paygilant

Fraudless. Frictionless. Effortless.

Resumen de la Solución

Introducción

paygilant.com

El mercado de pagos móviles está creciendo a un ritmo exponencial, ya que los consumidores y los comerciantes están adoptando nuevos métodos de pagos financieros, de comercio electrónico y de billetera digital. Con los pagos móviles convirtiéndose en la corriente principal, el fraude continúa cambiando el canal móvil, amenazando este ecosistema en desarrollo. Por lo tanto, el mercado digital financiero tiene el desafío de aumentar la seguridad de sus soluciones de transferencia y pago de dinero, y a su vez proporcionar una experiencia de usuario amigable, fluida y de confianza, respetando su privacidad.

Las soluciones de autenticación libre de obstáculos y de prevención de fraude móvil protegen todo el recorrido del usuario. Paygilant detecta transacciones fraudulentas desde la descarga de la aplicación hasta las transacciones en curso, autenticando sin problemas a los clientes legítimos. Esto elimina la necesidad de elegir entre ofrecer prevención de fraudes y poder dar una excelente experiencia de usuario y de privacidad.

Este documento muestra la solución móvil de detección de fraude y autenticación libre de obstáculos de Paygilant, presentando casos de uso específicos, arquitectura del producto y beneficios de la solución.

El Cambiante Panorama del Fraude Móvil

A medida que crece el uso móvil, también lo hace el fraude móvil. Los bancos en tecnología financiera (Fintech), priorizan la aplicación de una estrategia móvil al diseñar sus productos. Adicionalmente, las nuevas soluciones de pago móvil están llegando al mercado ofreciendo más valor a los consumidores, tanto a aquellos que pertenecen o no a bancos. Esto se ve en forma de pagos en la tienda, online, transferencias de dinero P2P y billeteras móviles. Así los proveedores de pagos móviles, emisores de tarjetas y comerciantes tienen el desafío de proteger sus aplicaciones y canales de pago contra distintos ataques fraudulentos:

Fraude Transaccional, Fraude de Cuentas Nuevas, Fraude de Posesión de Cuentas (ATO) y Fraude Interbancario.

Fraude de Cuentas Nuevas se refiere al uso de datos de identidad falsos o robados para abrir una cuenta nueva. Los estafadores se han convertido en expertos en el robo de identidades personales y su uso para el fraude móvil. Ya sea que los estafadores usen la verdadera identidad de alguien, o fragmentos de datos reales para crear una identidad sintética, el propósito es crear una cuenta nueva para cometer fraude.

Fraude de Posesión de Cuentas es una forma de robo de identidad obtenida a través de software malicioso, violación de datos, phishing (suplantación de identidad) y otras estrategias de manipulación social. De esta manera los estafadores toman posesión de cuentas ya existentes y validadas para utilizar el crédito en compras o liquidando por completo la cuenta.

Fraude Transaccional se produce cuando se utiliza una tarjeta de pago o datos robados para generar una transacción no autorizada. El paso a las transacciones en tiempo real está causando importantes desafíos de seguridad para bancos, comerciantes y emisores por igual. Los tiempos de transacción más rápidos aumentan las posibilidades de que las transacciones fraudulentas no se detecten.

Fraude Interbancario se refiere a un ataque de múltiples eslabones. Primero se inicia una posesión de cuenta en el banco #1, mientras el estafador crea cuentas falsas en el banco #2 (Fraude de Cuentas Nuevas) para liquidar los fondos robados. El dinero es transferido desde una cuenta externa que fue afectada (banco #1) a las cuentas nuevas (banco #2), y desde éstas últimas se transfiere todo a la cuenta legítima del estafador, donde finalmente liquida todos sus fondos.

Históricamente, los bancos, el comercio electrónico y los proveedores de billeteras digitales han estado persiguiendo la mitigación de este tipo de fraude, al tiempo que absorben las pérdidas amortizadas como un costo de hacer negocios. Sin embargo, a medida que los estafadores se vuelven más sofisticados y el costo del fraude continúa aumentando, este sentido de urgencia también está cambiando.

La Solución de Autenticación y Detección de Fraude Móvil de Paygilant

La solución de detección de fraude móvil Paygilant y la autenticación sin obstáculos, es una combinación de un SDK liviano, que se integra fácilmente, y un potente motor analítico de riesgo. Mediante el uso de sets de inteligencia únicos, la solución de Paygilant puede identificar con exactitud las transacciones legítimas o de fraude en milisegundos.

Paygilant provee un SDK diseñado para transmitir los puntos de datos necesarios de manera segura a los servidores de Paygilant, donde se genera una puntuación de riesgo. El proceso completo ocurre en milisegundos, donde la seguridad y privacidad del usuario se mantienen intactos. Paygilant aplica controles de seguridad de extremo a extremo y se adhiere a las regulaciones de privacidad globalmente.

Los 6 Sets de Inteligencia de Paygilant para Autenticar Usuarios y Prevenir Fraude Móvil

Al integrar, correlacionar y analizar los seis sets de inteligencia propietarios, Paygilant puede determinar si una transacción basada en dispositivos móviles es legítima o fraudulenta.

Paygilant analiza varios atributos a través de capas de dinámicas, que incluyen el comportamiento, dispositivo, la transacción y actividad del usuario, o si es realmente un usuario humano o bot. Esto se utiliza para tejer una representación de identidad del usuario móvil, proporcionando una puntuación que indica el nivel de riesgo de la transacción. La metodología única de fraude móvil de Paygilant consiste en múltiples conjuntos de inteligencia que incluyen Información de la Aplicación, Bio-Marcadores, Mapa de actividad, Espacio de Usuario, ADN del Dispositivo y Vista de Transacciones.

ADN del Dispositivo

Varios atributos observados en el dispositivo contribuyen en formar un ID único para cada dispositivo. Se observa el modelo de dispositivo, pantalla, memoria, UUID, OS, IP, geolocalización, emulación, rooting/jailbreaking y más. Esta fórmula de Paygilant analiza los parámetros del dispositivo de manera única, generado la nueva generación en huella digital para cada dispositivo. Esta huella digital permite identificar usuarios legítimos y ataques de fraude en serie.

Espacio del Usuario

El análisis inteligente que preserva la privacidad del espacio del usuario en el dispositivo móvil proporciona información valiosa sobre actividades fraudulentas. El Espacio del Usuario produce valor inmediato en escenarios difíciles de analizar, tales como apertura de cuentas nuevas, donde no hay historial previo sobre la existencia del usuario o dispositivo. A su vez, disminuye casi completamente los obstáculos que se presentan en la autenticación, y por ende en la experiencia del usuario. Esto se logra ya que permite distinguir entre un usuario legítimo que regresa de un nuevo dispositivo y un intento de adquisición de cuenta.

Mapa de Actividad

Paygilant analiza cómo interactúa el usuario con la aplicación móvil, generando un perfil de recorrido de la aplicación, para determinar si las interacciones son consistentes con el usuario legítimo o si es un usuario fraudulento que utiliza credenciales, tarjeta o identidad robada.

Bio-Marcadores

Paygilant observa los marcadores de comportamiento fisiológico para autenticar usuarios legítimos e identificar pasivamente actividades fraudulentas. Los bio-marcadores comunes que Paygilant observa incluyen la velocidad táctil, el intervalo de tiempo entre toques, el tamaño del dedo, la velocidad de los dedos, el ritmo de desplazamiento y arrastre, la biometría de escritura y más. La combinación de todos los factores de estos bio-marcadores crea un perfil confiable para cada usuario, legítimo o fraudulento.

Información de la Aplicación

A medida que los datos están disponibles para Paygilant por la aplicación, se utilizan con el fin de validar la identidad del usuario. Esto se realiza mediante referencias cruzadas con fuentes de datos internas y externas.

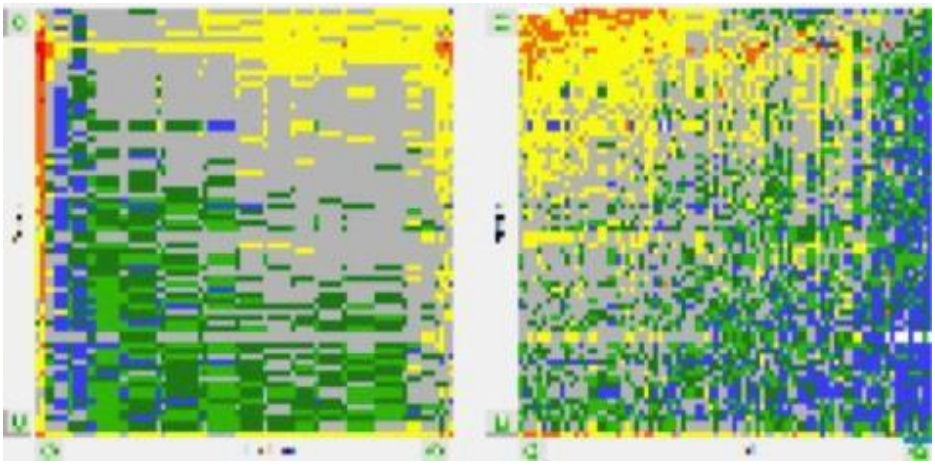
Vista de Transacciones

Paygilant emplea mapas de comportamiento de transacciones. Los mapas de comportamiento representan transacciones financieras y hábitos de compra de un cliente específico. Estos mapas se crean utilizando los algoritmos de aprendizaje patentados de Paygilant. Un mapa de comportamiento muestra una imagen clara y de alta resolución de las diferentes zonas de riesgo, y es un factor clave para determinar el riesgo de una transacción específica. El mapa tiene las siguientes características claves:

- Mapas Privados: Cada mapa es único. Este es calculado y mantenido por usuario, y por lo tanto representa un nivel de riesgo transaccional en cada transacción hecha por el usuario.

- Mapas Públicos: Cada mapa privado es comparado con el comportamiento público para determinar la distancia virtual de la transacción entre individuos y sus pares.

Mapas de Comportamiento de Paygilant



El Fraude Identificado en Cada Etapa del Viaje del Usuario

El viaje del Usuario es el proceso por el cual un usuario típico hace al realizar una transacción o proceso de pago. La trayectoria incluye los siguientes pasos:

Es el tejido preciso y la construcción acumulativa de los seis sets de inteligencia, lo que constituye la salsa secreta de Paygilant. Los conjuntos de inteligencia de Paygilant son capas dinámicas que son activadas a lo largo de las etapas del viaje del usuario.

Lanzamiento de la Aplicación (Etapa 1)

Una vez que la aplicación se ha descargado y puesto en marcha, Paygilant comienza a trabajar inmediatamente para examinar el Espacio del Usuario y el ADN del Dispositivo. Se investigan los atributos que caracterizarían un dispositivo robado o una tarjeta SIM intercambiada. La detección de Paygilant comienza desde el primer día, indicando la existencia de actividades fraudulentas, hechas tanto por humanos o usuarios no humanos como bots o emuladores. Paygilant advierte sobre potenciales amenazas desde ese mismo instante.

Registro de Usuario (Etapa 2)

La apertura de una cuenta nueva es altamente susceptible a fraudes. Durante la etapa de registro del usuario se activan el ADN del Dispositivo, Espacio del Usuario, Mapa de Actividades y Bio-Marcadores, indicando si la creación de dicha cuenta fue legítima o fraudulenta. Además, el proceso eKYC es enriquecido con la información proporcionada por Paygilant, determinando si la cuenta fue creada por un usuario auténtico

Inscripción de Tarjeta Nueva/Cuenta Bancaria (Etapa 3)

En casos donde la aplicación permite compras online, Paygilant activa el punto de chequeo de inscripción de tarjetas. La combinación de los 5 sets de Inteligencia de Paygilant indican la existencia de actividades anormales con respecto a tarjetas de crédito/débito en la aplicación. El conjunto de atributos de estos Sets de Inteligencia, proveen una evaluación de riesgo precisa y confiable.

Transacciones (Etapa 4)

La etapa de pago o transacción activa todo el arsenal de los Sets de Inteligencia, indicando si es un usuario auténtico o riesgo de fraude.

Resumen

El enfoque único de detección y prevención móvil de Paygilant integra y correlaciona múltiples Sets de Inteligencia para detectar comportamiento fraudulento, desde la etapa de lanzamiento de la aplicación hasta las transacciones en curso. Sin afectar la experiencia del usuario, Paygilant se ejecuta en segundo plano, alertando sobre la existencia de transacciones sospechosas antes que ocurran.

Paygilant tiene la habilidad de entregar análisis de datos de manera continua, reduciendo a un mínimo la necesidad de pasos extras de autenticación (claves, contraseñas, mensajes de texto, OTP, etc.). En el evento de una alta puntuación de riesgo, una alerta es activada para bloquear la transacción en tiempo real. Las puntuaciones de bajo riesgo indican con fuerte determinación a un usuario legítimo y una transacción que puede ser aprobada de manera segura.

Sobre Paygilant

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