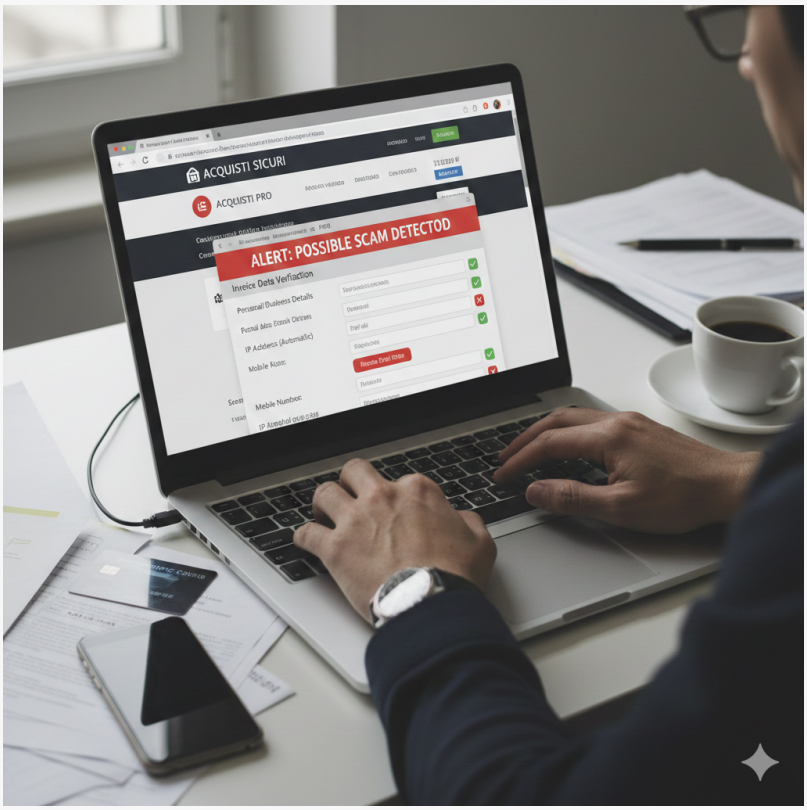
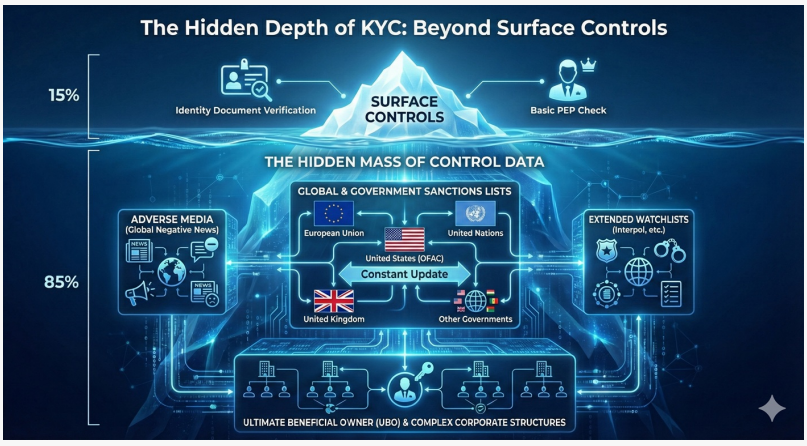
Digital Fraud in E-commerce: How Openapi.com Trust Score APIs are mitigating online threats at the source

No longer just reacting, but predicting. As cybercrime evolves, companies are adopting "silent screening" systems.

ENGLEWOOD CLIFFS, NJ, UNITED STATES, December 24, 2025 /EINPresswire.com/ -- Modern fraudsters are data craftsmen: they blend real information with synthetic traces. But if the phone number they use is an anonymous VoIP line or appears as 'leaked' on the dark web, the probability that the card is stolen nears 90%." These are the words of Alan Andrews, a Risk Manager on the front lines of cybersecurity, and they explain why old "reactive" defenses are no longer enough.



openapi trust



KYC API

While public debate often focuses on swindled consumers, there is a less explored gray area: the plight of the merchant. In 2025, e-commerce fraud based on identity theft has grown by double digits. This is the so-called "Card Not Present (CNP) Fraud," every online seller's nightmare. When a stolen card is used on a site, it isn't the bank that loses out—it's the website owner, who is forced to refund the amount and pay heavy penalties.

The Damage Multiplier: Why One Stolen Euro Costs Nearly Five

The data is clear: according to the True Cost of Fraud Study 2024-2025, for every euro lost in a fraudulent transaction, a merchant spends an average of €4.61. During our analysis, we broke

> Fraudsters create profiles by blending real and fake data. If a phone number is an anonymous VoIP line or appears as 'leaked' on the dark web, the probability that the card is stolen nears 90%”
>
> *Alan Andrews (Risk Manager)*

down the factors of this multiplier: it ranges from the loss of shipped goods and logistics costs to heavy "chargeback" fees (which can reach €50 per operation) and the staff time required to manage disputes.

Key statistics for 2024-2025 highlight the scale of the crisis:

- Global e-commerce losses have hit $44 billion.
- European merchants lose an average of 2.8% of their annual turnover to fraud.
- "Friendly Fraud" (real customers pretending they never received a package) now accounts for over half of all disputes.
- Despite this, only 16% of merchants perform preventive screening before payment.

The Liability Paradox: Who Doesn’t Check, Pays
In Europe, PSD2 regulations are strict. If a site fails to correctly implement Strong Customer Authentication (SCA), the financial liability for theft rests 100% on the merchant. But it gets worse: exceeding a 1% chargeback rate can lead networks like Visa and Mastercard to place the company into monitoring programs, with the very real risk of having payment processing suspended entirely.

Our Test: The "Reliability Profile" by OpenAPI.com
To understand how to stem this tide, we analyzed and tested the TRUST services by OpenAPI.com. The real story is no longer the attack itself, but the capacity for preventive defense through APIs (Application Programming Interfaces).

These digital connectors allow business systems to query global databases instantly. During our hands-on trial, we inputted typical transaction data—emails, IPs, and mobile numbers—receiving an incredibly detailed "reliability profile" in just a few milliseconds.

We focused specifically on Mobile Verification as a true "digital fingerprint" of risk. This is not a simple format check; it is an HLR (Home Location Register) Lookup that digs deep into global telecom networks. By using the POST /mobile-advanced request on the OpenAPI platform, we obtained over 25 critical parameters.

Key findings from our tests included:

The Fraud Score: A dynamic rating that immediately flags if a user is high-risk.

Line Status: Knowing if a SIM is active or if the phone is currently off allows merchants to nip "account takeover" attempts in the bud.

The "Leaked" Effect: OpenAPI signals if a number is present in breached databases (such as those from giants like Amazon or Google). A "leaked" number is a red flag: it is highly likely to be in the hands of a malicious actor who purchased it on the dark web.

VoIP and Carrier Analysis: The API identifies if the number is an anonymous virtual line, a common tool for fraudsters looking to hide their identity.

Creating "Intelligent" Sales Processes
Adopting these systems—which are fully GDPR-compliant based on the "legitimate interest" of the business—allows merchants to transition to "intelligent selling." If OpenAPI's system detects high risk, the company can block the operation at the source (saving the chargeback cost) or request supplemental verification, such as a Know Your Customer (KYC) identity check.

The TRUST channel by OpenAPI doesn't stop at mobile phones; it integrates Business Information, Sanction List checks (AML), and KYB (Know Your Business) data. In a world where crime is automated, the response must be equally high-tech. Integrating these services is now the dividing line between a vulnerable business and one ready to scale the global market in total security.

Luca Scuriatti
Openapi Spa
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
