paygilant

Fraudless. Frictionless. Effortless.

La Importancia de ser Mobile-first

Prevención de Fraude Móvil vs. Web

White paper

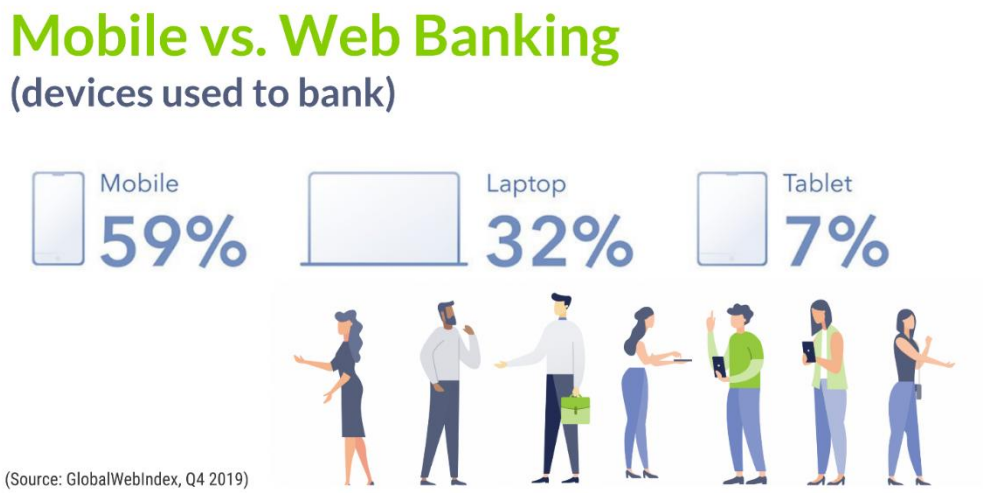
paygilant.com

Durante el año pasado, los encierros por coronavirus y el distanciamiento social han transformado por completo el panorama de los pagos. Las transacciones cara a cara han sido reemplazadas por métodos de pago digitales nuevos y emergentes, y junto con esto los estafadores están explotando el cambio acelerado a los pagos digitales.

Según un estudio reciente de Javelin Strategy Research y SAS, el fraude digital sigue siendo un fenómeno mundial multimillonario. Si bien los pagos digitales son rápidos, el fraude se mueve con la misma rapidez.

El fraude digital se puede dividir en dos sectores principales: fraude web y fraude móvil. Si bien ambos canales conllevan importantes pérdidas por fraude, las técnicas actuales de prevención del fraude no son suficientes para reducir el fraude en ambos canales por igual.

Si bien los métodos que utilizan los estafadores están evolucionando, las organizaciones han implementado múltiples controles antifraude para mantener a raya el fraude en la web. Según un informe de CyberSource, la tasa de fraude para las transacciones en línea (sin incluir dispositivos móviles) se ha mantenido estable desde 2010. Dado que la motivación de los estafadores para retirar efectivo no ha disminuido, la conclusión es que el fraude se desplaza hacia los canales menos protegidos y de rápido crecimiento, como lo es el canal móvil.



El fraude móvil ha aumentado en un 170% durante los últimos dos años y el uso de la banca móvil y los pagos durante la pandemia también han exasperado la situación. En junio de 2020, el FBI informó que con el aumento del 50% en la banca móvil desde principios de año, el riesgo de fraude está aumentando, respectivamente. Los troyanos bancarios basados en aplicaciones y las aplicaciones bancarias falsas se encontraban entre la variedad de técnicas que el FBI dijo que espera que empleen los estafadores.

En 2020, los estafadores continuaron alejándose del fraude web, mostrando un 62% de intentos de ataques de fraude de pagos provenientes de dispositivos móviles, en comparación con un 51% en 2019.

Seguridad Contra el Fraude Online

El fraude en línea ha sido un problema desde el comienzo del comercio electrónico a principios de los años 90. Internet era un concepto nuevo y las empresas no eran totalmente conscientes de sus riesgos. Las primeras estafas en línea llegaron en forma de estafadores que usaban tarjetas de crédito robadas y las atribuían a celebridades populares de la época. Siguió el robo de identidad masivo en línea. Estos eventos provocaron el nacimiento de la seguridad contra el fraude en línea y una gran cantidad de innovaciones adecuadas para la web:

Programas anti-malware
Estos se implementan en el servidor y el punto final (endpoint) para proteger contra el malware (software malicioso) adquirido en línea, el cual puede usarse para robar la identidad de una persona o la información de la tarjeta de crédito.

Cifrado del Sitio (Site Encryption)
Esto lo implementa el propietario del sitio web para proteger a los usuarios que navegan por la web. Esto es especialmente útil cuando se utilizan conexiones Wi-Fi públicas no seguras.

Geolocalización
Esto se implementa en el lado comercial e identifica la ubicación de un dispositivo para detectar fraudes. La ubicación de un desktop se puede determinar mediante la geolocalización WIFI o IP.

Seguridad Contra Fraudes Móviles

El fraude móvil se refiere a intentos de transacciones o transacciones fraudulentas realizadas en un entorno móvil, ya sea a través de una aplicación móvil o el navegador de un dispositivo móvil. El fraude móvil a veces se aprovecha de las debilidades inherentes a las aplicaciones que están vinculadas a los bancos Challenger/Neo, billeteras electrónicas, y comercio electrónico. La obtención de acceso a una aplicación bancaria móvil o billeteras digitales abre oportunidades de explotación para los estafadores. Los ejemplos de fraude móvil incluyen P2P fraudulento, transacciones de comercio electrónico, colusión fraudulenta de comprador / vendedor dentro de un mercado móvil, y cuentas de pago desde cuentas poseídas, entre otros.

El fraude móvil también puede ser perpetrado por estafadores que en realidad no utilizan un dispositivo móvil. Esto se hace mediante "emuladores" que permiten que el delincuente aparezca como si estuviera conectado desde un dispositivo móvil. Estas herramientas les permiten realizar compras a través de aplicaciones móviles o sitios web móviles, mientras que en realidad se utiliza una computadora portátil o de escritorio. Esto proporciona a los defraudadores una enorme escalabilidad y flexibilidad al fingir que provienen de una ubicación diferente y parecer que utilizan un dispositivo diferente para cada transacción / víctima.

Web vs. Móvil

Muchos de los métodos que se utilizan habitualmente para proteger las transacciones web no son eficaces para los dispositivos móviles. Por ejemplo, las direcciones IP móviles cambian constantemente a medida que un usuario se desplaza por las redes. Los usuarios también actualizan sus teléfonos de vez en cuando para estar al día con los modelos más nuevos. Esto dificulta la obtención de información sólida y la detección de fraudes. El hecho de que los dispositivos móviles sean por naturaleza “móviles” presenta un desafío para los defensores de la seguridad tradicional contra el fraude.

Si bien los atributos de comportamiento se pueden capturar en los navegadores, estos datos no son tan diversos. Los navegadores se limitan a la dinámica del mouse y el teclado. En un mundo donde los datos lo son todo, una menor cantidad de datos significa un perfil de comportamiento más débil. Además, las soluciones de biometría de comportamiento basadas en la web tienden a generar más falsos positivos. Esta es otra razón por la que el canal móvil presenta una oportunidad única para que las

organizaciones actualicen sus protecciones de prevención de fraude mediante el uso de nuevos métodos que reducen la fricción, los falsos positivos y aumentan la seguridad.

En el mundo del fraude móvil, la diversidad y cantidad de indicadores de fraude se han convertido en los principales métodos de prevención del fraude:

Huella Digital del Dispositivo

Esto se implementa para identificar un dispositivo específico en función de sus características únicas. Este es uno de los métodos más comunes y efectivos que se utilizan para detectar fraudes y verificar a los usuarios que regresan.

Biometría de Comportamiento

La biometría de comportamiento se utiliza para detectar actividad no humana y autenticar a los usuarios. Las pantallas táctiles móviles están equipadas para recopilar grandes cantidades de datos como el tamaño de la huella digital, presión, el comportamiento de deslizar y más. Los dispositivos móviles tienen el potencial de recopilar datos de latidos del corazón y patrones de venas. Una pantalla táctil puede discernir si las palmas de las manos de un usuario están sudando o no. Las empresas continúan innovando y descubriendo nuevas formas para que los dispositivos móviles recopilen datos de comportamiento. Por lo tanto, los atributos de datos que se utilizan para indicar si una persona es legítima o un defraudador suelen ser correctos.

Análisis de Transacciones

El análisis de transacciones se basa principalmente en el perfil del cliente y los hábitos de transacción. Analiza los datos de las transacciones (montos, beneficiarios, frecuencia, etc.), pero también los metadatos asociados a cada operación (por ejemplo, la ubicación del pago de una transacción, la ubicación del teléfono inteligente).

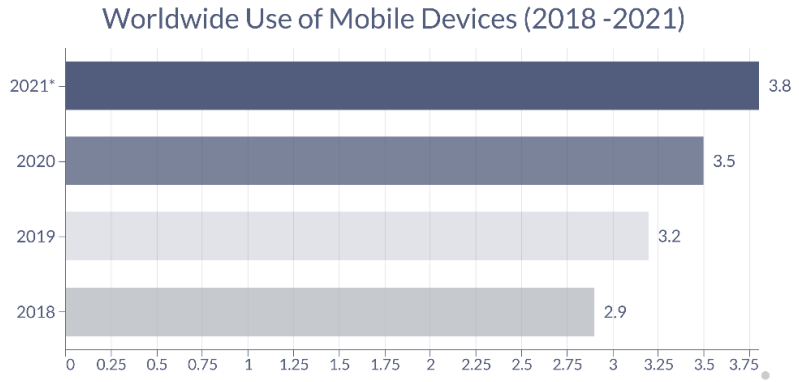
Estos datos recopilados abren una nueva dimensión para el análisis de la identidad de los clientes. A diferencia de los procesos de KYC (*Know Your Customer*) tradicionales, que representan una imagen bastante estática del cliente, una "identidad digital" puede evaluar dinámicamente el comportamiento del cliente mediante el análisis de los datos de la transacción (monto, beneficiario, emisor, etc.) y sus metadatos asociados. El nivel de conocimiento y seguridad del cliente se mejora mediante la combinación de "quién es el cliente" y "qué hace el cliente".

El Futuro en Prevención de Fraudes

Es importante reconocer que los canales web y móviles son diferentes. Lo que funciona para computadoras de escritorio no funcionará automáticamente para dispositivos móviles.

La realidad es que la Generación Z, los Millennials y, de hecho, todos nosotros aumentamos el uso de nuestros dispositivos móviles, al tiempo que disminuimos el uso de una computadora. Dicho esto, las empresas deben adaptarse a los tiempos o quedarse atrás. Esto implica adoptar métodos de prevención de fraude más avanzados y efectivos para garantizar una excelente experiencia de usuario y, al mismo tiempo, evitar la pérdida de dinero.

En todo el mundo para 2021, habrá 3.800 millones de usuarios de smartphone, y se prevé que el recuento de estos aumentará gradualmente año tras año.



Crecimiento (y Riesgo) de ser Centrado en Móvil

Es un hecho que los estafadores siguen el dinero, y con el fuerte crecimiento de las transacciones globales que se realizan a través de teléfonos móviles, es un terreno de caza rentable para los estafadores. Por eso es imperativo que las empresas y las instituciones financieras examinen más de cerca sus estrategias y controles de prevención de fraude móvil. Muchas instituciones financieras utilizan sistemas de gestión de riesgos obsoletos basados en procesos manuales, un residuo de los días en que los clientes visitaban sus instituciones financieras en persona para solicitar préstamos, retirar dinero, y realizar otras actividades bancarias. La propia naturaleza de las aplicaciones móviles requiere un cambio en los sistemas de gestión de riesgos de los bancos.

Los sitios de comercio electrónico también están tratando de adaptar las soluciones existentes a los dispositivos móviles, cuando es mucho mejor pensar en soluciones de prevención de fraude diseñadas específicamente para el canal móvil. Dado que no existe una solución milagrosa para erradicar el fraude móvil, las organizaciones deben considerar los métodos de prevención de fraude centradas en móviles (mobile-first) como un salvavidas principal.

En el mundo digital, el dispositivo de una persona actúa como su identidad en línea. También es una pieza de "identidad" que es mucho más difícil de reemplazar para los estafadores, en lugar de identificadores fácilmente intercambiables, como las direcciones de correo electrónico. Distinguir los dispositivos de los clientes a través de sus características únicas y analizarlos independientemente de los datos personales, permite a las empresas verificar los dispositivos de transacción y verificar al cliente conectado. Cuando se trata de banca móvil, la autenticación sólida del cliente (SCA) puede incluso eliminar la necesidad de pasos de autenticación secundarios para dispositivos confiables, identificados positivamente, lo que reduce en gran medida la fricción con el cliente.

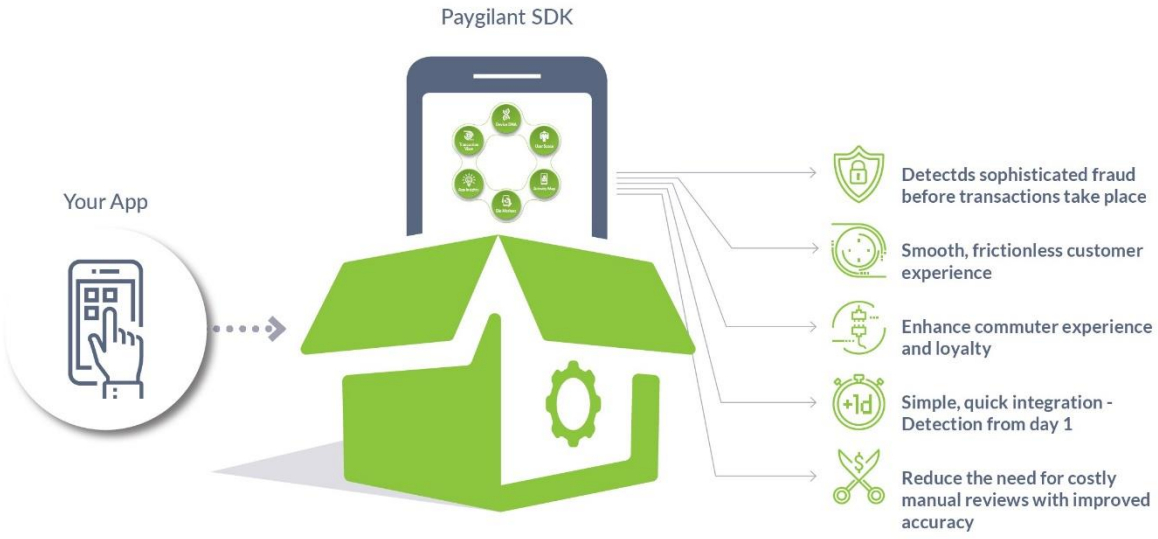
Una opción adicional a la que los bancos y las empresas pueden recurrir en la lucha contra el fraude móvil es una solución SDK (kit de desarrollo de software) móvil. Los SDK móviles de prevención de fraude se pueden integrar fácilmente en la aplicación existente, con un fragmento de código corto que permite a las empresas detectar anomalías de alto riesgo en todas las plataformas bancarias y de pagos móviles (billeteras electrónicas, aplicaciones de banca móvil, pagos con un solo clic, etc.). La ayuda del aprendizaje automático (machine learning) en tales soluciones puede detectar dispositivos manipulados, la presencia de una identidad robada e incluso el fraude de cuenta nueva, fraude de cuenta sintética, y el fraude de adquisición de cuenta, que son cada vez más omnipresentes. Esto permite la aceptación instantánea y segura de la actividad bajo demanda dentro de una aplicación móvil nativa, ya sea un gran retiro bancario o una costosa compra de comercio electrónico.

Para muchos proveedores, las transacciones móviles pueden ser más seguras que las transacciones web; mientras que, para los usuarios, la autenticación móvil puede proporcionar una autenticación de baja fricción. El principio básico es que los dispositivos individuales pueden identificarse de forma segura, mientras que los usuarios individuales pueden vincularse al dispositivo a través de múltiples indicadores de fraude. Un enfoque en capas que incluye una combinación de huella digital de dispositivos, biometría de comportamiento, aprendizaje automático, y análisis de transacciones puede ayudarlo a detectar el fraude móvil, maximizar sus tasas de aprobación y contener su nueva aplicación y el fraude de transacciones.

Paygilant – Una Solución Centrada en el Móvil

La solución de Paygilant está diseñada como una solución para dispositivos móviles. Lo que hace que Paygilant sea único es que integra y correlaciona múltiples conjuntos de inteligencia que detectan con precisión el fraude y permiten una experiencia de usuario sin fricciones, libre de obstáculos, desde el lanzamiento de la aplicación hasta las transacciones en curso. Sin impactar ni imponer al usuario, Paygilant opera en el fondo de la aplicación móvil para alertar sin problemas sobre una transacción sospechosa antes de que ocurra.

La capacidad de Paygilant para proporcionar análisis de datos continuo, reduce el uso de cualquier paso de autenticación extra (códigos PIN, contraseñas, SMS OTP y otros) al mínimo. En el caso de una puntuación de alto riesgo, se activa una alerta en tiempo real para bloquear la transacción. Las puntuaciones de riesgo bajas indican un usuario fuertemente autenticado, gracias a la autenticación de múltiples factores (MFA), y una transacción que puede aprobarse de forma segura.



Sobre Paygilant

Paygilant es una empresa revolucionaria que lucha contra el fraude bancario y pagos digitales, destinada a eliminar el compromiso de intercambio entre una fuerte prevención de fraude, autenticación sin obstáculos y privacidad del usuario.

Paygilant permite que las organizaciones financieras y de comercio electrónico incrementen sus ingresos, por medio de una mejora en la experiencia del usuario y la detección de fraude, antes que se produzca la transacción. Se trata de una tecnología patentada y fácil de integrar que utiliza seis sets de inteligencia patentados, que funcionan en armonía para proporcionar valor desde el primer día. Simplemente, Paygilant activa una alerta de "riesgo" en tiempo real cuando se detecta un fraude y una alerta "segura" cuando se identifica al cliente legítimo.

Paygilant office: 10 Ben Gurion Road, Ramat Gan, Israel
E-mail: info@paygilant.com | Phone: +972-3-5221879

paygilant.com