vesta.io

5400 Meadows Road, 5th Floor
Lake Oswego, OR 97035 USA

Informe Vesta: el fraude CNP se está volviendo cada vez más sofisticado y crea nuevas amenazas para los comerciantes de todo el mundo

El análisis de fraude global muestra que el fraude de CNP cuesta a los comerciantes millones de dólares en ingresos anuales y los estafadores se vuelven más sofisticados con sus ataques cada trimestre.

Septiembre, 2021. - Vesta, una plataforma de garantía de transacciones de extremo a extremo para compras en línea, lanzó hoy su primer Informe global de fraude con tarjeta no presente (CNP), que incluye un análisis de millones de transacciones digitales desde el primer trimestre de 2020 hasta el primer trimestre de 2021 para rastrear cómo evolucionó el fraude CNP durante ese período de tiempo. El porcentaje general de transacciones globales que su sistema identificó como potencialmente fraudulentas varió del 10% al 13%, con el valor promedio de cada transacción fraudulenta entre $126 y $155 dólares. Sin embargo, los intentos de fraude no se distribuyen de manera uniforme: los intentos fraudulentos contra comerciantes individuales oscilaron entre el 0.8% y más del 30%, según la verticalidad comercial y la geografía.

Una transacción CNP ocurre cuando se realiza una venta sin que el cliente presente físicamente su tarjeta de crédito al comerciante, y cuando una transacción CNP resulta ser fraudulenta, la responsabilidad recae en el comerciante. Cuando un comerciante aprueba una transacción CNP fraudulenta, se genera un contracargo, y los contracargos vienen con tarifas, a veces de hasta $25 dólares por incidente. En el primer trimestre de 2020, Vesta descubrió que el 13% de las transacciones totales probablemente eran fraudulentas y, por lo tanto, bloqueó esas transacciones para proteger a sus clientes. Es importante recordar que el 13% es un número agregado, que incluye a los comerciantes de alto y bajo riesgo. Para los comerciantes de bajo riesgo, Vesta aprobó hasta el 99% de todas las transacciones, pero para los comerciantes de alto riesgo esa tasa de aprobación varió mucho según la actividad fraudulenta. Para los comerciantes de alto riesgo que no tienen una solución como la de Vesta, aprobar tantas transacciones fraudulentas puede tener un impacto terrible tanto en los ingresos como en la reputación general de la marca.

“Si usted es una empresa de comercio electrónico que realiza 5 millones de transacciones por año y el 13% de ellas son fraudulentas, está experimentando 650,000 transacciones no auténticas, y si cada una de ellas viene con una tarifa de devolución de cargo de $ 25, entonces está gastando más de $16 millones de dólares en honorarios”, dijo Ron Hynes, director

© 2021 Vesta. All rights reserved.

ejecutivo de Vesta. “Por otro lado, si rechaza demasiadas transacciones legítimas en un esfuerzo por combatir el fraude, termina con pérdidas significativas. Por ejemplo, si ese mismo comerciante que realiza 5 millones de transacciones por año tiene un valor de pedido promedio de $125 dólares y bloquea el 30% de todas las transacciones, cuando solo el 13% eran fraudulentas, ahora está perdiendo más de $100 millones en ingresos anuales. Eso es lo que hace que el fraude CNP sea un problema tan difícil de abordar: debe lograr el equilibrio perfecto entre la lucha contra el fraude y, al mismo tiempo, maximizar las aprobaciones de transacciones legítimas”.

Hay cinco sistemas operativos que componen la mayoría de los pedidos de comercio electrónico: Android, iOS, Linux, OS X y Windows. Para comprender mejor cómo los sistemas operativos afectan el fraude de CNP, Vesta analizó el porcentaje de transacciones fraudulentas realizadas en cada una, así como el valor promedio de esas transacciones. Descubrió que Android es el sistema operativo con el porcentaje más alto de transacciones fraudulentas, con hasta un 26% en el primer trimestre de 2020, pero el monto promedio en dólares más bajo, lo que sugiere que los estafadores lo usan con frecuencia para transacciones de menor valor. El valor de las transacciones fraudulentas es más alto en OS X y Windows, lo que indica que los estafadores realizan sus ataques más costosos a través del escritorio.

Otro elemento crítico del informe de Vesta es un análisis del fraude CNP con vinculación directa en comparación con vinculación indirecta. La vinculación directa significa que existe una conexión común dentro de las transacciones que los comerciantes pueden buscar como signos de posible fraude; por ejemplo, si llegan cinco pedidos al mismo tiempo, para el mismo artículo y desde la misma dirección de correo electrónico, es una señal clara de que las transacciones pueden ser fraudulentas. La vinculación indirecta significa que las transacciones están vinculadas a través de una red de elementos más compleja, a menudo una señal de estafadores más sofisticados que intentan cubrir sus huellas, lo que hace que sea muy difícil para los comerciantes detectarlas.

“Desafortunadamente, estamos viendo transacciones fraudulentas con vínculos indirectos que aumentan en todos los ámbitos, y el valor promedio de esas transacciones es más alto que el de aquellas con vínculos directos, lo que hace que sea un problema aún más costoso y complicado para los comerciantes”, dijo Hynes. “La única forma de identificar y prevenir eficazmente el fraude de CNP con vínculos indirectos es con el aprendizaje automático, y es fundamental utilizar modelos que han sido entrenados con base en millones de transacciones globales y, por lo tanto, pueden establecer conexiones que los humanos simplemente no pueden ver”.

© 2021 Vesta. All rights reserved.

Puede ver el Informe global de fraude CNP completo de Vesta aquí. Para obtener más información sobre Vesta y sus soluciones de garantía de transacciones y prevención de fraude, visite www.vesta.io.

*****

Sobre Vesta

Vesta es la única plataforma con garantía de transacciones instantáneas integrales para las compras en línea que logra índices de aprobación incomparables, ofrece una mejor experiencia al cliente y elimina el fraude para marcas líderes en telecomunicaciones, comercio electrónico, viajes y servicios financieros. Utilizando el aprendizaje automático respaldado por 25 años de datos transaccionales, Vesta incrementa las aprobaciones de ventas legítimas para sus clientes, al tiempo que elimina los contracargos y otras formas de fraude digital, lo que reduce el costo real del fraude a cero y transfiere el 100 % de la responsabilidad del fraude, incluido el procesamiento de contracargos, para que los clientes puedan centrarse en aumentar las ventas. La compañía tiene su sede en Portland, OR, y oficinas en Atlanta, Miami, Irlanda, México y Singapur. Para obtener más información, visita www.vesta.io.

Contacto de prensa

Michelle O'Rourke
Clarity PR for Vesta
vesta@clarity.pr

© 2021 Vesta. All rights reserved.