GSMA

October 2025

Apate.ai use case: AI-Powered Scam Detection, Diversion and Real-Time Threat Intelligence

Apate.ai use case:

AI-Powered Scam Detection, Diversion and Real-Time Threat Intelligence

Scam calls are one of the most pressing and costly challenges for telecom operators, with organised crime networks exploiting voice channels to impersonate trusted brands, deceive customers, and steal funds. Globally these scams cause billions of dollars in losses each year and erode public trust in communications services, however the data around scam operations is still opaque. Traditional measures such as blacklists and reactive blocking struggle to keep pace as scammers rapidly adapt their tactics, rotate numbers, and use increasingly sophisticated social engineering. *As a result, TPG wanted a solution that could proactively identify and divert scam calls before they reached customers, while also collecting intelligence to adapt to new scam tactics faster than criminals could evolve them.*

Solution:

TPG Telecom partnered with Apate.ai to pilot a proactive, intelligence-driven defence against scam calls. The program was designed not just to block malicious calls, but to divert them into a secure environment where valuable threat data could be gathered and used to strengthen protections – with the intention of protecting customers in real time, gaining actionable intelligence on evolving threats, and building an approach that could be replicated across the industry.

Key elements of the approach included:

- **Scam diversion and containment** – High-risk calls were diverted to intelligent, multi-lingual AI-powered bots that convincingly emulate real people. This kept scammers engaged for extended periods (up to 54 minutes), wasting their time and resources so that they couldn't engage with real customers.
- **Comprehensive threat intelligence gathering** – Each interaction was analysed to identify impersonated brands, scammer scripts, financial artefacts (such as bank accounts and cryptocurrency wallets), behavioural patterns, and peak periods of activity.
- **Rapid false positive management** – A "false positive escape" process ensured any legitimate calls misclassified as scams were restored in under 20 seconds, maintaining customer experience.
- **Continuous feedback loop** – Insights from the diverted calls were fed back into TPG's network defences, enabling refinement of scam detection rules and improving future blocking accuracy.after, we also began alerting customers about suspicious international calls.

Impact

The collaboration delivered on its goal of significantly reducing scam exposure while generating industry-leading threat intelligence:

- **280,000+ scam calls** successfully diverted from the TPG Telecom network.
- **100+ days** of scammer time wasted.
- **$7.6 million+ in estimated scam losses prevented** (based on National Anti-Scam Centre methodology).
- **98%** scam traffic detection accuracy.
- **20,000+ impersonated organisations** identified including major banks, government agencies, and telcos.
- **First-of-its-kind insight** into scammer tactics, techniques, and procedures (TTPs), feeding into broader fraud prevention strategies.

Additional information

Cost: **Low**: Leveraged Apate's existing platform with light-touch integration and minimal infrastructure uplift for TPG Telecom.

Participating organisations: tpg TELECOM | Apate

Location: Asia Pacific

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom
www.gsma.com