

Burbank.

The Travel Trust Gap.

Why genuine travellers
can look like fraudsters

SEPTEMBER 2026



\$11m

lost to fraud each year
by the average travel,
ticketing or hospitality
company.

Source: Ravelin

+32%

year-on-year increase in
flight fraud risk recorded
in May 2026.

Source: Riskified

79%

of travel merchants
expect the cost of fraud
to increase.

Source: Ravelin

When genuine travel looks like fraud.

Travel has become one of the most sophisticated sectors in digital commerce. Online travel agents, accommodation platforms, airlines and travel intermediaries process billions in transactions each year, supported by increasingly sophisticated fraud prevention and authentication technologies.

Yet travel presents an unusual challenge: genuine customer behaviour can look remarkably like fraud. A traveller may make a high-value booking from a new device, while overseas, using a card issued in another country and booking for several other people. Each can be a legitimate part of the travel experience, and each can also be interpreted as a signal of elevated risk.

This creates a difficult commercial balance. Approve the wrong transaction and the merchant may face fraud and chargebacks. Decline the wrong one and a valuable customer may simply book elsewhere.

For years, the payments industry has become increasingly sophisticated at assessing risk. But risk assessment is ultimately based on probability. In travel, where what can be perceived as 'unusual' behaviour is often entirely legitimate, there is an opportunity to establish something stronger: proof that the genuine cardholder is authorising the transaction.

This paper explores the travel trust gap, its implications for travel businesses, and how a shift from predicting risk towards proving authenticity could change the way travel payments are trusted.

Ross Drayton
Head of Europe



Travel has a unique trust problem.

The same behaviours that can signal fraud are often simply part of travelling.





In travel, unusual behaviour is often entirely normal.

Most fraud prevention technologies rely, at least in part, on identifying unusual behaviour. In many industries, that makes sense. If a customer who normally shops locally suddenly attempts to make a high-value purchase from another country, using a new device and an unfamiliar delivery address, there are good reasons to take a closer look.

But travel is different. A UK cardholder might book accommodation in Asia while physically located in Spain. A family may spend thousands on a holiday six months before they travel. A booking may include multiple travellers, change several times before departure and be made from a device the merchant has never seen before.

None of this is inherently suspicious. In travel, this type of 'unusual' behaviour is often entirely normal. This creates a challenge for travel operators because many of the characteristics that make a transaction look risky are also natural characteristics of legitimate travel purchases.

Fraud prevention tools have become increasingly sophisticated at interpreting these signals. But ultimately, merchants are still being asked to make a judgement: how confident are we that the person behind this transaction is genuine?

That uncertainty is the travel trust gap.

And, there is a cost of getting it wrong.

When businesses talk about payment fraud, the conversation naturally focuses on financial loss. Fraud losses are visible. A fraudulent booking is identified, the value can be measured, and, in many cases, the merchant carries the cost of the resulting chargeback, dispute and investigation.

The cost of mistrust is harder to see. When a genuine booking is declined, the merchant may never know what happened next. The customer might retry, use another payment method or contact customer support. But in travel, where alternative flights, accommodation and package holidays may be only a few clicks away, they can just as easily book elsewhere.

The merchant sees a declined transaction. What it may not see is a lost customer who may well have been genuine. And the commercial impact can extend well beyond the value of that booking. It can mean lost commission and ancillary revenue, wasted acquisition spend, missed loyalty or membership opportunities, and the loss of future bookings from a potentially valuable customer.

This creates an uncomfortable tension for travel businesses. Controls designed to protect revenue can also prevent genuine revenue from being accepted. The challenge, therefore, is not simply reducing fraud. It is reducing fraud without unnecessarily turning good customers away.



Why existing controls still leave gaps.

Legitimate behaviour can look suspicious, so continually improving the prediction of risk can only take the industry so far. Because at the end of the day, it is only a prediction.

The travel industry has invested heavily in fraud prevention and authentication, with good reason. Machine learning, device intelligence, behavioural analytics, network data, 3D Secure and increasingly sophisticated fraud platforms have all strengthened the industry's ability to identify suspicious transactions and manage risk.

These technologies play an important role. But ultimately, they are only able to predict how likely it is that the transaction is fraudulent. A fraud engine can identify patterns associated with previous fraud. Device intelligence can assess the device being used. Behavioural analytics can identify anomalies in the customer journey. 3D Secure can add authentication to a card not present transaction.

Together, these signals allow increasingly sophisticated decisions to be made about risk. But they do not change the underlying nature of the transaction. It remains card not present. This distinction is important because the merchant is still making a decision based on the information available: whether there is enough confidence to approve the transaction, or enough concern to decline or challenge it.

For most categories of online selling, this model works remarkably well. Travel, however, creates a disproportionate number of transactions where the signals are harder to interpret and the consequences of getting the decision wrong can be significant.

Fraud takes many forms.

Across travel's most difficult fraud challenges, the same question persists: who is really behind the transaction?



Travel's most difficult fraud challenges.

The travel trust gap plays out in different ways across the customer journey. While the types of fraud vary, the underlying challenge is often the same: establishing whether the person behind the transaction is genuinely entitled to use the payment credentials or account.



Stolen card fraud

Travel remains an attractive target for criminals using compromised payment credentials. High transaction values, cross-border activity and delayed fulfilment can create opportunities to turn stolen card details into flights, accommodation and other travel products with real-world value.

The difficulty for merchants is that the credentials themselves may be valid, and the booking may appear entirely plausible. Furthermore, many of the characteristics that might otherwise indicate fraud, including high values, international activity and unfamiliar locations, are also commonplace in legitimate travel.

The challenge is therefore not simply validating the payment credentials. It is establishing whether the genuine cardholder is behind the transaction.



Account takeover

As travel businesses invest more heavily in loyalty, membership and personalised customer experiences, customer accounts are becoming increasingly valuable. A single account can contain stored payment credentials, traveller information, booking history, loyalty balances and premium benefits. That makes the account valuable to the customer, the merchant and, increasingly, fraudsters.

Account takeover creates a particular trust problem because many of the signals a merchant normally relies on may appear legitimate. The account is genuine, the payment credentials may already be stored, the booking behaviour may even resemble previous activity.

What has changed is the person controlling the account. The growth of loyalty and membership programmes raises the stakes further. Establishing trust is no longer only important at the point of payment. It can also matter when customers enrol, recover an account or attempt sensitive activity within an existing relationship.



Chargebacks and disputed transactions

Travel businesses also face a significant challenge when transactions are disputed. Travel purchases can be made months before fulfilment, involve multiple travellers and carry relatively high values. Some disputes are legitimate. Others can arise from forgotten purchases, confusion over transactions or deliberate misuse of the chargeback process. Whatever the cause, the merchant may be required to demonstrate that the genuine cardholder authorised the payment.

This exposes another dimension of the travel trust gap. The question is not only whether the merchant had enough confidence to approve the transaction at the time. It is whether it can later demonstrate that the genuine cardholder participated in and authorised it.

Across each of these challenges, more data can help merchants make better decisions. But there are limits to what additional signals can tell us when legitimate and fraudulent behaviour can look remarkably similar.

For travel businesses, that leaves a difficult commercial challenge: how to protect against fraud without creating barriers for the genuine customers they want to approve.





The approval problem.

For travel merchants, the challenge can be distilled into one question: *How do we approve more genuine customers without increasing fraud?*

Every fraud strategy involves a balance. Controls need to be strong enough to stop fraudulent transactions without creating so much friction or uncertainty that legitimate customers are caught in the process.

Over time, the payments industry has become extraordinarily sophisticated at managing that balance. Risk engines, behavioural analytics, device intelligence and authentication technologies can draw on an enormous range of signals to determine whether a transaction should be trusted. But the underlying model remains largely one of prediction.

The merchant is asking: How risky does this transaction appear to be?

That question will always be important. But there is another question that becomes particularly powerful in travel: *Can we prove that the genuine cardholder is authorising this transaction?*

The distinction is important. Risk assessment uses signals to determine the probability that a transaction is genuine or fraudulent. Proof provides direct evidence that the genuine cardholder is participating in the payment.

For travel businesses, this has the potential to change the approval equation. A high-value booking from an unfamiliar device or unusual location does not need to become inherently less suspicious. Instead, the merchant can have stronger evidence on which to make the decision.

This represents a shift in emphasis: from continually refining the prediction of risk towards creating stronger proof of authenticity. The objective is not to authenticate every customer more often or introduce unnecessary friction into every transaction. It is to establish greater certainty when the value or risk of a transaction makes that certainty worthwhile.

In other words, the opportunity is not simply to get better at identifying bad transactions, it's to become more certain about the good ones.

From card not present to card present.

Instead of adding another layer
of authentication to a card not
present payment, change the
transaction itself.



Change the transaction. Change the equation.

One way to establish stronger proof is to change the nature of the payment itself. Card Present over Internet (CPol®) extends the familiar principles of card present payments into online channels. Using their physical payment card and PIN, customers can authenticate an online payment in the same way they do at a payment terminal.

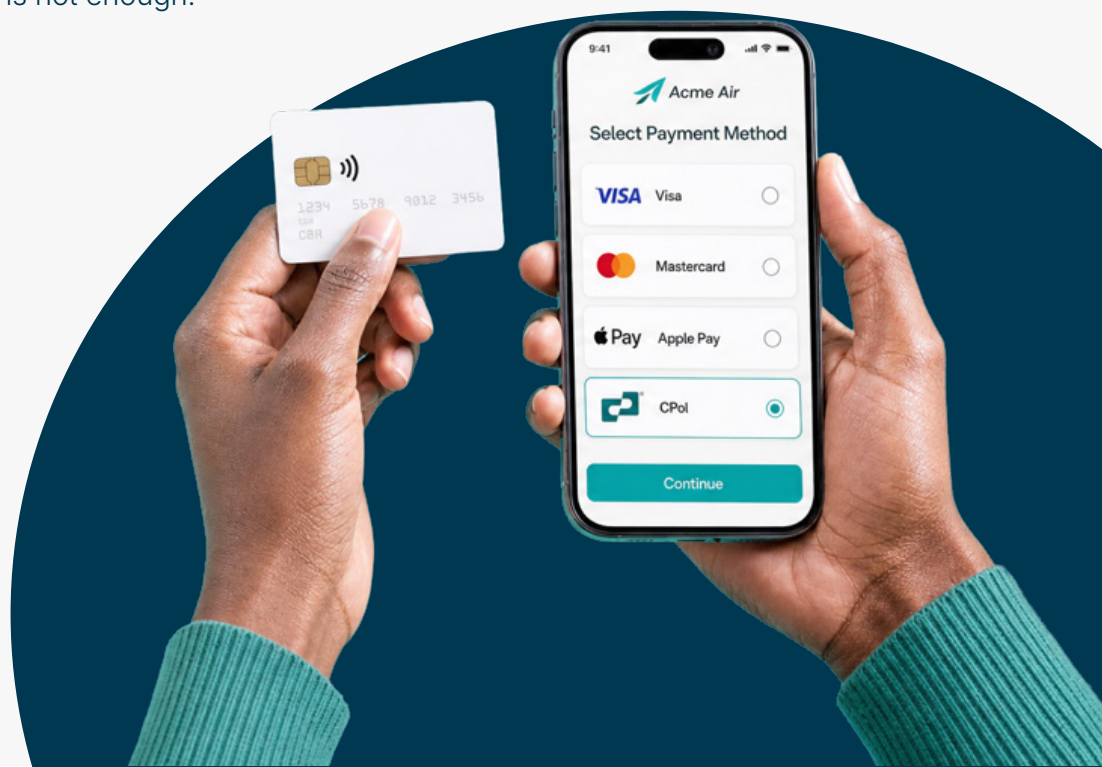
The important distinction is that CPol® does not simply add another layer of authentication to a card not present transaction. Instead, it enables a genuine card present transaction online.

Instead of relying solely on data, behavioural signals and risk models to determine whether the person entering card details is likely to be genuine, the physical card and PIN provide proof that the genuine cardholder authorised the payment.

For travel businesses, this creates potential applications wherever greater certainty has particular value, including high-value bookings, transactions identified as higher risk, account recovery and other sensitive customer journeys. It does not mean every transaction needs additional authentication, nor does it remove the role of existing fraud technologies. But it does provide another option when prediction alone is not enough.

For merchants, the opportunity is to make better decisions about genuine customers while reducing exposure to fraud and chargebacks. For customers, it means that unusual travel behaviour does not necessarily have to stand between them and a legitimate purchase.

And for the travel industry, it introduces a fundamentally different way to close the trust gap: not by trying to make ever more accurate assumptions about who is behind a transaction, but by providing stronger proof.



Closing the travel trust gap

Travel will always present challenges for fraud prevention. Customers cross borders. They change devices and locations, book for other people, make high-value purchases and plan trips months in advance. Many of the behaviours that make travel unique are also the behaviours that can make transactions more difficult to assess.

The answer is not to stop assessing risk. Fraud detection, behavioural analytics and other risk technologies will continue to play an important role in protecting travel businesses and their customers. But there is an opportunity to complement prediction with something stronger - proof.

When merchants can establish that the genuine cardholder is participating in and authorising a transaction, the decision no longer needs to rely on risk signals alone. That has implications beyond fraud prevention. Greater certainty can help merchants approve genuine customers, reduce unnecessary declines and challenge fewer legitimate transactions, while providing stronger protection against fraud and chargebacks. For years, the industry has become progressively better at asking: How risky does this transaction appear to be?

The next opportunity is to ask: **What can we prove?**

For travel, that could be the key to closing the trust gap.

About Burbank.

Burbank is a payments technology company and the creator of Card Present over Internet (CPol®), software that enables genuine card present transactions in online channels using the customer's physical card and PIN and their own mobile device.

CPol® is designed to help merchants reduce fraud and chargebacks, approve more genuine customers and bring the security of card present payments to digital commerce.

Find out more at paywithcpoi.com



Burbank.