Documentación del Proyecto: PayGuardian

Sector: Banca y Fintech

Necesidad del sector:

En la actualidad, los bancos y fintechs enfrentan un aumento en los casos de **fraude digital**, especialmente a través de dispositivos móviles. Las amenazas más comunes incluyen:

- **Suplantación de identidad (SIM Swap)**
- **Transacciones desde ubicaciones no habituales**
- **Números telefónicos temporales usados para registrar cuentas falsas**
- **Cuentas vulneradas en dispositivos en roaming**
- **Clientes no autenticados correctamente (KYC incompleto)**

Los canales móviles se han convertido en el principal blanco de fraude por ser accesibles, rápidos y, muchas veces, con mecanismos de seguridad débiles.

Solución Propuesta: PayGuardian

¿Qué es PayGuardian?

Es una **app modular de verificación antifraude**, que se puede integrar a plataformas bancarias o de pagos móviles. Usa inteligencia de red (a través de Open Gateway APIs) para detectar, prevenir y alertar sobre comportamientos sospechosos en tiempo real, durante pagos, transferencias o accesos.

Objetivo General

Desarrollar un sistema de **prevención de fraude** que proteja a los usuarios y comerciantes en transacciones móviles y pagos en línea, utilizando un conjunto de **APIs de verificación** para evaluar la legitimidad de las transacciones y la identidad del usuario, así como detectar accesos sospechosos en tiempo real.

Problemas que resuelve:

- **Fraude en pagos móviles**: Pagos no autorizados, uso de tarjetas robadas o identidad suplantada.

- **Fraude de compras en línea**: Transacciones fraudulentas realizadas con información falsa o números de teléfono temporales.

- **Uso de SIM Swap**: Fraude relacionado con la clonación de la tarjeta SIM para acceder a cuentas.

- **Accesos desde ubicaciones no confiables**: Identificar pagos o transacciones realizadas desde lugares no habituales.

Cómo funciona el sistema de prevención de fraude en pagos

El sistema de prevención de fraude será **integrado en el flujo de pagos de la plataforma** y evaluará cada transacción utilizando las **APIs disponibles**. El sistema analizará múltiples factores, como la validez del número de teléfono, cambios en la SIM, la ubicación del dispositivo, el estado del dispositivo y el perfil del usuario, para identificar patrones sospechosos.

Flujo de funcionamiento:

1. **Verificación del número de teléfono**:
   Cuando un usuario realiza una compra o pago, el sistema utiliza la **Number Verification API** para verificar si el número de teléfono es válido, activo y no pertenece a un número temporal. Esto es esencial para prevenir fraudes relacionados con números falsos o temporalmente generados.

2. **Verificación de SIM Swap**:
   Para proteger contra el fraude de **SIM swap**, el sistema consulta la **SIM Swap API** para detectar si ha habido un cambio reciente en la tarjeta SIM del teléfono. Si se detecta un cambio reciente, se activa una alerta y se solicita al usuario una verificación adicional (como un código de autenticación por SMS o una validación de identidad).

3. **Verificación de la ubicación geográfica**:
   Al realizar un pago, el sistema consulta la **Location Verification API** para verificar si la ubicación geográfica del usuario coincide con la ubicación registrada en la plataforma o el perfil. Si se detecta que el usuario está intentando realizar un pago desde una ubicación inusual o de alto riesgo (por ejemplo, otro país), el sistema puede bloquear la transacción o solicitar una validación adicional.

4. **Verificación de roaming**:
   Si el dispositivo del usuario está en **roaming internacional**, esto podría ser una señal de que la actividad es sospechosa, especialmente si el usuario no suele viajar. La **Device Roaming Status API** ayuda a verificar si el dispositivo está en roaming, lo que permite al sistema generar una alerta de posible fraude.

5. **Verificación de identidad**:
   Si la transacción es de alto riesgo (como una compra importante o transferencia de dinero), se puede utilizar la **Know Your Customer - Match API** para verificar que la identidad del usuario coincida con los registros existentes en la plataforma. Esto ayuda a prevenir fraudes como el uso de datos robados para realizar compras.

Tecnologías utilizadas

- **Carrier Billing API** – valida si se están realizando cobros vía operador.
- **Know Your Customer - Match API** – verifica la identidad del cliente.
- **Number Verification API** – valida si un número telefónico es real y activo.
- **SIM Swap API** – detecta cambios recientes de tarjeta SIM.
- **Home Devices QoD API** – revisa la calidad de conexión del dispositivo.
- **Device Roaming Status API** – identifica si el dispositivo está en roaming.
- **Location Verification API** – valida si la ubicación del dispositivo es confiable.

Casos de Uso

Caso de Uso Principal: Transacción Segura Móvil

1. **Escenario**:
   Un usuario intenta realizar una transferencia bancaria desde su app.

2. **Acciones del sistema:**

    - Verifica si el número telefónico es válido (`Number Verification API`)

- Comprueba si hubo un cambio de SIM en las últimas horas (`SIM Swap API`)
- Verifica si está en una ubicación segura (`Location Verification API`)
- Detecta si el usuario está en roaming (`Device Roaming Status API`)
- Chequea la calidad del dispositivo (`QoD API`)
- Llama a `KYC Match API` si es una operación sospechosa

3. **Resultado**:
   - Si todo es correcto: la transacción se autoriza
   - Si hay un riesgo: se bloquea, se notifica al usuario, y se pide validación adicional

Otros Casos de Uso

Caso	Qué hace
Registro de cuenta nueva	Valida el número, evita registros con SIMs recientes, solicita KYC.
Inicio de sesión desde nuevo dispositivo	Verifica ubicación, roaming y estado del dispositivo antes de permitir el acceso.
Alertas de actividad sospechosa	Notifica al usuario si hay intentos de acceso desde ubicaciones riesgosas o con SIM cambiada.

Beneficios

Stakeholder	Beneficio
Usuario	Seguridad al operar desde el móvil sin complicaciones.
Banco / Fintech	Reducción de fraudes y suplantaciones. Mejora en cumplimiento regulatorio (KYC, AML).
Operador Telco	Monetización a través de APIs de red; mejora en protección de identidad de clientes.

Etapas de desarrollo

1. **Diseño de prototipo (Figma):** Wireframes de las pantallas clave (login, dashboard, verificación, historial).

2. **Integración de APIs (backend):** Validaciones automáticas con Open Gateway.

3. **Desarrollo del frontend móvil (React Native o Flutter).**

4. **Módulo de gestión de alertas y notificaciones.**

5. **Pruebas de seguridad y comportamiento en escenarios reales.**

6. **Implementación de interfaz para bancos (dashboard web B2B opcional).**

Público objetivo

- **Bancos digitales**
- **Apps de pagos móviles / billeteras**
- **Compañías fintech que procesan pagos o prestan dinero**
- **Empresas que requieren verificación por móvil (ej. marketplaces, remesas, préstamos rápidos)**

Diferenciadores clave

Verificación **multi-factor contextual** (número + ubicación + SIM + red + roaming)
Integración directa con telcos gracias a Open Gateway
Interfaz amigable para usuarios y alertas en tiempo real
Modular: se puede integrar como SDK o API REST

Conclusión

PayGuardian responde a una necesidad real y creciente en el mundo digital: la **seguridad móvil proactiva**. Al conectar bancos y fintechs con datos directos de red, se crea una capa adicional de protección que **reduce el fraude sin afectar la experiencia del usuario.**

Sistema de Prevención de Fraude en Pagos Móviles y Compras en Línea:

Api Number Verification: Verificar el número del usuario existe o evitar registros con números temporales o de spam.
API: SIM Swap: Detecta cambios recientes en la SIM del dispositivo, lo que podría indicar un intento de fraude.
API Location Verification API: Verifica que la ubicación del dispositivo sea coherente con la ubicación habitual del usuario.
Device Roaming Status API: Detecta si el dispositivo está en roaming internacional, lo que puede ser una señal de acceso fraudulento.
Know Your Customer - Match API: Verifica que la identidad del usuario coincida con los registros de la plataforma, reduciendo el riesgo de suplantación de identidad.