Telefónica

API OVERVIEW

Overview, use cases and case studies on the Scam Signal API

Telefónica Open Gateway

20 May, 2025

Table of Contents

Description, Features, and Categorization

01

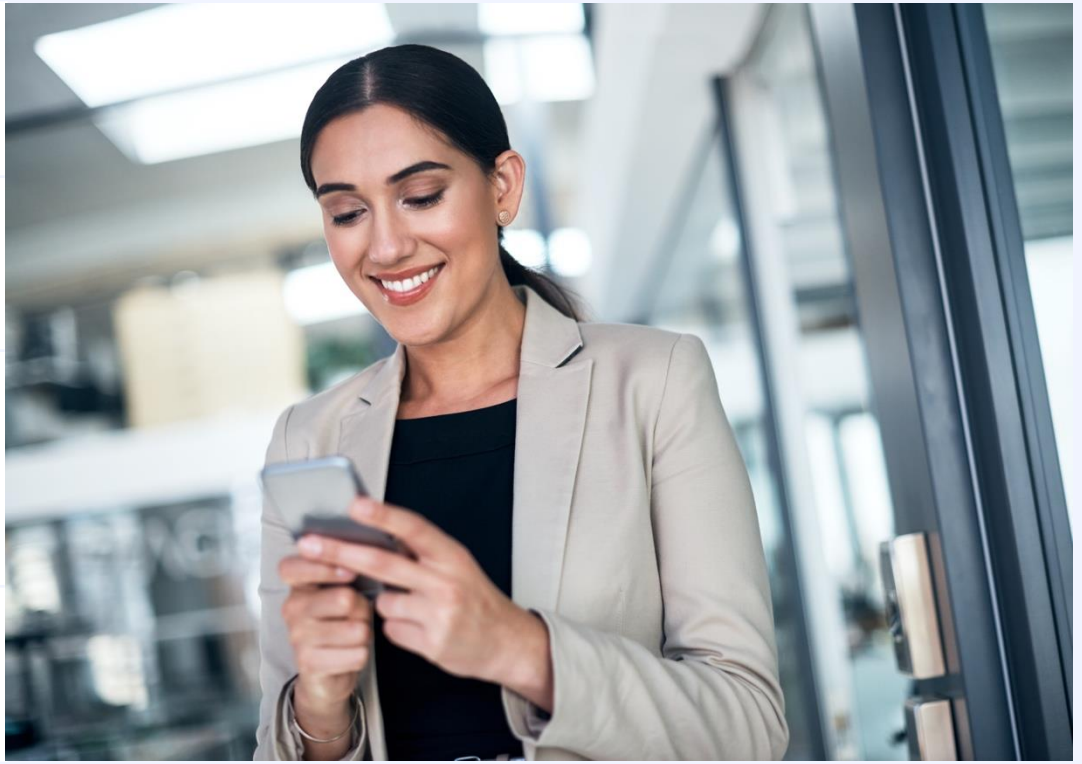
The “Scam Signal” API allows businesses to protect their customers from impersonation scams, particularly Authorized Pushed Payment (APP) fraud

Authorized Push Payment fraud occurs when a victim is tricked into transferring money to a fraudster, often through impersonation of banks, government agencies, family members, or via scams involving fake investments, counterfeit goods, or deceptive relationships.

NOTE: The Scam Signal API is not available on CAMARA. *The Scam Signal API was developed following CAMARA standards within the GSMA OPAG framework. To preserve its effectiveness, the API is hosted in a private GSMA repository, with access strictly controlled by GSMA. Access requests must be directed to the appropriate GSMA contact.*

Features and Categorization

CAMARA	✓
COUNTRIES	
SECTORS	BANKING & FINANCIAL SERVICES SECURITY AND FRAUD PREVENTION
SERVICES	ANTI-FRAUD



Characteristics of Scam Signal

02

Overview

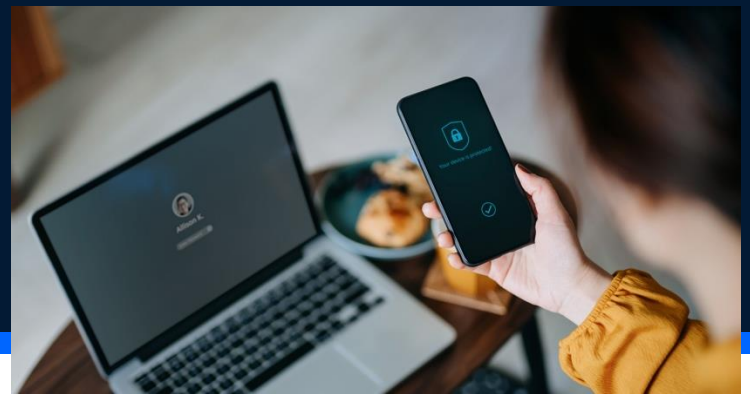
Characteristics of one standard Scam Signal API

Proven Field Results with High Impact

Early deployments (e.g. UK banks) report up to **41% reduction in live scams**, **44% fewer fraud losses**, and rapid customer protection at scale — validating the API's business value.

Enhances Fraud Risk Scoring Engines

Adds telecom intelligence to existing fraud models, improving detection accuracy and **reducing false positives (up to 55%)**, leading to better operational efficiency.

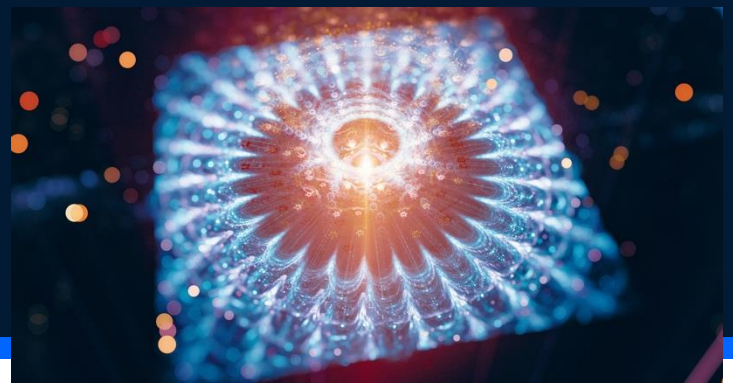


Supports Real-Time Intervention and Customer Protection

Empowers organizations to **interrupt fraud in progress** — enabling dynamic actions like pausing suspicious transactions, triggering alerts, or redirecting users to secure verification flows.

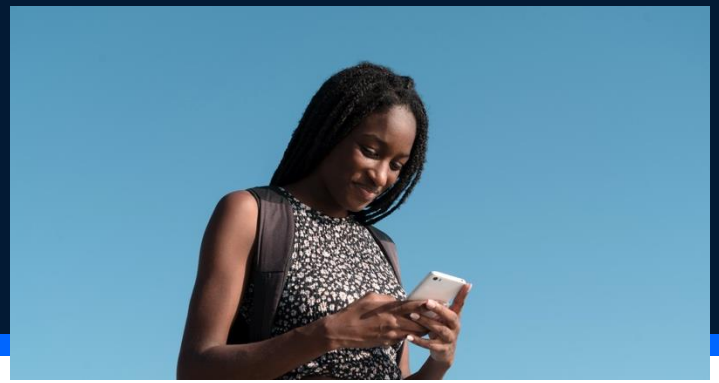
Overview

Characteristics of Scam Signal



Real-Time net. signals Context Awareness

Leverages advanced analysis of real-time network data to instantly enable fraud systems be informed about APP fraud indicators at the time of a transaction — a key indicator of social engineering scams like APP fraud.



Privacy-Preserving Signal Analysis

Verifies only network metadata— not content or counterpart details — ensuring compliance with privacy regulations and customer trust.

Cross-Industry Collaboration

Developed jointly by telecom operators and banks under GSMA Open Gateway, leveraging telco insights to enhance banking fraud detection with minimal integration effort.

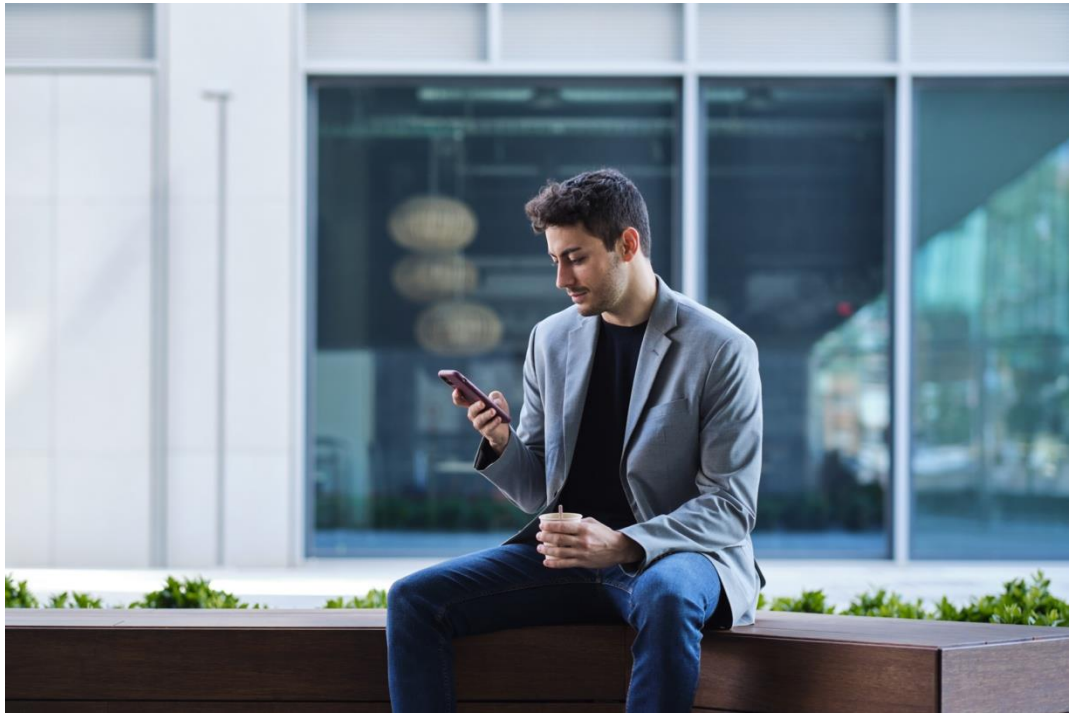
Use cases

03

Overview / Use Cases

Retail Banking – Real-Time Payment Scam Prevention

A customer attempting a high-value or unusual bank transfer can be protected by Scam Signal in real time. When the transaction is initiated, the bank's fraud system calls the API to check for concurrent network activity .The payment can be paused and the customer prompted with a warning or redirected to additional verification. This use case has already proven its worth – participating UK banks have intercepted ongoing scams through such real-time checks, **contributing to a reported 41% reduction in scams in progress during trials**



OTHER RELATED APIs

SIM Swap
Device Swap
Number Verification
Device Location

SECTOR	BANKING & FINANCIAL SERVICES
SERVICE	ANTI-FRAUD

RETAIL BANK NEEDS

- **Detect social engineering scams at the exact moment a payment is initiated**, especially when the customer may be unknowingly manipulated during a live interaction.
- **Access real-time contextual signals beyond traditional fraud indicators**, such as whether the customer is currently on a suspicious situation— a previously invisible risk factor.
- **Prevent fraudulent transactions before completion**, by enabling dynamic decisioning (pause, verify, or block) based on telecom network insights that enhance fraud detection accuracy.

Overview / Use Cases

Corporate and Small Business Fraud Prevention

APP fraud isn’t limited to retail banking – businesses are also targeted (e.g. CEO fraud, vendor impersonation scams). Scam Signal can be extended to corporate banking scenarios. For example, when a company’s finance officer is setting up an urgent wire transfer (perhaps due to a supposed directive from the CEO received via email or phone), the bank’s portal could use Scam Signal to detect if that officer’s phone has scam signals. If yes, it might suggest a “call-back verification” step before releasing funds. In another scenario, a small business owner might get a call from someone posing as a supplier or even a government authority demanding immediate payment; a fintech app or bank could catch it via Scam Signal.

OTHER RELATED APIs

SIM Swap
Device Swap
Number Verification

SECTOR	BANKING & FINANCIAL SERVICES
SERVICE	ANTI-FRAUD

CORPORATE NEEDS

- **Identify if financial staff are under real-time social engineering pressure**, by checking if they are currently on a network signal during sensitive payment operations.
- **Introduce secure verification workflows for business-critical transactions**, such as call-back steps or multi-channel authentication, when scam-like patterns are detected via network signals.

Start using SCAM SIGNAL API!

04

Getting Started with Scam Signal API

Harness the power of Open Gateway and seamlessly integrate our API services into your app

Follow these initial steps for seamless API services to Developers within Channel Partners' environments, including Operators API Services integration for a cohesive product experience and efficient collaboration among stakeholders.

1 CHOOSE A CHANNEL PARTNER

Select a suitable channel partner or payment aggregator that offers integration with the Open Gateway API to meet your needs and business goals. Contact an expert to get more information about the channel partners availability or to become a new Open Gateway Partner

2 PRODUCT DISCOVERY

You can access the Open Scam Signal through the Channel Partner's developer portal.

3 DEVELOPER REGISTRATION

To use Open Gateway Products, you must undergo a registration process that includes signing up on both the Channel Partner and Operator platforms.

4 SCAM SIGNALAPI CONSUMPTION

After subscribing and sharing credentials, You can access the Open Gateway Product on registered Operators, making API calls through the Channel Partner's gateway.

5 PRIVACY MANAGEMENT

Some Open Gateway Products require end user consent for Developers to access Operator's network capabilities on their behalf.

FAQs

05

Scam Signal API / FAQs

How does the API detect a potential scam?

A client may query the API when a money transaction appears suspicious. The API will inform about different indicators leveraging advanced analysis of real-time network data to identify and prevent APP fraud activities.

What network signals does Scam Signal analyse to help detect potential fraud?

Scam Signal leverages advanced analysis of real-time network data that is strictly processed in full compliance with the GDPR and other applicable privacy regulations. Due to the nature of the social engineering fraud, we do not publicly disclose the risk signal types.

If you're interested in exploring this further, we encourage you to reach out via the partner contact form on our website. We would be happy to schedule a dedicated session to share more details under the appropriate confidentiality and security framework.

What kind of organizations can benefit from using Scam Signal?

Primarily banks, fintechs, and payment providers. Any organization seeking to reduce social engineering fraud (like APP scams) can use this API to improve detection and intervene in real time.

Is integration with Scam Signal complex?

No. Scam Signal is delivered as a standardized RESTful API via GSMA Open Gateway, with consistent implementation across telecom networks. Most institutions can integrate it within existing fraud platforms or decisioning engines with minimal effort.

Does Scam Signal replace other fraud detection tools?

No. It's designed to complement existing tools such as SIM Swap detection, KYC Match, location verification and behavioural analytics. It adds unique telecom-layer insight that enriches fraud models and increases their accuracy.

Are there proven results from early adopters?

Yes. In the UK, participating banks have reported up to 41% reduction in scams in progress, 44% drop in fraud losses, and 55% fewer false positives after implementing Scam Signal.

Other relevant information

06

Discover more

Join our Developer Hub

Join the **Telefónica Open Gateway Developer Hub** to test our APIs, develop use cases with the power of the network and improve user experiences.

Enroll our Partner Program

If you are interested in the potential of Telefónica Open Gateway and you are willing to collaborate with us, you can **enroll our exclusive Partner Program**.

Subscribe our newsletter

Find out all about the latest of Telefónica Open Gateway in our **newsletter**.

Contact our experts

If you have any questions about the initiative, don't hesitate to **contact our experts**.

Telefónica

opengateway.telefonica.com