AVIATION · BRAND PROTECTION · MANAGED EXTERNAL THREAT INTELLIGENCE (M/ETI) · TAKEDOWN

The Site They Didn't Know Existed:

How Banyax Detected, Documented, and Took Down an Active Brand Impersonation in 8 Days

How Banyax turns fragmented brand monitoring into a board-ready external exposure governance program with measurable KRI reduction, forensic evidence automation, and structural client retention.

INDUSTRY Aviation / Passenger Air Transport (Low-Cost Carrier) · Mexico

01 · WHAT CLIENTS ACHIEVE

Four measurable outcomes from a single engagement that changed how the airline governs its external brand exposure.

Takedown Speed	Prior Visibility	Active Threat	Scope Expansion
8 days	**Zero**	**Live form**	**+Ongoing**
from detection to domain deactivation	*client had no knowledge the site existed*	*functional data-capture form at time of detection*	*continuous brand monitoring activated post-incident*

Before Banyax, the airline's security team had no continuous monitoring for brand impersonation. Exposure was discovered reactively — only after customers reported suspicious sites. The gap between a fraudulent domain going live and the team's awareness of it was measured in weeks, not hours.

After Banyax, the team knew about an active fraudulent site before any internal process detected it. They had documented evidence to act, a structured takedown process, and a continuous monitoring layer that reduced future exposure. The conversation changed from 'we react when users complain' to 'we govern our external brand surface proactively.'

02 · THE PROBLEM NO ONE WAS SOLVING

The airline's security team was not facing a technical gap — it was facing a governance gap. External brand exposure was growing in real time, and the organization had no mechanism to detect it, measure it, or act on it before customers were affected.

No early detection, only late reaction

The team depended on isolated findings, delayed reports, and manual reviews. By the time a fraudulent site was identified, it had been live long enough to capture customer traffic and erode brand trust. There was no systematic way to know what was happening outside the organization's perimeter.

The gap between creation and awareness

The critical window — between a fraudulent domain going live and the airline's security team becoming aware of it — was the period of maximum risk. During that window, the site was indexed, reachable by customers, and actively impersonating the brand with no countermeasure in place.

No structured takedown process

Even when a fraudulent site was discovered, the airline lacked a structured process to document the threat, build the evidence package required for takedown requests, and coordinate the deactivation. Response was ad hoc, slow, and resource-intensive.

What accelerated the decision

There was no regulatory pressure or pending audit. What made the decision urgent was simpler and more concrete: customers were already being affected. A fraudulent site was live, functional, and using the airline's visual identity and commercial elements to appear legitimate. The risk wasn't theoretical. It was already happening.

03 · THREE CORRELATED CAPABILITIES — ONE GOVERNANCE PROGRAM

Banyax did not deploy generic brand monitoring. The engagement was structured around a detection-to-takedown process built specifically for the airline's brand exposure context — visual identity, promotional patterns, and the customer experience that makes impersonation credible in aviation. Banyax Quest, our proprietary platform, orchestrates all three capabilities. AI-led: AI processes the volume, human analysts validate every escalation.

The moment that changed the conversation

Banyax identified a fraudulent domain the airline's internal team had no knowledge of. The site was not just registered — it was fully active, with a functional data-capture form designed to impersonate the airline's booking experience. The client had no idea it existed. When the finding was presented with documented evidence, the response was immediate: this was not a theoretical risk. A real threat was live and affecting real customers.

Detect

AI-led correlation of brand signals — domain similarity, visible content, source code elements, and visual identity markers — to prioritize genuine impersonation threats from thousands of potential matches.

AI-led role: *Filter volume and score risk at a scale no manual review can sustain. Analysts validate context and confirm genuine threat.*

Document

Structured evidence package built for each confirmed threat: screenshots, source code analysis, active form confirmation, and timeline of the site's activity. Evidence is formatted for takedown requests and internal escalation.

Vertical context: *The impersonation replicated the airline's expected customer experience — promotions, visual identity, and booking flow.*

Take down

Coordinated takedown process from detection to domain deactivation: 8 days for the primary domain. After resolution, monitoring was expanded to cover related domains and reduce time-to-detection for future incidents.

Expansion: *The single incident revealed a broader pattern. Continuous monitoring was activated — the engagement moved from incident response to ongoing brand governance.*

04 · HOW THE SERVICE OPERATES

From signal detection to evidence-ready takedown in five steps — all orchestrated through Banyax Quest.

1	2	3	4	5
DETECT	**SCORE**	**DOCUMENT**	**TAKE DOWN**	**GOVERN**
AI-led brand signal correlation	*Risk prioritization vs. false positives*	*Evidence package for takedown request*	*Domain deactivation coordinated by Banyax*	*Continuous monitoring activated post-incident*

05 · WHY BANYAX — THE STRUCTURAL MOAT

Four differentiators that create governance dependency, not contract dependency.

- **Governance dependency, not vendor dependency.**
  The first incident proved that external brand exposure was real, ongoing, and invisible without dedicated monitoring. Once that visibility existed, the conversation changed permanently. Discontinuing Banyax means returning to the reactive posture that allowed an active phishing site to operate undetected for weeks.

- **Aviation-context detection, not generic brand monitoring.**
  The impersonation was credible because it replicated the airline's expected customer experience — promotions, visual identity, and booking flow. Banyax's detection is built for that specificity. Generic domain monitoring would not have surfaced this threat at the right priority level.

- **AI-led at scale, human-validated at every escalation.**
  Thousands of potential brand signals are processed continuously. AI filters and scores risk; human analysts from Banyax validate context before any escalation reaches the client. The client sees qualified threats, not noise.

- **Managed service — zero internal team required.**
  The client buys outcomes: detection, documentation, evidence packages, and takedown coordination — all under contractual SLA. No licenses, no tools, no internal headcount required to operate the brand monitoring layer.

06 · OUTCOMES — BEFORE AND AFTER

Before

No continuous external monitoring. Threats discovered reactively, only after customers reported problems. No structured takedown process. The team invested significant time in manual research to confirm whether a site was real or fraudulent.

Avoided cost

The fraudulent site exploited customer trust in a promotional context — the highest-risk surface for an airline brand. Had it remained active: credential theft, financial fraud, and sustained reputational damage. Banyax contained it before any of those scenarios escalated.

After

Active threat detected before internal team was aware. Documented evidence package delivered. Domain taken down in 8 days. Security and brand teams freed from manual research. Continuous monitoring activated — future exposure reduced through proactive detection.

Team efficiency

The airline's security and brand reputation teams stopped investing time in reactive manual searches. Banyax centralized detection, validation, and evidence preparation — allowing internal teams to focus on decisions and follow-through rather than investigation.

INVESTOR SIGNALS

Retention Active — scope expanded post-incident

Expansion Single incident → continuous monitoring program

NPS signal Team acknowledged value of proactive detection

Risk profile Aviation brand exposure = board-level incident category

Governance CISO + brand team now report on external exposure

"The risk wasn't theoretical. The site was already online — with a working form — and we didn't know it existed."

— Security & Brand Protection Lead, Major Mexican Low-Cost Airline

That is what investors should underwrite — not the contract length, but the governance dependency.

07 · IDEAL CLIENT PROFILE

Airlines, low-cost carriers, and aviation operators with strong brand recognition and frequent promotional activity in digital channels — particularly those that have experienced brand impersonation incidents, are under regulatory or reputational pressure, or operate in environments where a fraudulent booking site could trigger passenger fraud at scale.

08 · LEARN MORE & CONTACT

Learn more about Banyax M/ETI (Managed External Threat Intelligence)

Discover how Banyax's Managed External Threat Intelligence (M/ETI) service continuously monitors your brand's external exposure — detecting impersonation, fraud sites, and credential threats before your customers are affected.

Visit: banyax.com

Want to learn more?

If this document was forwarded to you and you'd like to explore how Banyax can help protect your brand's external surface — reach out directly.

Email: marketing@banyax.com

Website: banyax.com