los hackers y estafadores se juntaban para comprar y vender información robada y para intercambiar consejos, estrategias y formas en constante evolución de monetizar esa información. Cuando escuchas el término "Dark Web", Shadow Crew es donde comenzó todo.

Johnson ha recorrido un sinuoso camino desde hacker/estafador famoso, a el delincuente más buscados en EE. UU., A prisionero federal, hasta ex convicto y ladrón reformado. Actualmente, se gana la vida asesorando a empresas legítimas sobre cómo protegerse de personas exactamente como él. Fue un innovador en fraudes y pasa mucho tiempo en los antiguos lugares en línea que solía visitar para mantenerse informado sobre cómo ha evolucionado su negocio. Y, en este peligroso momento, Johnson está convencido de que contar con un proceso para evaluar el riesgo de una dirección de correo electrónico asociada con una transacción o cuenta en línea es lo más importante que una empresa puede hacer para protegerse.

La Dirección de Correo Electrónico Como un Pasaporte Digital Global

Originalmente, las empresas comenzaron a recopilar direcciones de correo electrónico de clientes o solicitantes para establecer un canal de comunicación abierto y directo, una actividad de servicio al cliente. Los clientes vieron la utilidad y se sintieron cómodos suministrando su correo electrónico en todas sus interacciones en línea. Las empresas vieron rápidamente su valor como identificador.

Desde una perspectiva digital, dos características la convierten en la mejor forma de identificación. Es omnipresente: hay 2.700 millones de usuarios activos de correo electrónico en todo el mundo (la siguiente cuenta rastreable más cercana sería Facebook, con 1.600 millones, lo que requiere una dirección de correo electrónico válida para crear una cuenta). Y es persistente: el 91 por ciento de los usuarios activos de correo electrónico han tenido la misma dirección durante al menos tres años y el 51 por ciento han conservado la misma dirección de correo electrónico activa durante al menos 10 años.[1]

DE IDENTIFICADOR UNIVERSAL A DESTRUCTOR DE FRAUDE

Por qué la evaluación de riesgos por correo electrónico se ha vuelto indispensable para su negocio

De acuerdo con Amador Testa, Jefe de Producto (CPO) de inteligencia de correo electrónico de Emailage, no existe una sola pieza información que pueda decirte tanto sobre un usuario en línea como una dirección de correo electrónico.

"Realmente vemos la dirección de correo electrónico como el pasaporte digital global de una persona", dice Testa. "El correo electrónico funciona en todas partes y todos están en el mismo estándar: un identificador, un 'arroba' y un dominio, independientemente de dónde se encuentre una persona en el mundo".

Creando un 'Pasaporte' Falso

Por lo tanto, la utilidad del correo electrónico tanto para los comerciantes en línea como para sus clientes quedó bien establecida y el correo electrónico surgió como la única información requerida para cada transacción. Pero, como el potencial del comercio electrónico como herramienta para el fraude se hizo evidente para el elemento criminal, otra característica del correo electrónico permitió a los ladrones cumplir con ese requisito: no es difícil crear una cuenta de correo electrónico. Si cada transacción en línea y cada cuenta en línea solo necesitaran una dirección de correo electrónico válida como identificación, los estafadores simplemente harían lo que han estado haciendo en el mundo físico desde siempre: crear una identificación falsa.

Desde la primera instancia de fraude con tarjeta no presente hasta el día de hoy, según Johnson, el proceso para que los delincuentes moneticen la información robada en línea casi siempre comienza de la misma manera: recibir la información robada y luego crear una dirección de correo electrónico.

"El objetivo de un defraudador es conseguir que el puntaje de fraude de una transacción sea lo más bajo posible siempre que sea posible", explica. "Para hacer eso, comprará una tarjeta y luego generará un correo electrónico con el nombre en la tarjeta" en "algún dominio".

Johnson dice que ha envejecido las direcciones de correo electrónico en el pasado y otros probablemente lo estén haciendo ahora, pero la mayoría de los delincuentes quieren que el nombre en la dirección de correo electrónico se asocie de algún modo con el nombre en la tarjeta. Los defraudadores son muy conscientes de que los identificadores genéricos generan más alertas en la detección de fraudes de un comerciante que si el identificador tiene el mismo nombre que el instrumento de pago.

"Los delincuentes serios investigan compañías de seguridad", advierte. "Verán cómo operan esos proveedores y tratarán de identificar qué empresas realmente están midiendo las direcciones de correo electrónico. Entonces están empezando a envejecerlos. Esa es la forma en que los estafadores experimentados tienden a trabajar ".

El dominio es otra área que aprovechan los defraudadores en un intento de lanzar sistemas antifraude fuera del camino, dice Johnson. Una cuenta de correo electrónico gratuita de un servicio como Gmail, Yahoo o Hotmail es buena para clientes legítimos con una serie de otras características (por ejemplo, una dirección de envío igual a la dirección de facturación) de las que no se levantarán banderas de fraude. Un estafador estará haciendo otras cosas sospechosas. Como resultado, él (o ella) tratará de reducir el puntaje de fraude de una transacción de cualquier manera que pueda. Pero aunque los defraudadores pueden crear constantemente nuevos correos electrónicos, es extremadamente raro que los clientes legítimos lo hagan.

DE IDENTIFICADOR UNIVERSAL A DESTRUCTOR DE FRAUDE

Por qué la evaluación de riesgos por correo electrónico se ha vuelto indispensable para su negocio

Los estafadores expertos están usando direcciones .edu o han comprado dominios comerciales basados en negocios existentes. En ambos casos, una compra de comercio electrónico por parte de un estudiante o una empresa, una discrepancia entre la dirección de envío y la de facturación no generará tantas banderas.

Como siempre, los defraudadores se adaptan. Pero, no importa qué técnicas usen, no pueden evitar crear una dirección de correo electrónico. Como señala Johnson, "el correo electrónico cruza todo el espectro del cibercrimen". Tener tanta visibilidad como sea posible en la historia de la dirección de correo electrónico asociada con un pedido de comercio electrónico, la solicitud de préstamo o la cuenta bancaria es vital. De hecho, en la opinión informada de Johnson, es fundamental para la postura de seguridad de una empresa "tener un administrador de firewall y contraseñas".

Pero, ¿cómo puede una empresa obtener esa visibilidad?

Evaluación del Riesgo del Correo Electrónico Como un Servicio

¿Cuándo fue la última vez que abriste una cuenta o compraste algo en línea sin una dirección de correo electrónico? Es casi imposible. La dirección de correo electrónico ha evolucionado como el único identificador -el pasaporte digital- de cada usuario en línea. Los comerciantes se han dado cuenta rápidamente de su potencial para validar compradores durante las transacciones de comercio electrónico. Sin embargo durante mucho tiempo, este potencial no se visualizo, de acuerdo con Testa.

"Los comerciantes estaban recopilando el correo electrónico, pero haciendo muy poco con él, desde el punto de vista de la prevención del fraude", explica. "Ellos estaban construyendo listas blancas y negras. ¿He visto ese correo electrónico asociado con un evento de fraude? ¿He visto ese correo electrónico asociado con un buen cliente? Pero eso fue solo para clientes que regresan. Si un comerciante tenía un nuevo cliente, el correo electrónico no tenía mucho valor desde la perspectiva de la prevención del fraude ".

Eventualmente, los comerciantes comenzaron a hacer más y mejores preguntas sobre las direcciones de correo electrónico asociadas con sus transacciones en línea. ¿Es este correo electrónico válido y activo? ¿Cuánto tiempo ha estado activo? ¿Cuándo fue creado? ¿Ha sido asociado con un evento de fraude en otra compañía?

Desafortunadamente, muchas de esas preguntas quedaron sin respuesta. Las empresas no tenían visibilidad de cuándo se crearon los correos electrónicos, solo cuando los habían visto por primera vez. Tampoco sabían sobre eventos de fraude fuera de su propia compañía.

DE IDENTIFICADOR UNIVERSAL A DESTRUCTOR DE FRAUDE

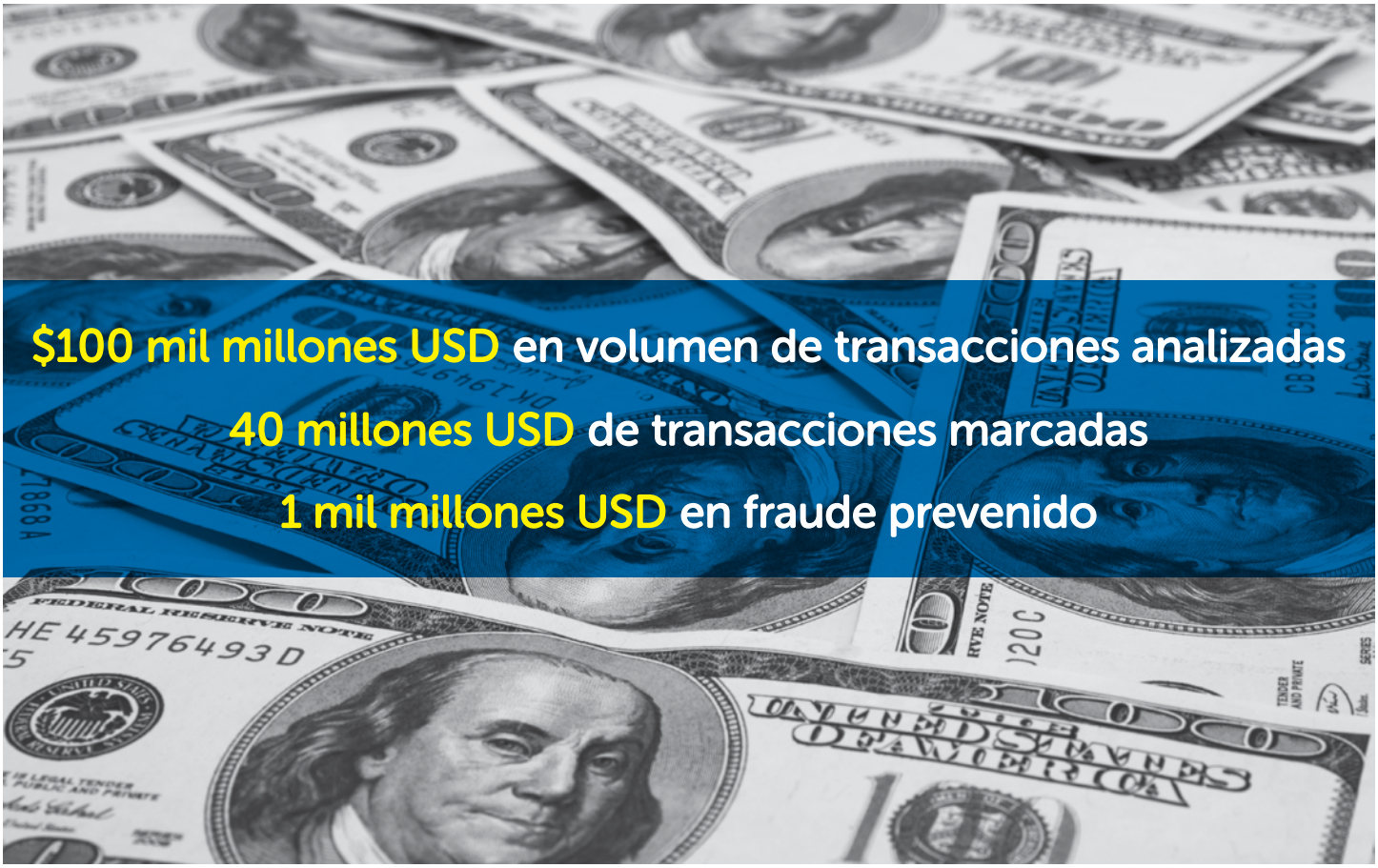
Por qué la evaluación de riesgos por correo electrónico se ha vuelto indispensable para su negocio

A mediados de la década de 2000, Yahoo comenzó a compartir información sobre la validez y la antigüedad de los correos electrónicos con los comerciantes. Pero, si bien fue un desarrollo increíblemente bienvenido, solo permitió a las empresas investigar los correos electrónicos de Yahoo y en unos pocos años, Yahoo suspendió el servicio.

Introduciendo a Emailage basado en Arizona.

Fundado en 2012, Emailage fue el primer servicio de terceros dedicado estrictamente a acumular inteligencia en direcciones de correo electrónico. A través de diversas asociaciones, fuentes de datos y tecnología de aprendizaje automático, Emailage puede construir un perfil histórico asociado con cualquier dirección de correo electrónico y generar una puntuación que predice qué tan confiable es el usuario.

Lo que Emailage proporciona a las empresas no lo pueden hacer por sí mismas, según Testa, es la escala y el acceso a una red.



DE IDENTIFICADOR UNIVERSAL A DESTRUCTOR DE FRAUDE

Por qué la evaluación de riesgos por correo electrónico se ha vuelto indispensable para su negocio

"Cualquiera puede tratar de construir inteligencia sobre la identidad, sobre cuánto tiempo han estado activos los correos electrónicos, si se han asociado con la actividad social o si se han relacionado con eventos de fraude", dice. "Pero es un proceso intensamente manual para las empresas que intentan hacerlo por sí mismas y tienen una visibilidad limitada de algunas de las características que seguimos".

Además de la edad de una dirección de correo electrónico y el nombre de su propietario, Emailage puede decir en qué país se originó, conectarlo con datos de IP, detectar irregularidades como caídas y más. Además, su algoritmo puede identificar patrones sospechosos debido al tamaño de su red.

> *"Hay muchas compañías evaluando el riesgo de fraude...algunos son impulsados por dispositivos, algunos son basados en datos genéricos, otros se basan en el aprendizaje automático. Pero nosotros podemos aprovechar todas estas tecnologías y conectar esos elementos con el correo electrónico"*

También hay una otra cara de la moneda: el mismo proceso funciona con clientes legítimos. Cuando puede identificar comportamientos positivos, puede aprobarlos más rápidamente.

Entre los más de 1,000 clientes que confían en Emailage para la evaluación de riesgos de correo electrónico se encuentran cuatro de los seis bancos emisores más importantes de EE. UU., Uno de los 10 principales minoristas de comercio electrónico, tres de las cinco mayores aerolíneas mundiales, los tres principales fabricantes de computadoras y las cinco principales empresas de transferencia de dinero P2P. Además, muchos más son parte de la red a través de asociaciones con las cinco plataformas antifraude más grandes.

Con la visibilidad de los miles de millones de transacciones generadas por las empresas que utilizan su servicio, todas las empresas conectadas a su red se benefician de una visión holística del riesgo del correo electrónico. Si un correo electrónico está asociado con un caso de fraude confirmado en uno de sus clientes, se alerta a cada cliente. Es un poderoso multiplicador de fuerza.

"Hay muchas compañías evaluando el riesgo de fraude", señala Testa. "Algunos son impulsados por dispositivos, algunos son basados en datos genéricos, otros se basan en el aprendizaje automático. Pero nosotros podemos aprovechar todas estas tecnologías y conectar esos elementos con el correo electrónico ".

DE IDENTIFICADOR UNIVERSAL A DESTRUCTOR DE FRAUDE

Por qué la evaluación de riesgos por correo electrónico se ha vuelto indispensable para su negocio

Caso de estudio: Abercrombie and Fitch

Introducción: La marca de ropa minorista Abercrombie and Fitch obtuvo casi un tercio de los 1.04 mil millones USD en ingresos del cuarto trimestre de 2016 del canal en línea. De acuerdo con el Analista de Fraude Senior Trent McGough, la principal preocupación de fraude de la compañía se centra en su programa de tarjeta de regalo electrónica. Desde la implementación de Emailage, McGough dice que A&F no solo ha podido prevenir decenas de miles de dólares en fraudes con tarjetas de regalo electrónicas por mes, ha permitido a la compañía aprobar automáticamente miles de pedidos por trimestre que anteriormente se hubieran detenido para su revisión manual.

El problema: Hace varios años, McGough y su equipo notaron un aumento preocupante en los contracargos asociados con las compras de tarjetas de regalo electrónicas. Notaron algunas anomalías con los correos electrónicos asociados con los pedidos de tarjetas electrónicas de regalo y comenzaron a buscar formas de encontrar más información sobre esas direcciones de correo electrónico. En ese momento, Yahoo compartiría cuándo se crearon sus cuentas de correo electrónico con los comerciantes que solicitaron la información. A&F se benefició de esa visibilidad, pero solo para los correos electrónicos de Yahoo y solo hasta que Yahoo suspendió el servicio. McGough necesitaba más información sobre los correos electrónicos que llegaban a las órdenes de tarjetas de regalo electrónicas.

La solución: McGough evaluó varios proveedores y eligió Emailage. Inicialmente el minorista usó el servicio solo por clic para pedidos que ya se habían retenido para su revisión manual. El equipo de fraude de A&F utilizó Emailage para verificar la edad de las cuentas de correo electrónico en esos casos. Con base en los éxitos en ese entorno, McGough comenzó a realizar pruebas en el otoño de 2016 para evaluar la expansión del servicio y agregarlo de una manera más automatizada. A través de pruebas, la compañía decidió utilizar Emailage para seleccionar automáticamente todos los pedidos solicitados para revisión manual, todos los pedidos de tarjetas de regalo electrónico y todos los pedidos superiores a 150 USD.

El resultado: Las pruebas revelaron dos efectos.

1. Actividad significativamente más fraudulenta, que los controles previos habrían aprobado, fueron detenidos
2. Los falsos positivos que involucran a clientes legítimos también se redujeron

En los primeros cuatro meses de 2017, McGough dice que Abercrombie y Fitch evitaron casi 150,000 USD de fraude que habrían sido aprobados bajo su viejo sistema. Además, durante el mismo período de tiempo, casi 4,000 pedidos legítimos que se habrían retenido para su revisión se aprobaron automáticamente con un bajo puntaje de riesgo de Emailage.

Abercrombie & Fitch datos de fraude del 2017

	Ordenes Fraudulentas Prevenidas	Revisiones Manuales Prevenidas
Enero	180	952
Febrero	237	856
Marzo	287	984
Abril	214	1,072

"Hemos visto un retorno de la inversión muy convincente de Emailage", dice McGough. "Definitivamente expandimos el programa desde donde comenzamos y solo lo hicimos porque encontramos valor en él. Ha habido muchas ocasiones en donde usando la dirección de correo electrónico he podido detectar que el pedido se ve extraño, pero luego se puede saber a nombre de quién está registrado o que su información coincide con el nombre. Otras veces que descubrió un correo electrónico se creó hace dos días. Si el pedido ya se veía un poco sospechoso, es muy fácil rechazar el pedido usando eso. Encontré que la evaluación de riesgos por correo electrónico es un buen indicador de conductas positivas y negativas ".

Conclusión

La dirección de correo electrónico se ha convertido en el identificador más importante relacionado a la actividad en línea. Es omnipresente, forma parte de casi todos los inicios de sesión, transacciones o cuentas creadas o realizadas en la arena digital. Y, aunque los estafadores intentan adaptarse, no hay forma de evitar el hecho de que, para cobrar, deben robar o crear una dirección de correo electrónico.

Como dijo el ex estafador Johnson, "cada cosa sobre la legitimidad de una transacción depende del historial y la actividad de una dirección de correo electrónico. Y la mejor manera para que los estafadores funcionen es crear una cuenta de correo electrónico bajo demanda. En este momento, es extremadamente vital para las compañías que realizan la detección de fraudes tener un sistema implementado para evaluar las direcciones de correo electrónico como un factor de riesgo ".

DE IDENTIFICADOR UNIVERSAL A DESTRUCTOR DE FRAUDE

Por qué la evaluación de riesgos por correo electrónico se ha vuelto indispensable para su negocio

Sobre Emailage

Como centro global de inteligencia de correo electrónico, el equipo de Emailage tiene un objetivo singular: unir a las empresas en el combate contra el fraude. Aprovechamos el poder de la dirección de correo electrónico para ayudar a nuestros clientes a equilibrar la detección efectiva de fraude con una gran experiencia del cliente. Las empresas de todo el mundo usan nuestra puntuación predictiva en transacciones de todo tipo. El crecimiento constante de nuestra red permite que el 90% del fraude detectado sea impulsado por atributos provenientes de nuestros algoritmos patentados. Antes de que Emailage se fundara en 2012, las empresas confiaban en sus propias tecnologías y bases de datos aisladas para incorporar el correo electrónico en sus herramientas de fraude. Esto consistió principalmente en procesos manuales, comparaciones uno a uno y mantenimiento de listas negras internas. Emailage ha cambiado todo el panorama del fraude rompiendo estos silos con una cobertura global sin igual y un compromiso para unir a las compañías en el combate contra el fraude.

Sobre CardNotPresent.com

CardNotPresent.com, parte del Grupo RELX, es una voz independiente que genera noticias, información, educación e inspiración originales para las empresas y personas que operan en el espacio de tarjetas no presentes, una de las únicas fuentes de contenido enfocado exclusivamente en este creciente segmento de la industria de pagos. Nuestro único producto es la información. Nuestro único objetivo es proporcionarlo de manera imparcial a nuestros suscriptores. Las plataformas de medios de la compañía incluyen el portal CardNotPresent.com, el centro de noticias, información y análisis sobre los problemas de pagos que la mayoría afecta a los comerciantes que operan en el giro; el Informe CNP, un boletín electrónico que entrega esa información enfocada directamente en su bandeja de entrada de correo electrónico dos veces por semana sin ningún tipo de confusión; la CNP Expo, una reunión anual de las compañías líderes en el giro, desde los sitios web más pequeños de comercio electrónico y proveedores de tecnología hasta minoristas globales y procesadores de pagos; y los Premios CNP, un evento anual que rinde homenaje a los productos y soluciones en los que confían los comerciantes de CNP para aumentar las ventas. Para más información visite www.CardNotPresent.com.

Este documento fue producido en un esfuerzo conjunto entre CardNotPresent y Emailage.

PIE DE NOTAS

1. DMA Insight: Estudio de seguimiento del correo electrónico del consumidor, 2015.
https://dma.org.uk/uploads/56543b6e6d645-email-tracking-report-2015_56543b6e6d5b5.pdf