VISA

The next step in payment security:

How airlines can get ahead of fraudsters

Cora Constantin
Europe Tech and Risk Advisory at Visa

Foreword

In today's interconnected travel ecosystem, opportunity, risk, and resilience coexist in equal measure. The rapid evolution of digital payments, complex supply chains, and global mobility has brought unprecedented convenience to businesses and travelers alike. Yet, it has also created new opportunities for fraud, financial crime, and operational disruption. Building resilience into every layer of the value chain is paramount.

At Visa, we understand that **trust is the currency** upon which the travel industry thrives. Every transaction, every booking, and every journey depends on the assurance that payments are secure, data is protected, and risks are managed proactively. The stakes are higher than ever and the challenges more dynamic.

Our commitment is clear: we support our clients and partners as they navigate this increasingly complex landscape with security and resilience by design. Through advanced analytics, real-time fraud detection, and AI-driven risk intelligence, Visa helps organizations to stay one step ahead of fraudsters. We **invest relentlessly in innovation and operational resilience**, ensuring our tools not only respond to threats, but anticipate them—enabling our partners to protect their operations, safeguard revenues, and deliver seamless travel experiences.

This whitepaper reflects our shared mission: to equip B2B travel providers with the insights, strategies and products needed to thrive in an environment where security, speed, and adaptability are paramount.

Travel is ultimately about connection: bridging distances, cultures, and opportunities. Together, we can ensure that those connections remain secure, resilient, and future-ready.

Introduction

Europe's airline industry is growing fast, with sales up by 11.8% year-on-year. Yet this growth brings more opportunity for fraud; and fraud is becoming increasingly sophisticated, targeted, and scaled.[1]

Airlines and travel organizations wanting to stay protected need resilient, adaptive strategies that don't compromise on security controls, let alone the customer experience. Their approach must strike the perfect balance between friction, speed and convenience - but how?

The airline fraud landscape today

As total sales are on an upward trend (on a YoY basis), the airline industry's fraud volumes have concurrently risen to $77.7 million for the year ending in March 2025.[1] Encouragingly, the overall fraud rate* has dropped by 2.9% to single-digit levels.[1]

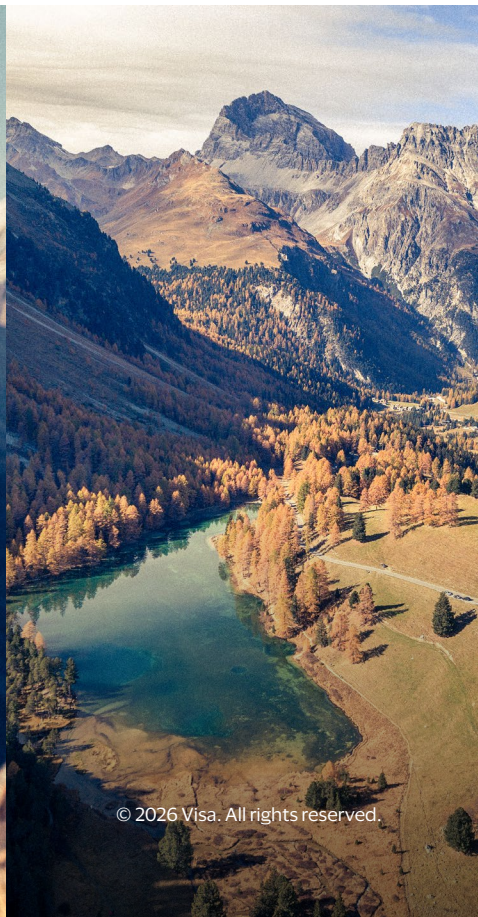
What the averages don't show, however, is the changing nature of fraud that airlines face: increasingly cross-border, more concentrated, and more targeted. Today, fraudsters leverage a variety of methods, notably:

- **CNP (Card Not Present) fraud in ticketing.**
  Accounting for 99% of fraud share, ecommerce is the dominant environment for airline fraud; fraudsters use stolen card details to purchase airline tickets; these are often obtained through social engineering campaigns, data breaches or purchased on the dark web.[2]
- **Account takeover.**
  Using means such as credential stuffing attacks, enumeration, exploitation of dormant accounts, social engineering, and brute force attacks, fraudsters gain access to customer accounts and make non-monetary changes to accounts/profiles, cancel bookings for cash vouchers, etc.
- **Data extraction.**
  Criminals harvest data through techniques such as card testing, fictitious booking and enumeration—reverse engineering response codes to determine valid credentials. These are used in subsequent attacks.
- **Triangulation fraud.**
  Fraudsters act as middleman by setting up fake travel sites with cheap fares/promotional deals. A customer buys a ticket, paying the fraudster. The fraudster then uses someone else's stolen credit card to purchase a legitimate ticket for the customer (from the genuine airline). The traveler has their flight booking, but the airline is left to deal with the fraudulent transaction and an eventual chargeback.

* Fraud rate is expressed in basis points and defined as the fraud volume divided by the sales volume over a given timeframe.
[1] VisaNet MIS Fraud Insights. Study commissioned by Visa Inc. Analysis timeframe: Apr 2024 – Mar 2025.
[2] Visa data for airlines segment. Over a one-year analysis (2024 Q2-2025Q1) CNP fraud is $77.07m and CP fraud is 0.72m. That's just 99% of fraud share (99.07%) for CNP Tx.

- **Insider threat and partner vulnerabilities.** Fraud isn't just an external threat. Employees, vendors, or third-party staff can abuse their system access; attackers increasingly exploit weak partner system controls to gain unauthorized access.
- **Synthetic ID and mule accounts.** Fraudsters combine real and fake identity information, creating synthetic identities that they use to open accounts and abuse buy-now-pay-later schemes, or other instalment offers. Alternatively, criminals use networks of 'mule' accounts (fake profiles) to launder stolen travel benefits or transfer fraudulent money while protecting their identity.
- **Friendly fraud/chargeback abuse.** An emerging concern for merchants, where consumers dispute legitimate transactions, usually after they have received the service. While this is considered a form of chargeback abuse (in Visa's terms fraud is tied to unauthorized use of a payment credential), it still leaves airlines out of pocket.

Fraud rates may be dropping, but the sophistication and complexity of the activity happening today leaves airlines needing to be even more vigilant when protecting customers. And this protection needs to cover both domestic and international transactions (intra-regional, inter-regional).



Mapping high risk fraud corridors

The expansion of airline sales across international borders is elevating the industry's exposure to fraud. While intra-regional fraud rates sit at 5.9 basis points**, the inter-regional fraud rate has reached 24.4 basis points, driving 40-50% of total airline fraud.[3] Then there's significant risk concentration of cross-border transactions; 47% of Europe's airline sales are now cross-border, and these contribute to ~65% of fraud share.[4]

It's important to understand what the higher-risk cross border transactions are. 75% of cross-border fraud involves an issuer from outside of Europe, meaning the majority of airline fraud is driven by international transactions across a small number of high-risk corridors.[4]

When it comes to cross-border fraud share, intra-European transactions account for 25% of the airline cross-border fraud share, with a fraud rate of 2.3 basis points. Comparatively, inter-regional transactions represent 75% of the airline cross-border fraud share, with a more elevated blended fraud rate of 15.1 basis points. The breakdown of issuing region contribution to European airline merchants highlights uneven risk profiles:[4]

North America
- Fraud share: **51%**
- Fraud rate: **20** basis points for USA cardholders and **16.9** basis points for Canadian cardholders

Latin America
- Fraud share: **13%**
- Fraud rate: **23.7** basis points

Asia Pacific
- Fraud share: **8%**
- Fraud rate: **8.2** basis points

CEMEA
- Fraud share: **4%**
- Fraud rate: **4.9** basis points

With a total fraud share of 64%, the Americas stand out as an area of high-risk fraud origination, making the region a key focus for airlines looking to strengthen their payments security.[4] The fluctuating levels of geographical risk also show that the sector needs to take a targeted approach by deploying corridor-specific controls at a global scale and doubling down on secure payments in high-risk inter-regional flows.

** A fraud rate of five basis points is equivalent to $5 of fraud out of $10,000 payment volume.
[3] Visa Net MIS Fraud Insights. Region Trends Over Time (Dom vs XB) 2025 Q1 with History.
[4] Visa Net MIS Merchant region and Issuer fraud (XB Airliner EU) Q1 2024 – Q1 2025.

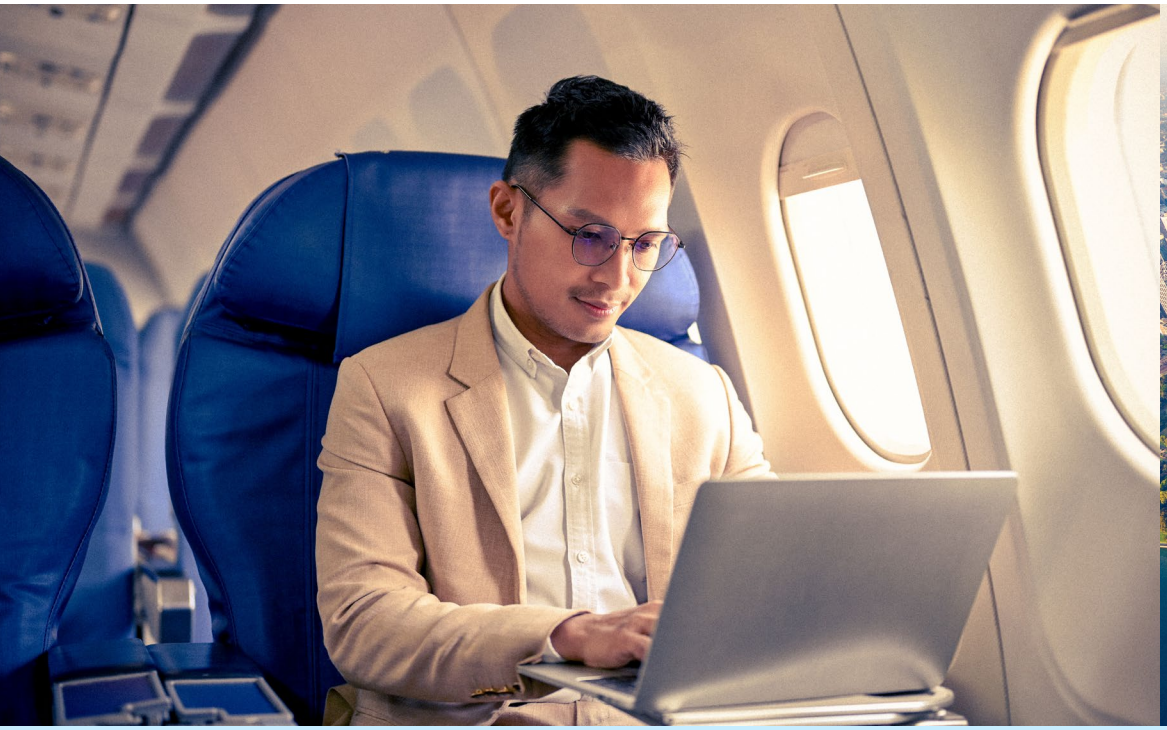
Protection without compromise

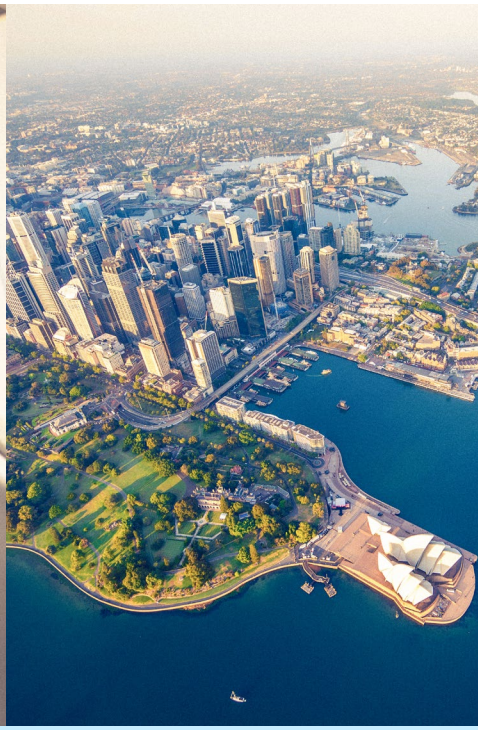
To address the complex, cross-border fraud risks they face today, airlines need robust controls that are resilient to the evolving capabilities of fraudsters. With revenue margins and customer loyalty at stake, airlines should consider the customer experience at every step; balancing speed with security and convenience, adding friction where it matters and invisibility where it doesn't.

Bringing unique technology capabilities and industry expertise, Visa can provide the tools airlines need to mitigate risk and drive growth. This includes:

- **Account Takeover Protection.**
  Protects online customer accounts from unauthorized access, averts fraud attempts before they take place, and preserves customer trust and loyalty.
- **Click to Pay.**
  Like contactless, but online. Click to Pay eliminates the need for customers to enter card details to provide a more secure checkout experience that's convenient for everyone involved.
- **Decision Manager.**
  An AI-powered, real-time fraud management solution supported by robust data to help detect fraud and automate decision-making, balancing risk with revenue and exceptional customer experiences.
- **Payer Authentication.**
  Adds security but not friction by using the latest EMV 3-D Secure capabilities to authenticate payment credentials at the time of transaction. This allows airlines to identify bad requests before sending for authorization and shift liability while reducing false declines.
- **Tokenization.**
  Limits exposure of sensitive data and minimizes fraud liability by turning sensitive card details into tokens, enhancing security and driving conversion.
- **Visa's B2B virtual card product, Visa Commercial Choice Travel (VCCT).**
  A proven solution with a travel fraud rate of 0.0009 basis points, virtual cards securely support transactions across a wide range of borders with single-use numbers to reduce fraud risk.[5]
- **VPRI (Visa Protect Risk Insights).**
  Leverages predictive intelligence to prevent ecommerce transaction fraud. The solution uses identity dynamics, behavioral analysis, geographic relationships, velocity, and frequency of key events to detect anomalies and high-risk transactions.

[5] Visa corporate T&E, Visa Purchasing, Visa Purchasing with Fleet, Visa Commercial Agriculture, Visa Commercial Choice Travel.





Why Visa?

Home to one of the largest payment networks, Visa is the ideal partner for airlines wanting to build global cooperation frameworks that allow them to embed fraud prevention measures across the entire customer journey.

With a suite of data-driven solutions on hand to prevent evolving fraud threats, including virtual cards and Decision Manager, Visa's support can adapt to your company's specific needs—ensuring you're always one step ahead.

Take the next step with the Visa B2B travel team.

Get in touch