



Meet The Speakers



**Balázs Péter
Hámornik PhD**

Senior AI/ML Product
Manager, SEON

Matyas Varga

Head of Global Fraud
Services, SEON



Agenda

01	Intros / Fraud Challenges	12:30 - 12:35
----	---------------------------	---------------

02	Presentation	12:35 - 12:55
----	--------------	---------------

Case Study: Two threats, One platform
Key Takeaways for Travel Fraud Teams
Adapting to Threats at the Speed of AI

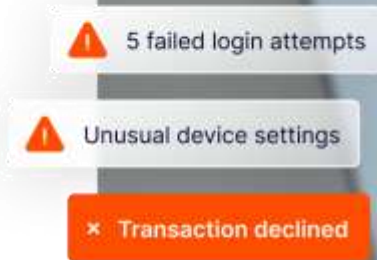
03	Q&A / Wrap Up	12:55 - 13:00
----	---------------	---------------



Case Study

Two Threats, One Platform

How a Travel Management Platform
Stopped ATO and Stolen Card Fraud



GAFPG Madrid 2026

Case Study

A Travel Management Platform Hit by Two Fraud Schemes at Once



A **free-to-use B2B travel management platform** serving corporate organizations, SMBs, and government clients - managing bookings and travel logistics at scale.

Sector:

Travel management (B2B)

Users:

Corporations, SMBs, government & military

Situation:

Two simultaneous fraud schemes: one pre-existing, one emerging

SEON:

Real-time scoring at login and booking events

Consultancy:

Utilized SEON's **Managed Risk Services**, working closely with a dedicated senior fraud consultant

Two Simultaneous Schemes

	Account Takeover (ATO)	Stolen Card Fraud
Method	Phishing emails + fake SEO-ranked site harvesting credentials; session hijacking	Freshly registered accounts + stolen cards used for bookings
Motive	"Launder" bookings via compromised partner accounts	Self-use - fraudster personally staying at booked locations
Profile	Organized, resourced operation Sophisticated	Single repeat actor, New York-based Persistent



Case Study - Threat Profile 1

Account Takeover (ATO)

The Scheme

Fraudsters harvested credentials at scale using phishing emails and a **fake website ranked high in search results**.

They hijacked active sessions, logging in from their own devices immediately after user authentication. Finally, they routed fraudulent bookings through compromised partner accounts to extract funds.

The Complication: Military Context

Context is crucial. **Military** customers routinely **mask** their **device details** for security reasons. macOS-specific spoofing was the signal that cut through the noise without affecting legitimate users.

Key Detection Signals

1. `paste_used`

Credentials pasted - not typed/autofilled - indicating automated credential stuffing

2. `fake_os` Flag

Device intelligence revealed OS spoofing (specifically macOS)

3. Velocity & Device Switching

Rapid switching between different devices within the same user session



Stolen Card Fraud

The Scheme

A single repeat actor based in New York systematically exploited the platform using **freshly registered accounts** and **stolen credit cards** for bookings.

Unlike the ATO ring, this was partially **self-use fraud**. The fraudster was personally staying at the booked locations in some cases, making the activity highly localized but frequent.

The Challenge

Because the actor used fresh accounts and new cards each time, traditional basic blocklists were ineffective.

Key Detection Signals

1. Velocity Logic

Matching device details to identified fraudulent booking events and referencing registration-to-booking velocity

2. Location signals

Targeting specific high-risk ZIP codes associated with the actor's pattern

3. ML-Surfaced Correlations

SEON's Machine Learning model automatically identified a hidden correlation among affiliate ID values, providing a high-confidence signal to block the actor's new accounts



The Solution

How Prevention Worked: Labeling as the Foundation

The Power of State Labeling

By consistently **labeling transactions/events** according to the **fraud vectors**, the platform created a closed feedback loop. This allowed the system to automatically recognize patterns across seemingly unconnected events.

1. Feedback Loops

Labeling enabled the system to track shared attributes across multiple accounts. If one account was flagged, others sharing the same **device, IP subnet, or browser profile** were automatically elevated in risk.

Key Mechanism

Velocity & Link Analysis

2. Machine Learning Insights

The Whitebox ML model analyzed the labeled data and surfaced unexpected correlations that human analysts missed, such as the strong link between fraud and specific **affiliate IDs**.

Key Mechanism

Automated Feature Discovery

3. Context-Aware Rules

Rules were tuned to the client's specific user base. For example, military users' spoofed devices appeared with Windows OS only, so rules were adjusted to **prevent false positives** for legitimate government travel.

Key Mechanism

Custom Rule Tuning



Key Takeaways for Travel Fraud Teams

1



Contextualize Your Rules

Generic rules fail in travel. You must build logic that accounts for your **specific customer base** (e.g., military personnel vs. standard corporate travelers) to avoid blocking legitimate high-value bookings.

2



Labeling is the Foundation

Without accurate transaction labeling, you are flying blind. Setting up **structured feedback loops** is what allows you to effectively use available information and understand behaviors across seemingly unrelated accounts.

3



Let ML Find the Hidden Links

Human analysts can't spot every pattern. Machine Learning excels at surfacing **unexpected correlations** (like the affiliate ID link in the stolen card scheme) that manual reviews may miss.



Adapting to Threats at the Speed of AI

Natural Language Rule Builder

Analysts can describe detection logic in **plain English**, and the AI automatically generates complex rules and filters. No technical coding knowledge required.

The Impact

Eliminates lengthy testing cycles and technical back-and-forth, allowing teams to adapt to new fraud patterns in minutes.

AI Investigation Summaries

Generates clear, bullet-point explanations of each alert and transaction, turning **complex digital fingerprints** into concise narratives that explain why activity was flagged.

The Impact

Provides instant context for analysts, drastically reducing manual review time and accelerating decision-making.



Explainable AI for Fraud Teams

Similarity Ranking →

Automatically links and ranks connected users through **shared devices, behaviors, IPs, and contacts**.

Benefit

Analysts can skip manual graph-building and instantly focus on top-priority fraud rings.

Risk Signals →

Color-coded indicators surface high, medium, and low-risk activity across **email, phone, device, OS, and IP data**.

Benefit

Spot the most critical triggers at a glance, reducing manual review time by up to 50%.

Explainable AI Scoring →

Provides complete visibility into what drives the risk score, including **individual signal contributions**.

Benefit

No black boxes. Clear decision rationale supports both analyst confidence and regulatory requirements.



Proactive Fraud Ring Detection

When you can see the full picture instantly

Automatically identify hidden relationships to dismantle fraud and money laundering rings before they impact your business.

Move from reactive fire-fighting to proactive prevention

Identify emerging threats and mitigate risk before significant losses occur

Continuously analyze your customers to detect threats of suspicious activity

Customize detection to fit your business by choosing the signals that matter the most

Search and filter detected networks to cut triage time

