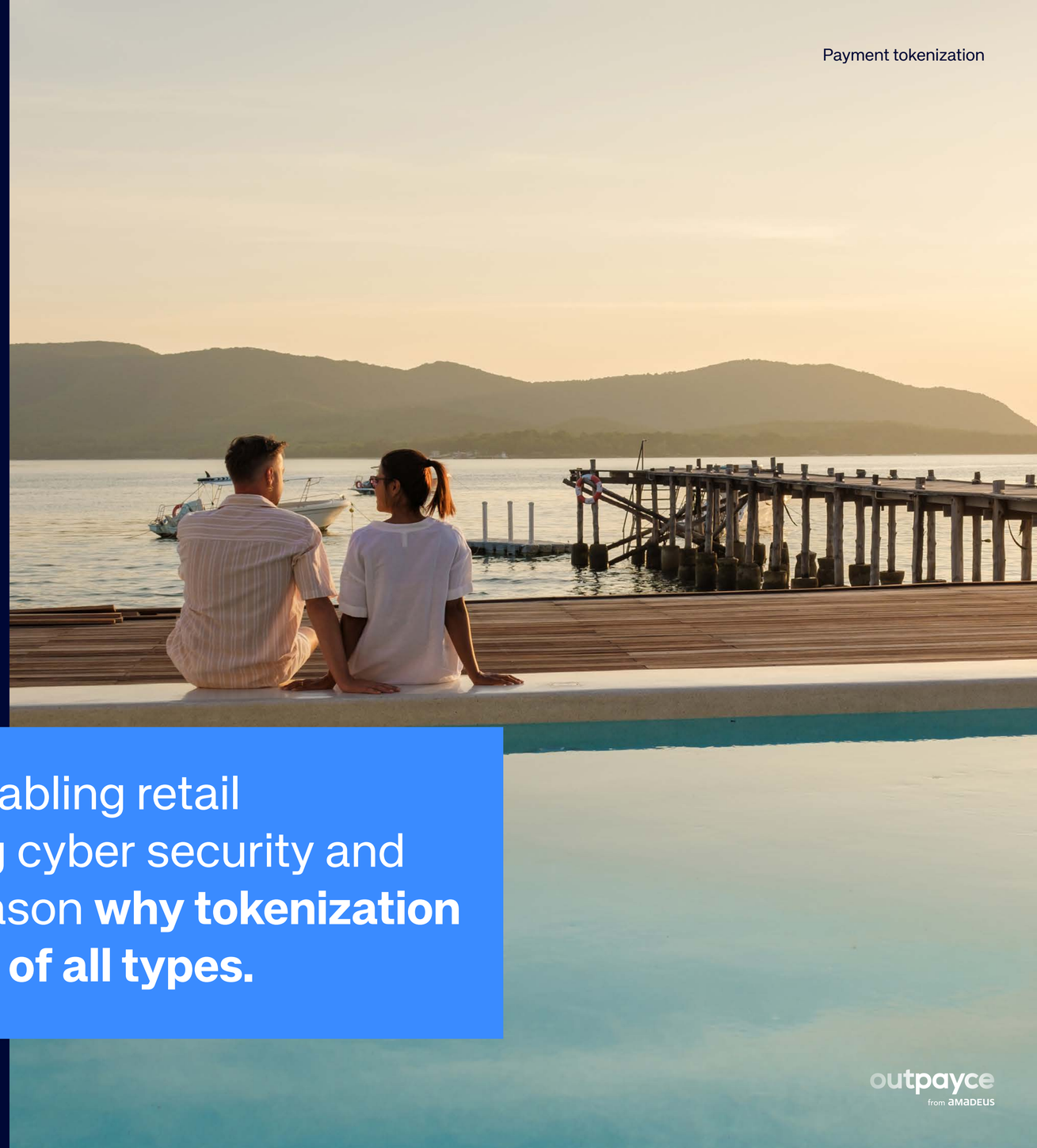
outpayce from AMADEUS | Travel. Simply paid.

Payment tokenization:

A key enabler of airline e-commerce security

E-commerce is a crucial channel for airlines, with online bookings expected to account for approximately 65% of all global bookings by 2026 and continue to grow, particularly for Low-Cost Carriers (LCCs), many of which sell exclusively online. As airlines demand rebounded post-pandemic, airlines had to rapidly digitalize the customer journey, accelerating the modernization of the payment experience.

With airlines' large transaction volumes, global reach, and expanding digital infrastructure, robust payment security is essential as they handle growing volumes of sensitive customer and payment data. Concurrently, the core role of the payments function – to securely accept traveler funds in a way that supports conversion and revenue generation – remains paramount. In fact, with airlines investing to become retailers of more third-party products, the need to exchange payment information with partners and provide a smooth checkout experience increases.



This dual challenge of enabling retail success while minimizing cyber security and compliance risk is the reason **why tokenization is a key focus for airlines of all types.**

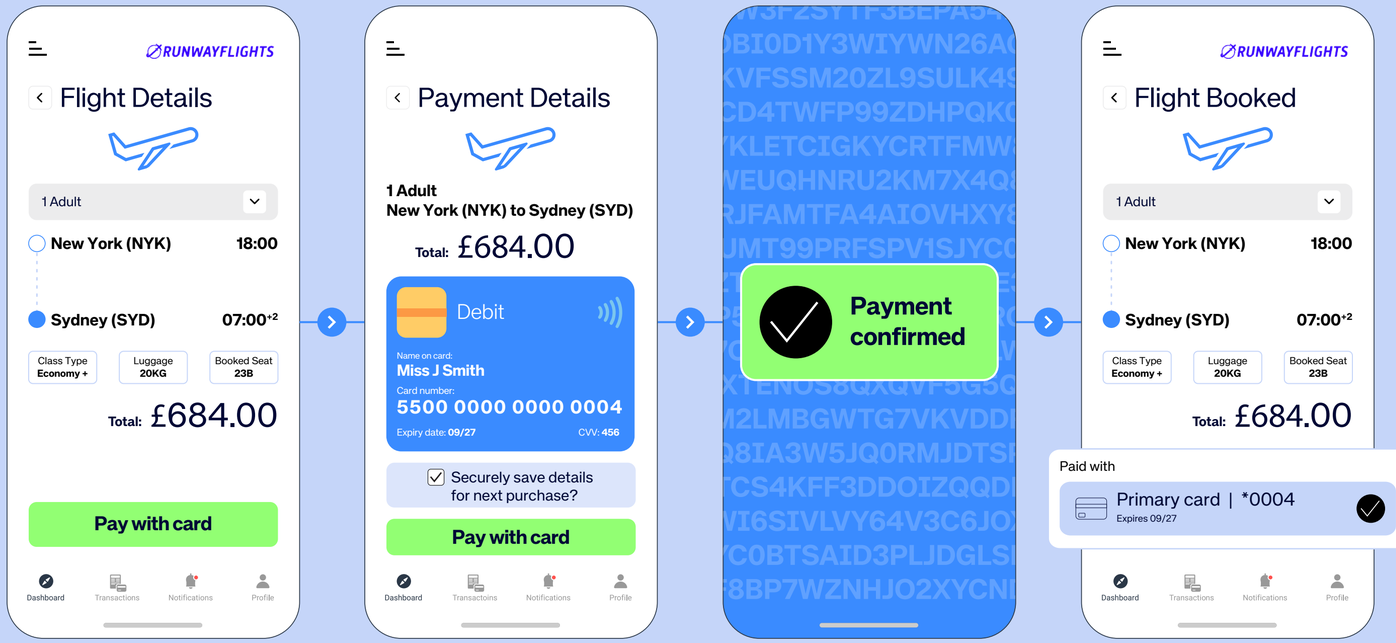
01 What is tokenization?

Tokenization is a security technique that protects sensitive payment card data.

When a merchant tokenizes the customer's payment card, this sensitive 16-digit card number is stored securely in a vault provided by the tokenization supplier. Within the merchant system, the card number is then represented by a surrogate value, such as alphanumeric characters or other forms of identifier, that have no meaning outside the intended environment.

The merchant can then work with the token rather than assuming the risk associated with storing and processing the sensitive 16-digit card number.

A common analogy is that of a casino, where you exchange cash for chips. Those chips are only valid in the casino environment when placing bets, and you can't use them outside, for example, to pay for a meal at the restaurant next door.



outpayce
from AMADEUS

Tokens follow the same principle – they can be used for processing payments within an airline's ecosystem, but they're useless in any other context. That means if tokens are lost during a cyber breach, the attacker cannot use them to fraudulently spend the traveler's funds.

Amongst tokenization, there are two main types of token: **proprietary tokens** and **network tokens.**

Both approaches strengthen payments security, with proprietary tokenization ensuring card data never enters the merchant's environment, while network tokens optimize payment performance. When combined, airlines can achieve the optimum balance between control, security, and interoperability.

Proprietary tokens enhance security by replacing the 16-digit card number and are valid only within the airline's own ecosystem. They provide airlines with complete control over tokenization and are provided by a partner like Outpayce from Amadeus. When combined with 'online and offline walls', they provide interoperability for smooth payment processing with third parties.

Network tokens are provided by card schemes and are designed to work throughout the payments chain. They include interoperability as standard but provide airlines with less control as they depend on support and readiness of issuers, acquirers, card networks, and other third parties.

outpayce
from amadeus

02 Why tokenization is essential for risk management

outpayce
from AMADEUS

As evermore commerce becomes digital, payments security is critical for merchants in every sector. For example, data from Edgar Dunn & Co shows that Europe's travel e-commerce sales are expected to grow from $113B in 2026 to $171B by 2031.

At the same time, growing digital exposure is leaving merchants facing an arising number of cyber-attacks and fraud attempts. Card fraud cost merchants $34.1B in 2024, with research showing the airline industry is the most targeted.

A high purchase price and delayed delivery of the service mean our industry remains a primary target, to the extent that 36% of all fraudulent card transactions occur in the airline sector. Even more concerningly, data shows that airlines are ~3 times more likely to suffer a data breach than banking, technology or healthcare organizations.

Travel e-commerce sales set to grow from

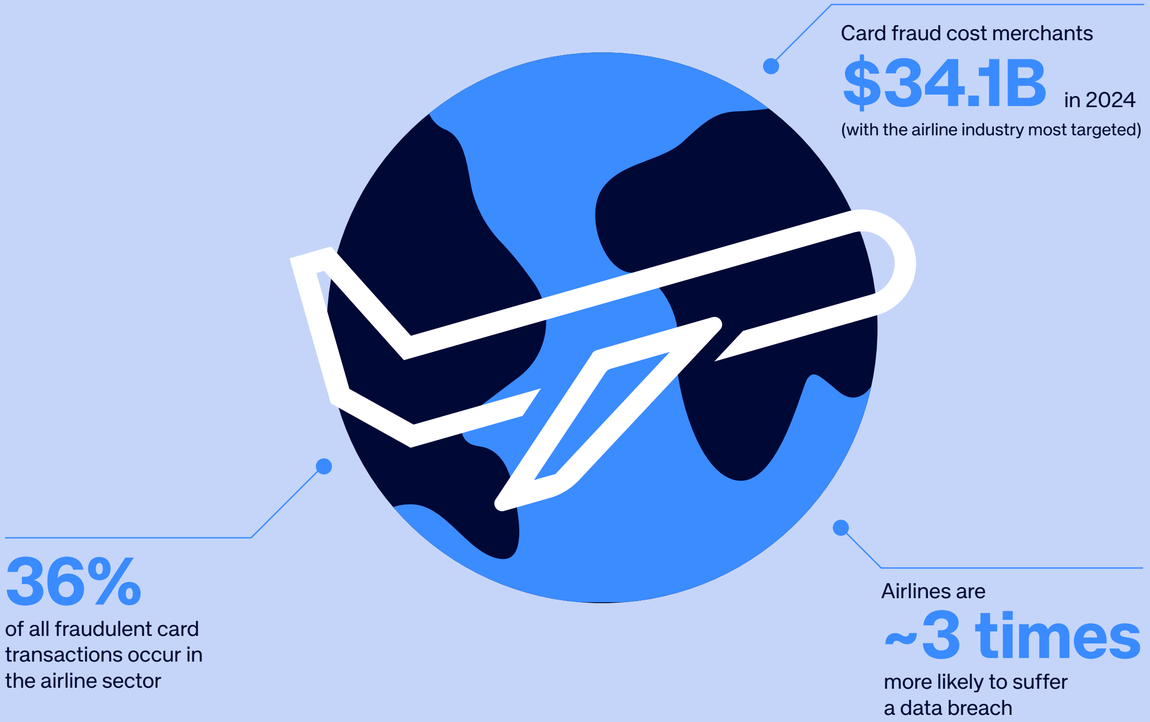
$113B

in 2026 to

$171B

by 2031

In this context, it's essential that airlines protect traveler data by providing secure digital payments that build trust while meeting security and compliance obligations and reducing the burden of industry regulations.



outpayce
from AMADEUS

Reduce PCI DSS compliance requirements up to 90%

Payment Card Industry Data Security Standard (PCI DSS) is an industry regulation that applies on a global basis, with stringent requirements for merchants to protect sensitive payment information. Airlines are required to ensure all card processes are PCI DSS compliant, so traveler payment data is adequately protected. A PCI DSS audit to review key processes is required each year, with annual compliance costs running into millions of euros for a large airline.

For example, when embarking on tokenization with Outpayce from Amadeus, Air France identified 160 separate processes across its sales and back-office operations where customer card details were handled. With card details collected during booking, sent to acquirers during payment processing and used for reconciliation in the back office, achieving compliance wasn't straightforward.

By replacing sensitive card details with secure tokens, airlines can greatly reduce the number of business processes where card details are handled and therefore limit the cost and workload of PCI DSS compliance.

AIRFRANCE

How Air France reduced PCI DSS requirements by 75%

Air France conducted a thorough audit of its business processes to identify everywhere the airline worked with customer card details.

More than 160 different processes were identified including:

- Payment processing when card details were provided to fraud and acquirer partners
- The back office, where payments are reconciled to bookings
- Refund and dispute process, for example, when responding to chargebacks

The airline worked closely with Outpayce from Amadeus to apply tokenization across its entire operations including digital, call center and airport processes.

Today, Air France no longer holds passenger card details on its own systems and tokens are used throughout its business processes. Outpayce from Amadeus' online and offline walls are used to securely detokenize as needed to facilitate third-party processing.

Thanks to the project, Air France has been able to:

- Significantly enhance security for its customers while reducing its own risk exposure
- Reduce its PCI DSS workload from 350 on-going requirements to just 60
- Retain ownership over the payment flow to facilitate orchestration and analytics
- Reduce its cost of compliance and operation

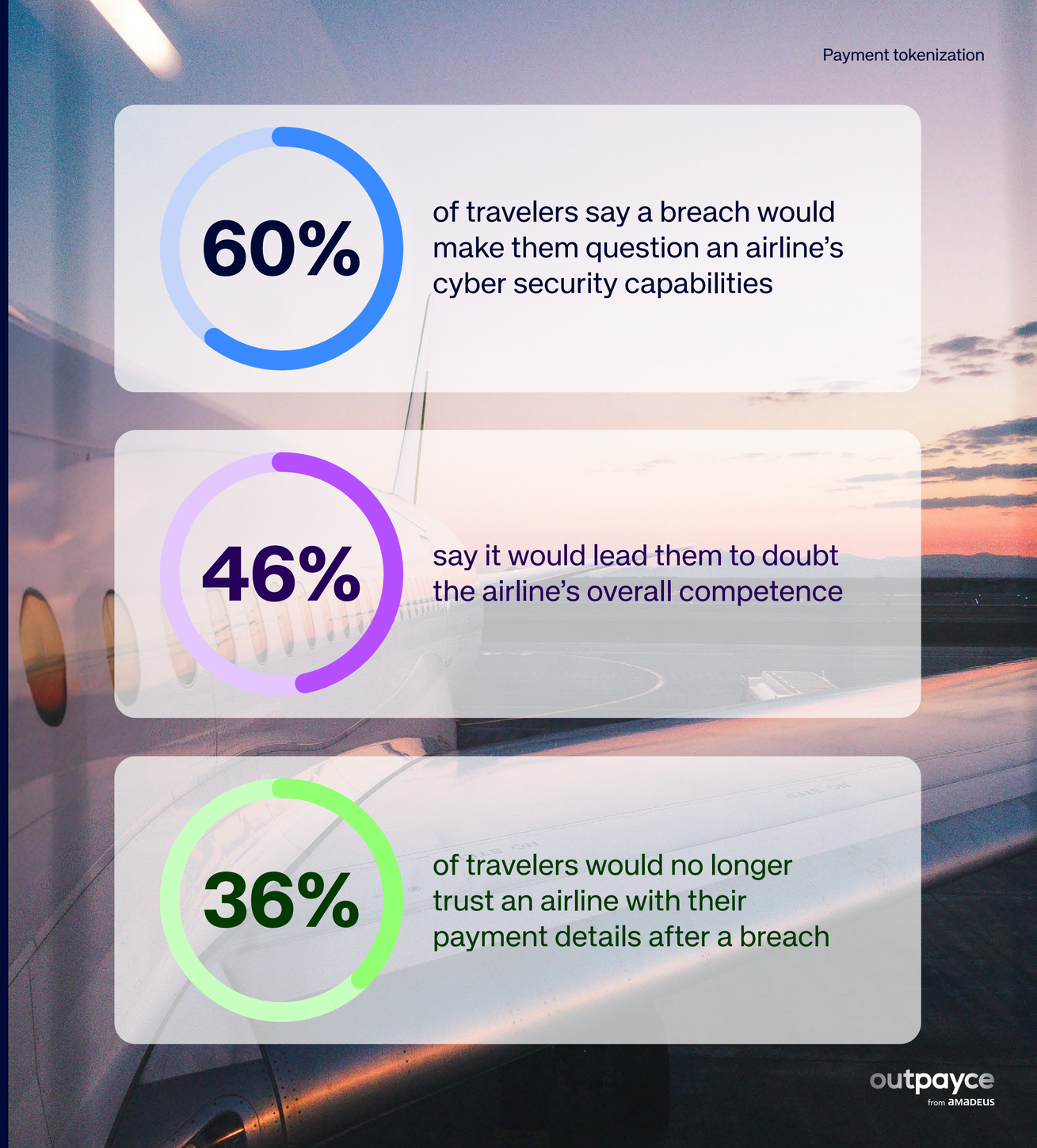
Protect reputation and market capitalization

Data breaches can have a material impact on a company's reputation and its market capitalization.

Research conducted by Oxford Economics on behalf of IT services firm CGI was the first study to isolate the share price impact of a data breach. The economists examined all data breaches that impacted FTSE 100 firms over a five-year period and found a major breach led to an average long-term share price decline of 1.8%. Across the 65 firms impacted, this equated to £42B in lost market value.

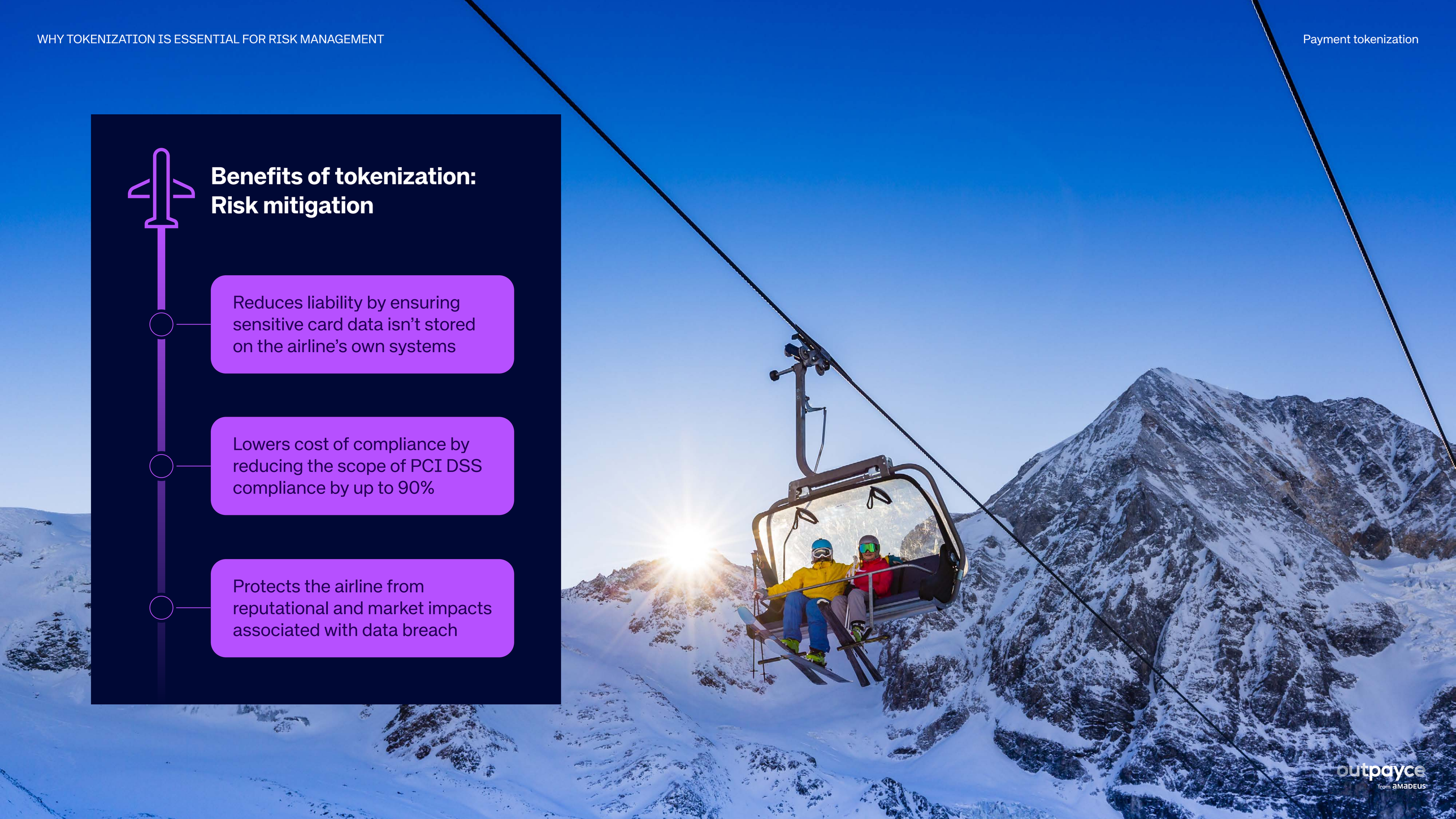
Not every impact from a data breach can be measured as tangibly. While harder to measure, reputational impact can also be significant as customers, investors, employees, and stakeholders lose confidence in the organization.

Our latest Security in travel payments research with travelers found that a cyber breach leaves a lasting impact with 60% saying they would question the firm's cyber security capabilities and 46% confirming they would 'question the airline's overall competence, including in respect of safety'. If an airline had suffered a breach, 36% said they would no longer be willing to store their payment details with the company in the future. These findings clearly highlight how data breaches can quickly erode traveler trust and damage long-term customer relationships.



Benefits of tokenization: Risk mitigation

- Reduces liability by ensuring sensitive card data isn't stored on the airline's own systems
- Lowers cost of compliance by reducing the scope of PCI DSS compliance by up to 90%
- Protects the airline from reputational and market impacts associated with data breach



03

Why tokenization is essential for airline retailing

outpayce
from AMADEUS

While risk reduction objectives have traditionally driven tokenization projects, the technology is emerging as a key enabler for airline retailing. As airlines invest in the transformation to offers, orders, settlement and delivery, secure payment is a key enabler.

When travelers trust that their payment details are handled securely, they’re more likely to store them with an airline, which leads to a smooth checkout experience.

Tokenization improves conversion with a smooth checkout experience

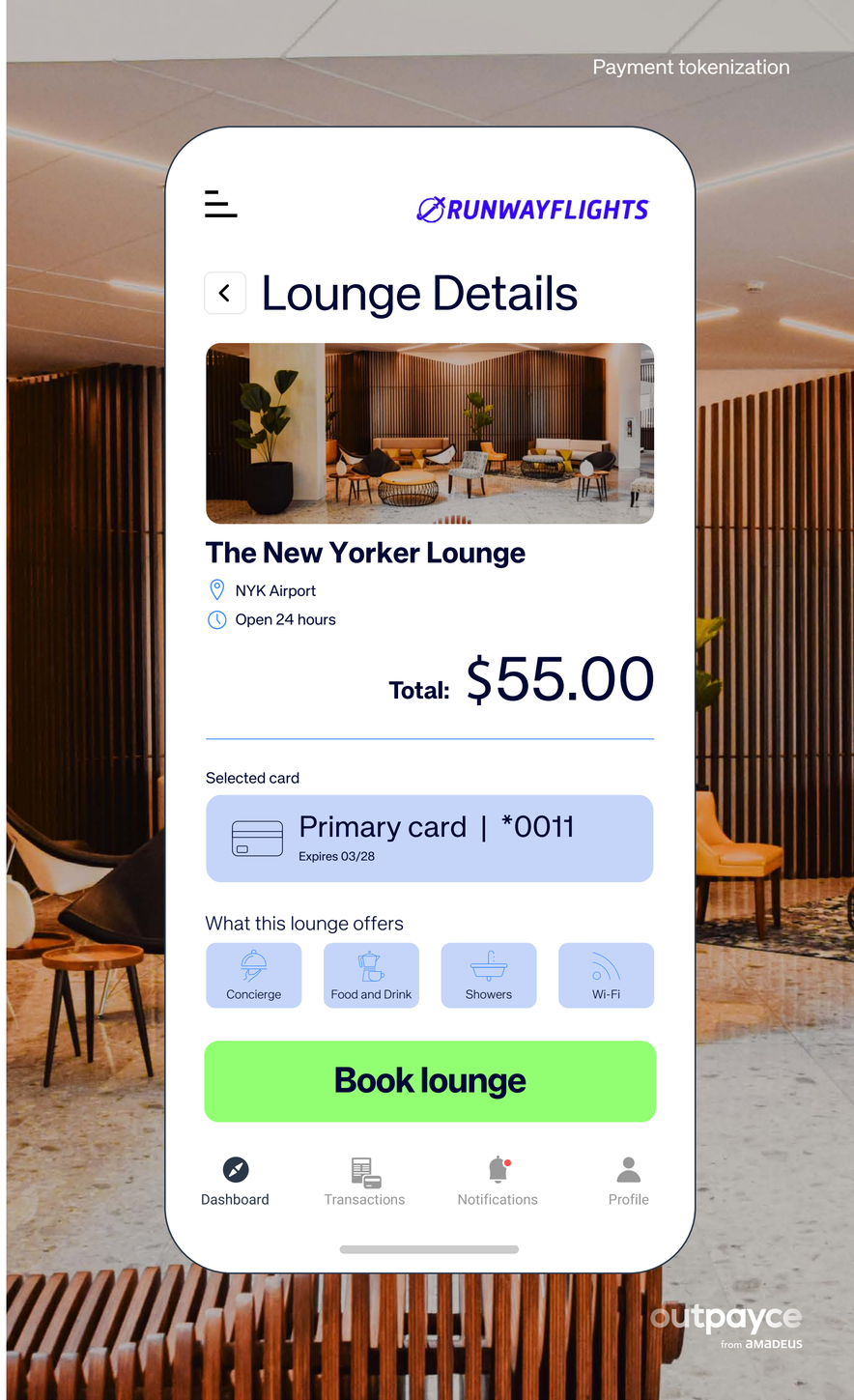
As airlines continue with the transformation to become modern retailers, the need to store the traveler's payment information on file grows. The industry wants travelers to easily add lounge access to their order from a mobile phone during the taxi ride to the airport, or to add an experience when sightseeing at the destination. Airlines want to retail their own and third-party products throughout the entire journey, and they're upgrading to a new generation of standards and technology to make it happen.

Achieving this vision requires a smooth one-click payment experience that's as easy as paying for an Uber. Such an experience requires the airline to be trusted to store the traveler's payment card on file, which in turn requires tokenization in the background.

Imagine trying to add speedy boarding or upgrade your seat from a mobile and being asked to manually type your 16-digit card number. In this scenario, the payments experience completely undermines any wider investment the airline may have made in offer creation and personalization.

Our research found that more than half of consumers find manually entering card details frustrating, yet large numbers still choose this option when traveling. It also identified the fear of fraud (63%) and data privacy (53%) as the top reasons consumers were reluctant to store their payment details with an airline.

Tokenization offers a proven way to facilitate one-click payments by securely storing card details without exposing travelers or airlines to the risk of fraud. When an airline has the traveler's card-on-file the checkout experience is transformed from a clunky 16-digit typing exercise to an invisible payment that's authorized in an instant.



Grow third-party retailing securely

The ability to securely share sensitive payments information with partners is a key capability for airlines. This is particularly true for LCCs, many of which drive upwards of half their revenue from the sale of ancillary products.

In some ancillary sales models, an airline will offer third party products like insurance or transfers without becoming the merchant of record. In this model, the airline may process a payment for the flight element of the booking and then pass the traveler's payment details through to the insurer and transfer company to process their element of the booking.

Here the right approach to tokenization can facilitate third-party sales by enabling the secure sharing of the traveler's payments information. At Outpayce we operate secure 'online and offline walls', which means we can detokenize and tokenize as needed in either batch or real-time mode.

In the above scenario, Outpayce would tokenize and store the traveler's payments information, removing the need for the airline to carry any risk. When the payments information needs to be shared with a commercial partner, like the insurer, Outpayce can detokenize and securely convey it as required.

Having tokenization in place supports third-party ancillary sales while limiting risk for the carrier.

Differentiate with a reputation for secure e-commerce

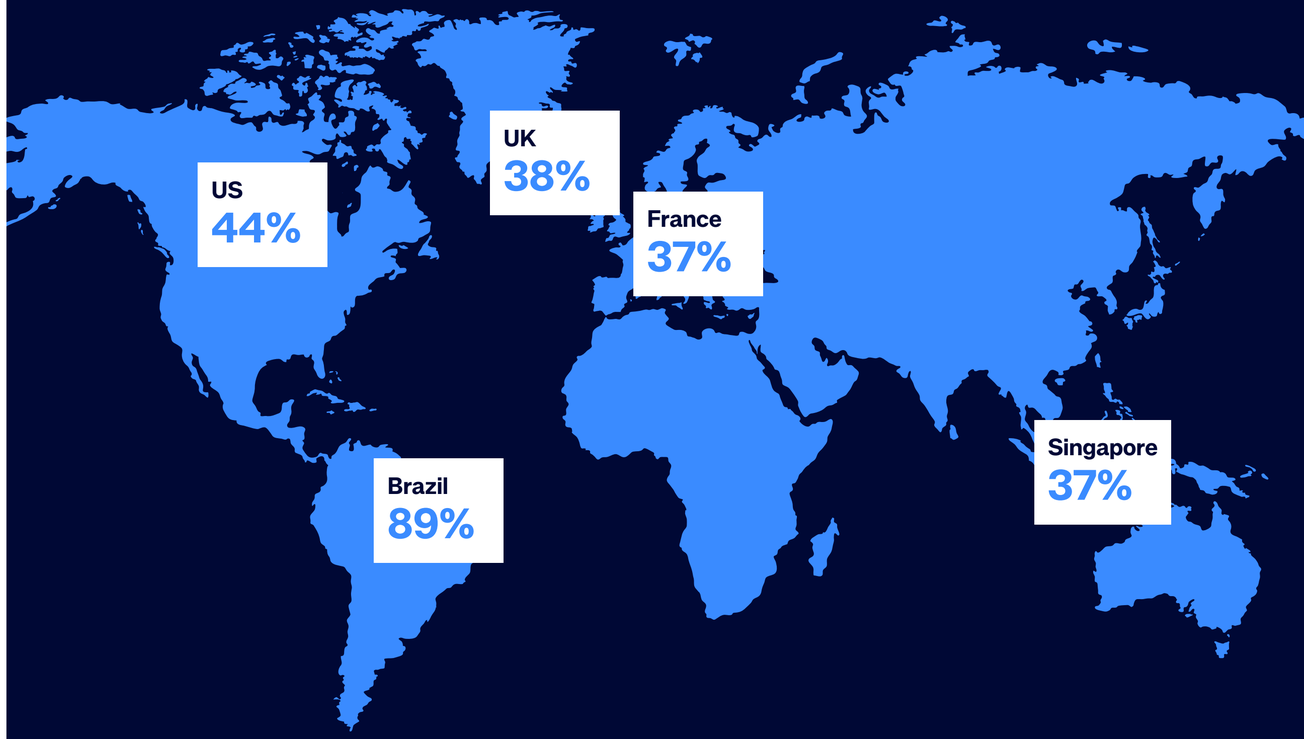
Airlines are focused on achieving differentiation and a recent Outpayce commissioned survey with 4,500 travelers from five key markets revealed that secure payments can play a role. According to the research, 72% of travelers said a ‘reputation for secure e-commerce’ would encourage them to choose one airline over another.

Rates of fraud vary significantly across geographies, with some higher risk markets across LATAM and APAC reaching levels that make operating or expanding routes more complex, costly and risky. When travel companies seek to benefit from commercial opportunities in these high growth markets, tokenization becomes an essential enabler of secure and scalable expansion.

72%

of travelers say a strong reputation for secure e-commerce influences their choice of airline.

Respondents who have experienced payments fraud



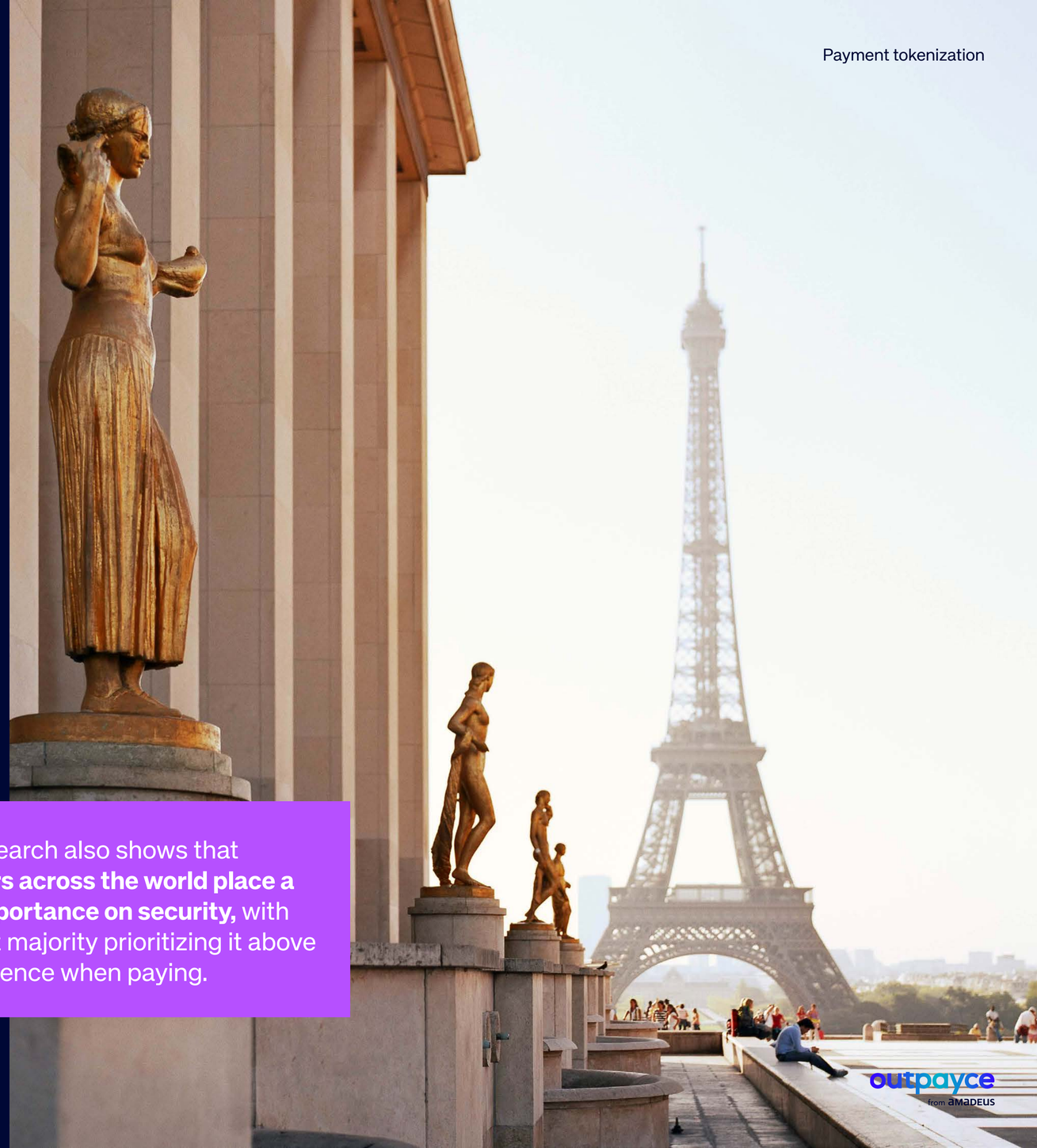
Source: Outpayce survey with 4,500 travelers

outpayce
from AMADEUS

Do you prioritize security or convenience when paying?

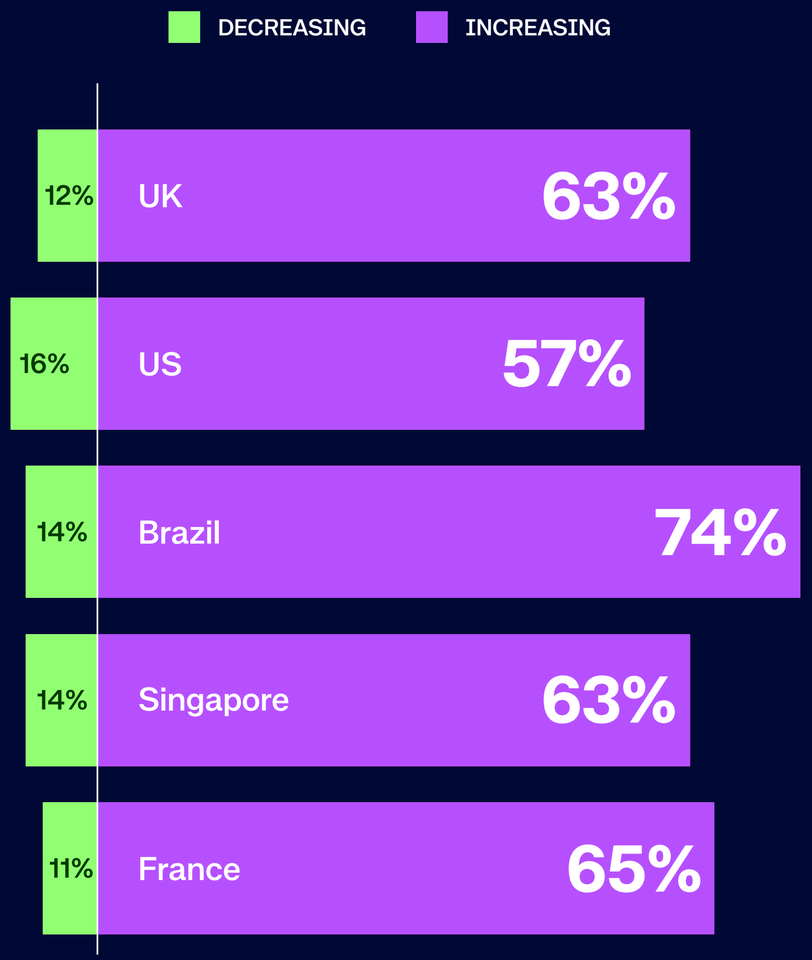
	SECURITY	CONVENIENCE
UK	56%	14%
US	53%	18%
Brazil	69%	9%
Singapore	51%	14%
France	64%	10%

The research also shows that **travelers across the world place a high importance on security,** with the vast majority prioritizing it above convenience when paying.



outpayce from AMADEUS

Do you feel like payments fraud is increasing or decreasing?



The research shows a connection between traveler perception of fraud growth and the importance placed on security. In markets like Brazil and France, where fraud is perceived to be increasing, **more travelers said they would prioritize security.**

In an environment where 35% of travelers told us they don't currently trust travel companies to keep their payments details secure, **the research highlights the growing importance that travelers place on secure commerce.**

outpayce from AMADEUS

04

How can airlines secure traveler card details with flexibility?

outpayce
from AMADEUS

The key to reducing risk is to achieve a payments architecture that eliminates the need to store sensitive card details. Tokenization achieves this by replacing the traveler's 16 digital card number with an alphanumeric token which is meaningless outside the airline's ecosystem and cannot be used to initiate a payment.

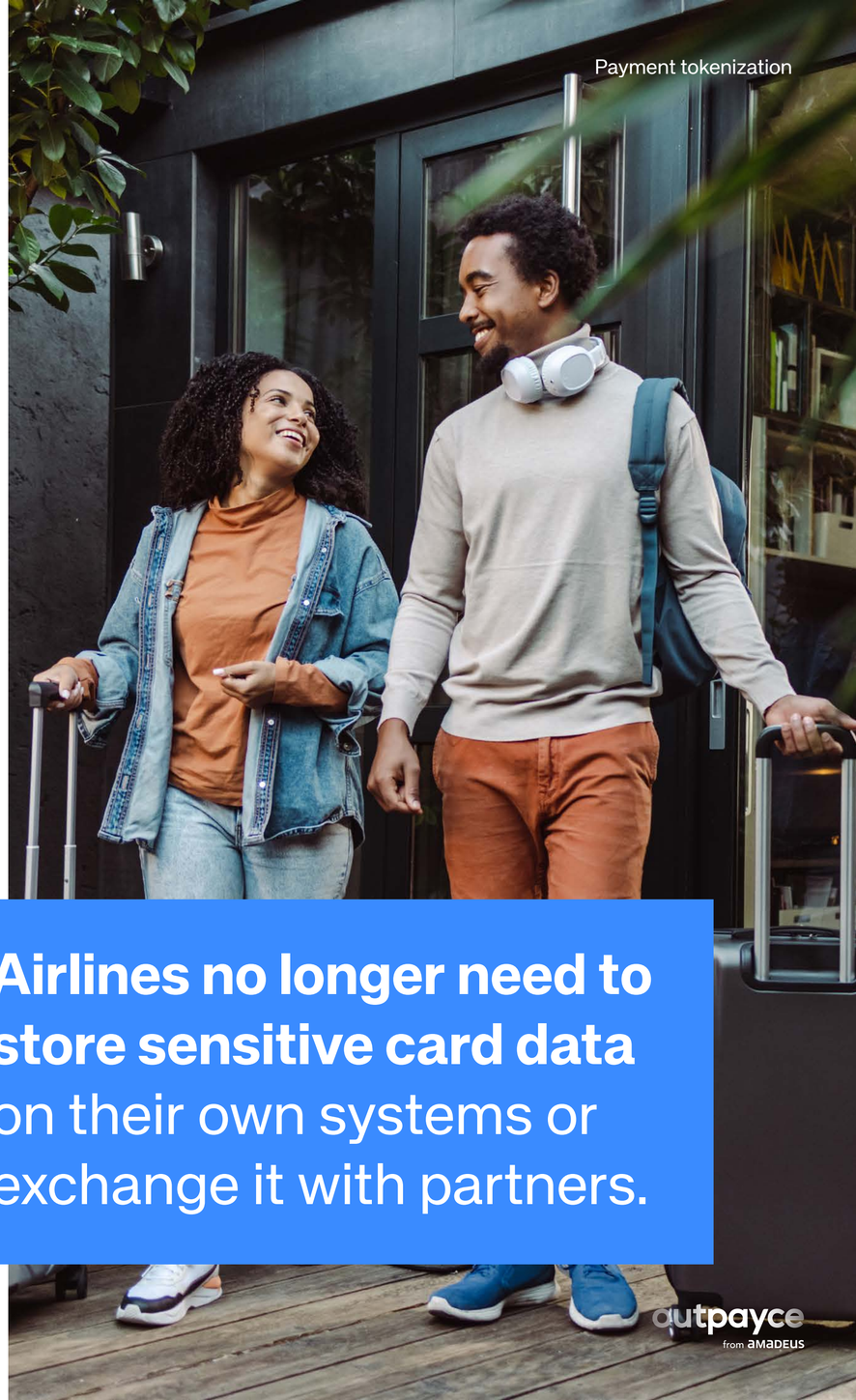
Instead, the traveler's sensitive card data is held securely in Outpayce's tokenization vault. We take a market-leading approach to securing this sensitive data, including splitting each card number into chunks and storing those chunks in separate databases, each of which is thoroughly encrypted. This approach drastically increases the burden for a would-be attacker as they must breach several layers of encryption. In the unlikely event this occurred, they would still lack the ability to successfully reassemble each 16-digit card number.

In addition, Outpayce only holds Card Verification Value (CVV) data for a maximum of ten minutes, after which it is deleted. This approach meets PCI DSS requirements and further removes risk by ensuring a would-be attacker cannot obtain the CVV number, which is required when initiating a retail transaction.

Even though tokenization achieves secure storage for sensitive payments data, airlines do need the ability to work with the underlying card data for a range of activities. For example, to pass to third parties like fraud analysis tools, authentication providers and acquirers when processing the payment. Airlines may also need to charge the passenger's card as part of a Merchant Initiated Transaction (MIT), perhaps as part of a loyalty transaction.

All these use cases require a tokenization partner that can tokenize and detokenize data as needed, without exposing the airline to PCI DSS risk. At Outpayce we achieve this with our secure online and offline walls. This capability means our airline customers can send tokens to third-party partners in the payments chain and Outpayce steps in to detokenize in real-time for both real-time online messages and batch file scenarios.

With this set-up, airlines no longer need to store sensitive card data on their own systems or exchange it with partners, greatly reducing liability while enabling secure commerce.



Airlines no longer need to store sensitive card data on their own systems or exchange it with partners.

outpayce from AMADEUS

05 Where next for tokenization?

outpayce
from AMADEUS

The introduction of network tokens is a positive development for the airline industry. The network token approach promises tokens that work throughout the broader payments chain, so payments can be processed securely without the need to exchange the underlying card details.

With network tokens, a passenger can store their card with an airline and should the card reach its end of life, be lost or stolen, the token is automatically updated with the new card details. This is possible thanks to the close links the card schemes have to card issuing banks.

While network tokens offer advantages for airlines and the payments industry at large, the benefits require every player in an airline's payment chain to be ready, e.g. issuers, acquirers, fraud and authentication partners. Today this is rarely the case, but with Mastercard working towards 100% network tokenization in Europe by 2030, this is expected to change.

Another limitation with existing Card-on-File network tokens is limited support for indirect channels, primarily due to the separation between the payment initiator (e.g. OTA or travel agency) and the merchant of record (e.g. airline or hotel).

Current network token frameworks are typically designed for direct channel use cases, where the same merchant captures the payment details and acts as the merchant of record. These scenarios are predominantly guest checkout flows involving customer-initiated transactions.

Accordingly, within the direct channel, Outpayce supports network tokenization through solutions such as Apple Pay and Google Pay, which are optimized for real-time, customer-present transactions and are fully aligned with existing network token capabilities. At Outpayce we also help airlines reduce PCI DSS compliance costs and secure their own ecosystem with our proprietary token solution and continue to evolve our capabilities in line with market needs and regulatory requirements.

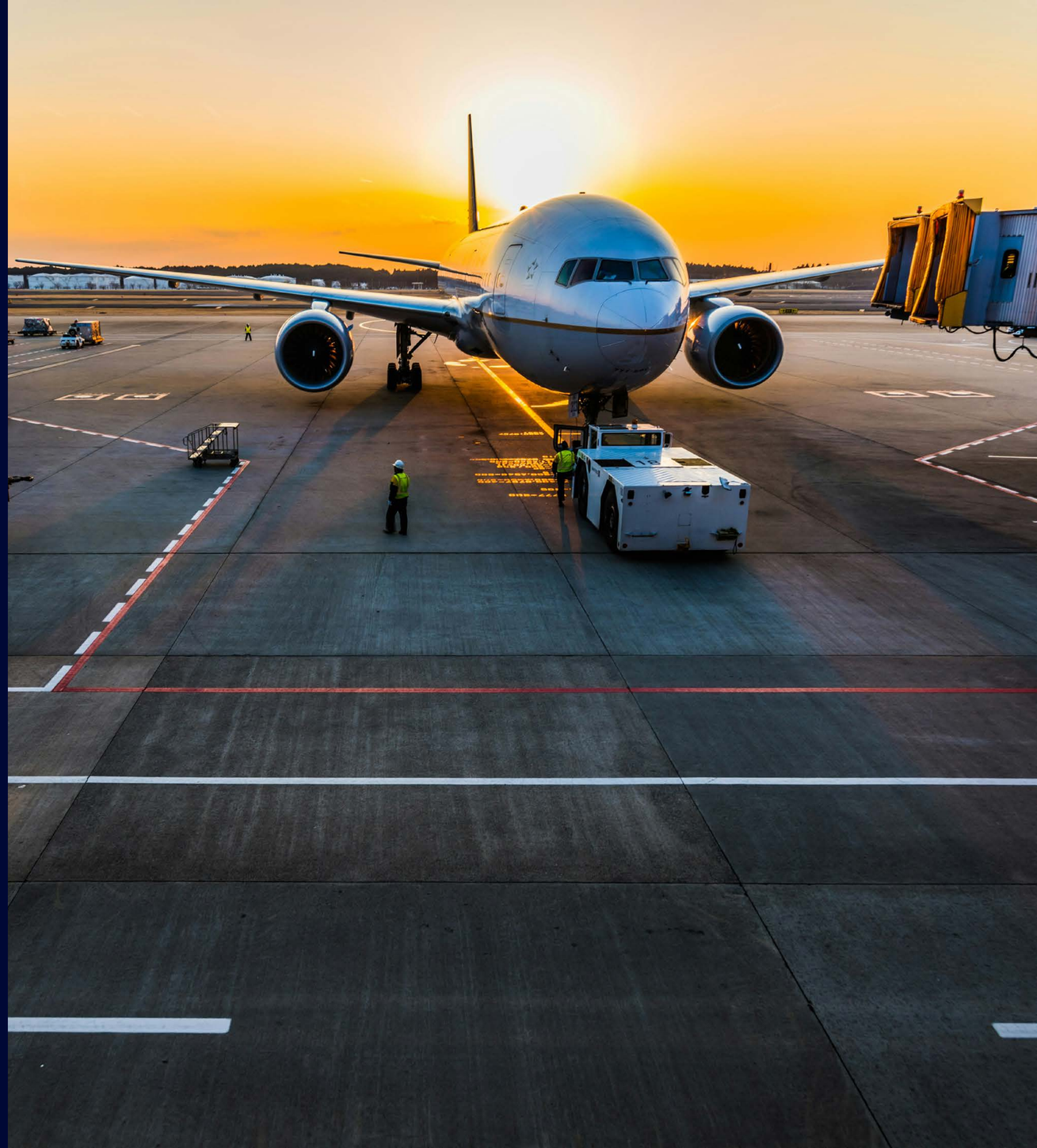
At Outpayce **we help airlines reduce PCI DSS compliance costs and secure their own ecosystem** with our proprietary token solution.

outpayce from AMADEUS | Travel. Simply paid.

Ready to step up your payments security? **The journey starts now.**

Outpayce's Tokenization solution is built by travel experts for today's travel leaders. With our in-depth knowledge of the airline industry, you can be confident your unique payment complexities, challenges and risks are covered.

Contact us



About Outpayce

Outpayce delivers smoother end-to-end travel experiences by making travel payments simple. Our open platform connects FinTech and banking service providers to the entire travel ecosystem, allowing customers and travelers to easily benefit from new advances in payments.