outpayce
from amadeus

Security in travel payments: the hidden differentiator

Read the report

Foreword

Payments has always been about achieving the right balance between security and convenience. If controls are too onerous there's a chance that legitimate purchases could be abandoned. If security controls are too loose then the company may face significant costs arising from fraud.

There are very tangible reasons that travel companies should make payments security a priority. From regulatory compliance to enabling commerce, security is a necessity. But there are softer reasons too.

This report, commissioned by Outpayce from Amadeus, draws on a multi-market survey with 4,500 travelers which shows that our industry's customers are increasingly security conscious and have come to expect high levels of security from their travel provider. Concerningly, 64% of respondents to our survey said they perceive rates of payments fraud to be increasing and 35% said they do not currently trust travel companies to keep their payments data secure, which is higher than almost every other sector of the economy.

Rates of fraud continue to grow across the entire economy, but travel is known to be a particular target. There are very few high value services you can buy months before the service is due to be delivered. In travel, fraud can take place at any point from booking until disembarking.

But those travel companies that get security right are likely to be rewarded. Our research suggests travelers are willing to save their payment details online with companies they trust to enable frictionless payments. On average, they would also prefer to pay a significant price premium for this security, rather than book with a provider that has not invested in these capabilities. 72% say a travel company's strong reputation for cyber security would encourage them to choose that firm over another provider with a less favorable reputation. An investment in security is an investment in differentiation and your company's reputation.

It is encouraging to note that the introduction of Strong Customer Authentication (SCA) across the economy in Europe appears to have reduced payments fraud. The European Banking Association's recent analysis found that payment card fraud has now dropped to €29 in every €1,000. At Outpayce, we have worked tirelessly alongside our customers to help them prepare for the introduction of SCA.

Yet there is significantly more work to do, and payments security is a continually evolving game of cat and mouse. I hope this report provides useful insights that help to elevate this important issue within your travel business.

Jean-Christophe Lacour
SVP & Global Head of Product & Delivery
Outpayce from Amadeus

Travel is a target

Travel companies face a growing range of cyber security risks, many of which relate directly to payments. Travel is a particular target for bad actors seeking to use someone else's payment details, often to buy high value airline tickets, before claiming a refund or using the service.

The industry also holds data on travelers ranging from personally identifiable name and address details through to highly regulated payment card data. This means travel companies are also a target for malicious actors that seek to breach company systems to steal such data at scale.

Both problems are the subject of stringent regulation designed to ensure companies take positive action to limit fraud and data loss. Remaining compliant and ensuring the company's approach to payments provides high levels of security requires attention, skilled teams and advanced technology.

However, this work can pay dividends. According to our survey with 4,500 travelers, the vast majority say a travel company's strong reputation for cyber security would encourage them to choose that firm. Similarly, when asked whether they prioritize 'security' or 'convenience' when making payments, the balance was skewed 59% to 13% in favor of security on a net basis.

> A travel company's strong reputation for cyber security would encourage travelers to choose that firm.

Data breaches

Data breaches occur when a hacker successfully penetrates a company's systems and manages to steal data. Security company Gemalto published a detailed index of every public cyber breach globally until the company was acquired in 2019.

In the first half of 2018, the index recorded that **more than 3.3 billion records had been compromised**, representing a **72% rise** on the first half of 2017.

Subsequent reports show this trend accelerating, with **security company IT Governance's** dashboards suggesting more than 26 billion records were compromised in January 2024 alone. This huge number was driven by MOAB (The Mother of All Breaches), which impacted many companies and governments.

Unfortunately, data theft and sale occurs at an industrial scale with people's 'identity data', like usernames and passwords, often sold by the thousand on the dark web.

Some types of data are more sensitive than others. Payment card data is particularly sensitive given that a person's 16-digit card number can be used to initiate a purchase. That's why PCI-DSS or the Payment Card Industry Data Security Standard was introduced to ensure companies that store or transfer payment card data meet specific data security standards.

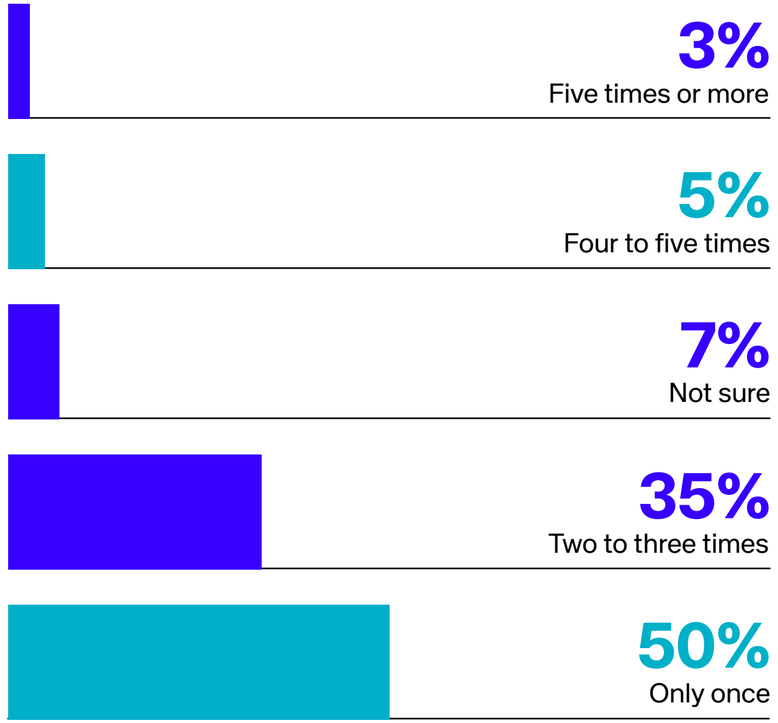
According to our survey with travelers, more than half of respondents have been the victim of payments fraud, where their card details were stolen and used to make purchases. **For those who have been a victim of payments fraud, it has often happened more than once.**

While someone's card details can be stolen in a number of ways, malign actors increasingly focus their efforts on data breaches where many thousands or even millions of customer records can be compromised in a single attack.

Like retail, many companies in travel handle customer card details and must comply with PCI-DSS. Indeed, with more travel companies deciding to become the Merchant of Record and assume responsibility for processing payments, this number is increasing.

The travel industry has witnessed its fair share of data breaches in the recent past, some of which have resulted in significant fines. Yet the damage caused by such incidents extends beyond financial penalties and can seriously impact travelers as well as negatively impacting company reputation.

Number of times individuals have been victim of payment fraud:



Impact a cyber breach has on perception of travel company:

Would question their cyber security capabilities

Would question their overall competence (including safety)

Wouldn't be willing to store their payment details with the company

In fact, 68% of respondents to our survey confirmed that if a travel company suffered a breach, it would negatively impact their perception of the company, 32% say significantly. Such reputational impact may extend beyond security, impacting perceptions of the company's overall competence.

Of course, travelers are only one stakeholder the industry must consider. Data breaches have also been shown to significantly impact investor sentiment too. **Work conducted by Oxford Economics and IT services firm CGI in 2017** analyzed the impact of a public data breach on the share price of listed companies in the UK.

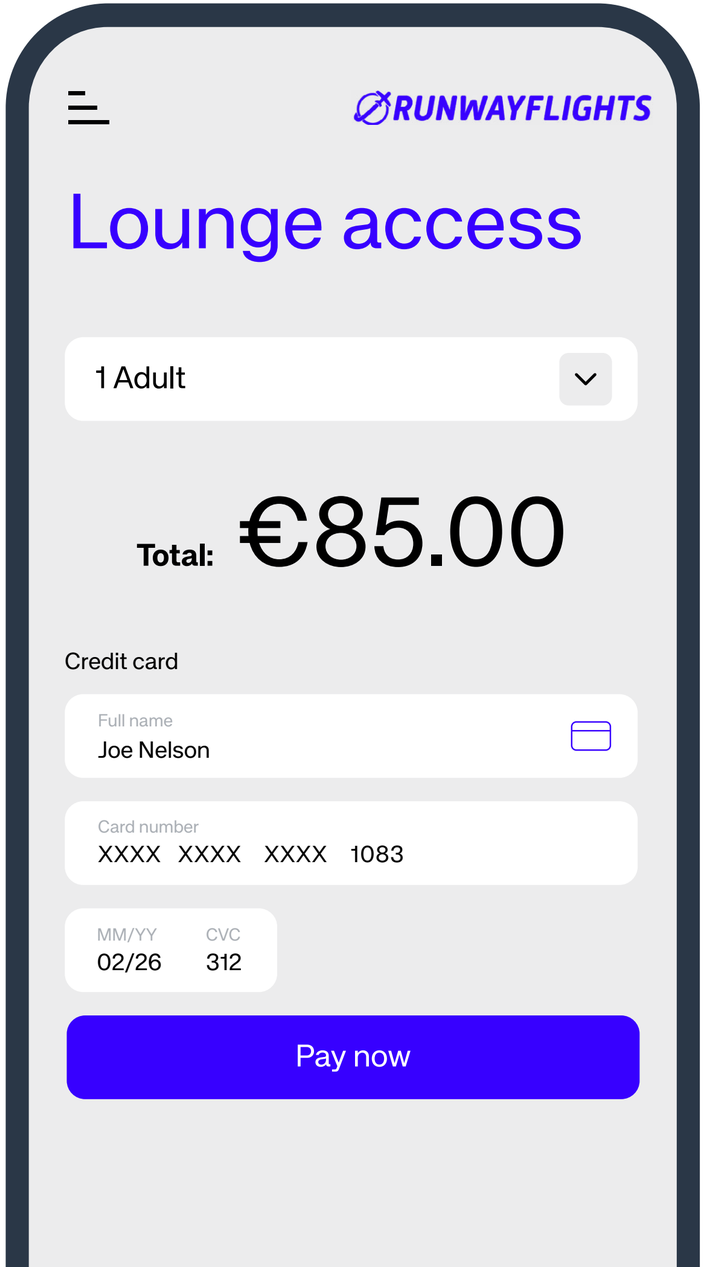
The analysis was the first of its kind, isolating the share price impact of breaches from other market-moving events. The research established and quantified the link between the share price performance of a company and cybersecurity breaches. Across the 65 companies in the sample, affected by a severe cybersecurity incident, the average long-term effect on share price was found to be 1.8%. Extrapolating that across the 65 companies in the sample resulted in an estimated loss of £42 billion for shareholders.

Reducing risk with payments tokenization

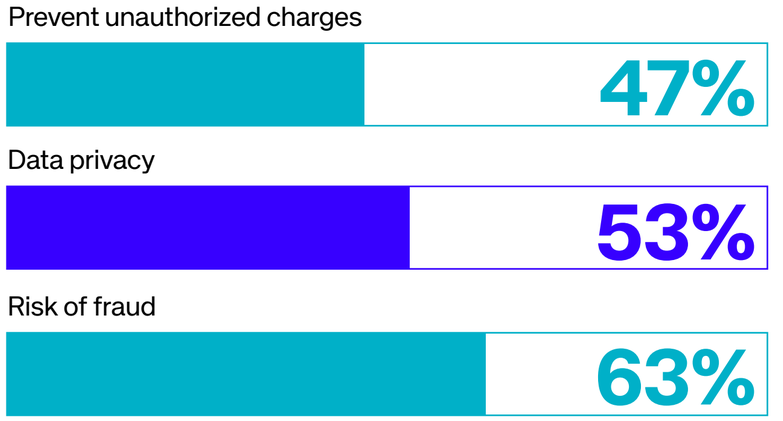
The risk of a data breach poses challenges for travel companies and other retailers seeking to deliver a simple and convenient payments experience. For travelers to pay for hotel stays, airline tickets or ancillary services with a single click, travel companies need to keep the customer's preferred payment method on file. Doing so allows the merchant to offer a much better payments experience without the traveler needing to re-key their card number each time they make a purchase.

Imagine a busy traveler wishing to add lounge access from their phone whilst taking a taxi to the airport. In this scenario, it's easy to see why a smooth payments experience is so important to travel companies. Indeed, our research with travelers found that 73% opted to save their payments details with merchants 'at least sometimes' and a third choosing to do so 'frequently'. On average, respondents to our survey have saved payment details with four different merchants in the past year.

So, how can the industry securely store payment card information whilst limiting exposure to data breaches? Tokenization is emerging as a fundamental approach that can help the industry overcome this challenge.



The main reasons people choose not to store a payment method on file:



Rather than storing the traveler's card number, a merchant can choose to replace it with a token. Card data is typically tokenized using one of three different techniques.

Non-format preserving: card data is replaced by a string of alphanumeric characters.

Format preserving: the token retains the format of the card number but scrambles the ordering of the numbers.

Masking: some of the card numbers remain the same, which can help with verification, while some others are replaced.

Importantly, tokenization is not the same as encryption. When data is encrypted, there is always the ability to decrypt the data back to its original form, typically using a private key. This isn't possible with a token, instead the original 16-digit card number is held securely within a vault.

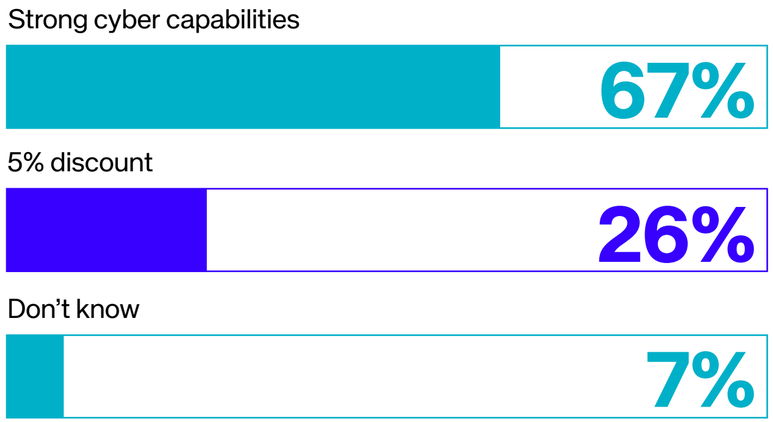
How does tokenization benefit travel companies?

The primary benefit is improved security. If the token is stolen during a breach, it's useless to the attacker and they cannot turn the token back into the traveler's card number or use it for another purchase. The decision to tokenize payment card data also reduces the PCI-DSS compliance burden. If a company tokenizes the card data it holds this effectively pushes some of the compliance burden to the specialist third-party tokenization provider, and away from the travel company. In some scenarios, the travel company doesn't have to store PCI-DSS relevant data on its own systems at all.

Our research demonstrates that consumers assign significant value to the security of their payments data. Respondents were given the hypothetical choice of flying with an airline that invested in strong cyber security capabilities or another airline that did not invest in payments security but offered a 5% discount. Two-thirds opted for security ahead of the discount, compared to 26% that preferred the cheaper option, the vast majority of which were drawn from younger age brackets.

In fact, when asked how large a discount would need to be for them to choose the airline that did not invest in security, the average response was a discount of 38%.

Percentage of travelers who would choose security over discounts:



Converting sensitive card information into a secure token also reduces the need for travelers to repeatedly enter their card details for subsequent transactions. This convenience encourages more frequent and frictionless payments, as travelers can instead complete transactions with just a few clicks. The reduction in manual data entry not only speeds up the checkout process but also minimizes the risk of errors, contributing to less failed payments and a better experience.

At Outpayce, we provide tokenization services at enormous scale to the travel industry, helping our customers to reduce risk and improve security. We are seeing growing demand from airlines of all types, but particularly from low-cost carriers (LCCs) that recognize tokenization improves compliance whilst also creating new opportunities to reduce third-party payments costs due to the added reassurance that tokenization provides.

For many travel companies that retail third-party products from other providers, like agencies or airlines, tokenization also plays a crucial behind-the-scenes role in the transfer of sensitive card data. This is done with online and offline 'walls' that act as a protective barrier between any third party that needs to transmit sensitive card data to the merchant—or vice versa. These walls intercept card data from online messages or offline files and allow the merchant to remain compliant whilst facilitating third-party sales, without the need for the traveler to complete multiple payments.

Tackling fraud in travel payments

In addition to the risk of a data breach, travel companies must also contend with increasing rates of payments fraud. In this scenario, the bad actor uses someone else's payment details to buy travel services, often with a view to claim a refund and sometimes with the intention to actually travel.

Due to its complexity, high transaction values and cross-border nature, the travel industry is a primary target for fraud. Fraud is a growing challenge for airlines, with **RSA Security and Juniper Research** finding that 46% of all fraudulent transactions occur in the airline industry and half of travel payments leaders identified fraud as their biggest challenge in Amadeus' latest **Travel Technology Investment Trends research**. Travelers are aware of the issue too, with 64% perceiving rates of payments fraud to be increasing and 32% perceiving a 'significant' increase.

46% of all fraudulent transactions occur in the airline industry

Source: RSA Security and Juniper Research

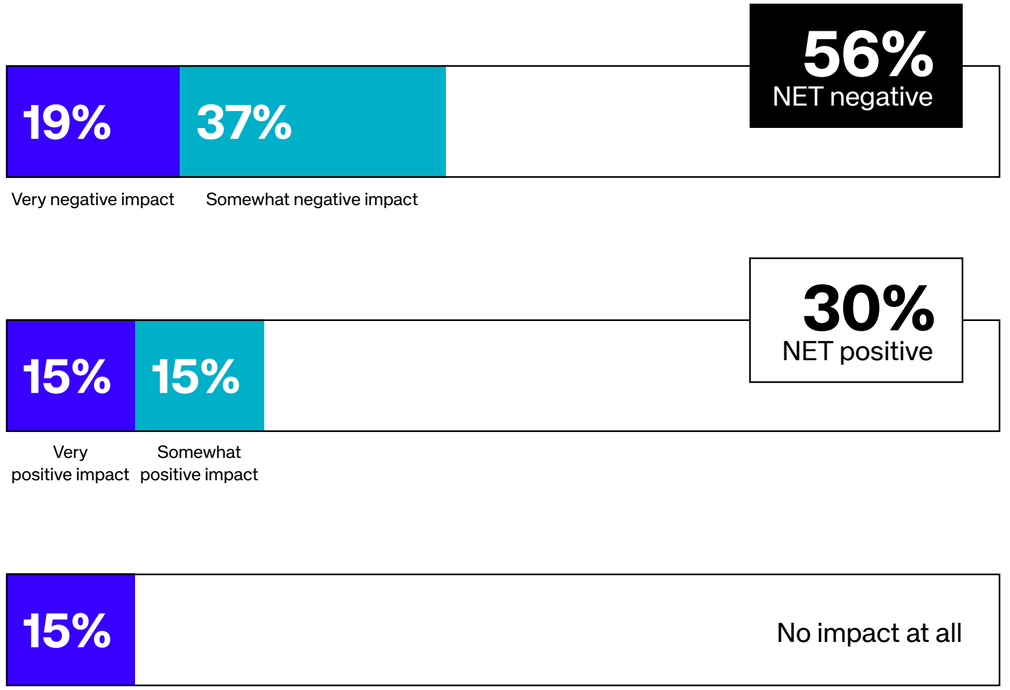
Preventing payments fraud is a constantly evolving game of cat and mouse, where fraudsters use a variety of techniques to try and make fraudulent purchases and merchants invest in evermore sophisticated technology to screen transactions and identify fraud.

Merchants are obliged to take action to prevent fraud in most parts of the world, for example under the second Payments Services Directive (PSD2) and the Payments Services Regulation (PSR). In certain circumstances, merchants can also become liable for the cost of fraud. Therefore, at first glance, it may seem sensible to set very strict rules when screening for fraud to ensure compliance and to limit any resulting liability.

The problem is that any fraud management tool which is calibrated to be too sensitive risks increasing 'false-positive' rates. That is, when a payment is incorrectly identified as fraudulent and either sent for manual investigation or declined. In our latest research with travelers, two-thirds told us they have experienced payments being declined when making a genuine travel purchase.

This can be extremely costly for the industry, lowering payments acceptance rates and ultimately resulting in lost revenue as customers abandon the purchase. There is also a frustration factor for the traveler, with over half of respondents to our survey saying it left them with a negative perception of the merchant. Interestingly, 30% said it left them with a positive perception of the travel company, perhaps because they understand it indicates an attempt to prevent fraud.

Perceived shopper impact of incorrect payment declines:



In reality though, too many false-positives suggest there is an opportunity to improve how a company approaches fraud screening. Whilst there are many products available for general retail scenarios, there are very few designed specifically for the intricacies of travel. The ability to spot fraudulent behavior requires a deep understanding about how people search for and book travel, combined with the payments and travel data assets upon which a rules-based engine and machine learning algorithms can be run.

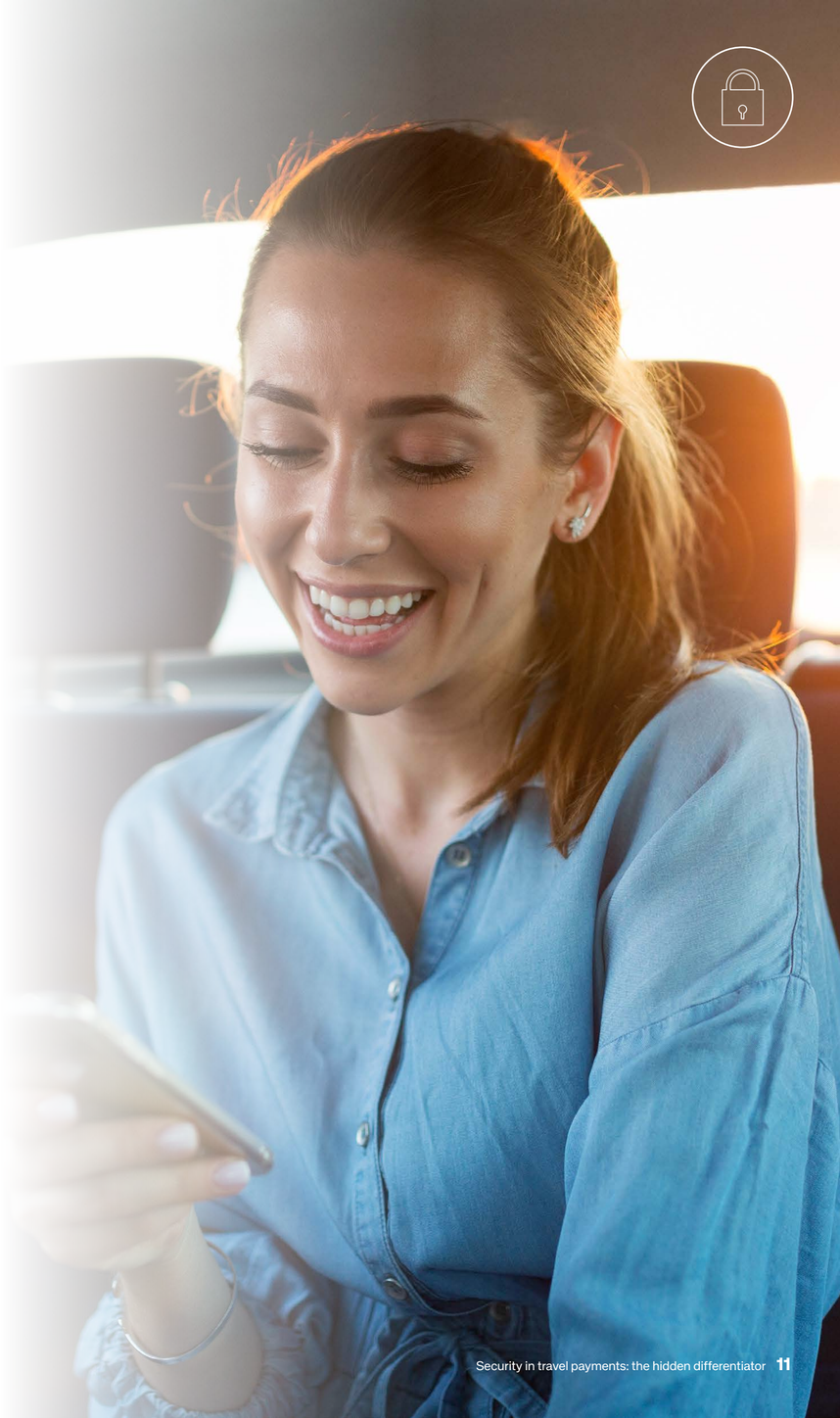
If a shopping session had the following characteristics, it would likely have a high fraud score:

- ☑ Immediately navigate to a premium flight without reviewing options
- ☑ Payment card details entered with a different pattern of keystrokes than is typical (fraud tools can remember how we tap the keys when entering our card number)
- ☑ The booking is unusual for the travel patterns of the card / card holder
- ☑ The shopping session was initiated from an IP address in a market associated with high rates of fraud

While such factors do not guarantee the transaction is fraudulent, they are likely to increase the fraud score assigned to that payment. With a deep enough understanding about what looks unusual in travel, fraud screening can stop almost all fraud. Failure to stop fraud at this early stage can result in much more costly outcomes later, for example, a rise in chargebacks issued by fraudsters.

It's for this reason that Outpayce recently entered a strategic partnership with Precision, the fraud management tool from leading OTA, Etraveli Group. Etraveli Group developed Precision based on key learnings from use across its own online travel agency brands. The advanced technology already successfully screens multibillion-dollars of transactions in more than 200 countries and is now available to the wider travel industry via Outpayce's Xchange Payments Platform.

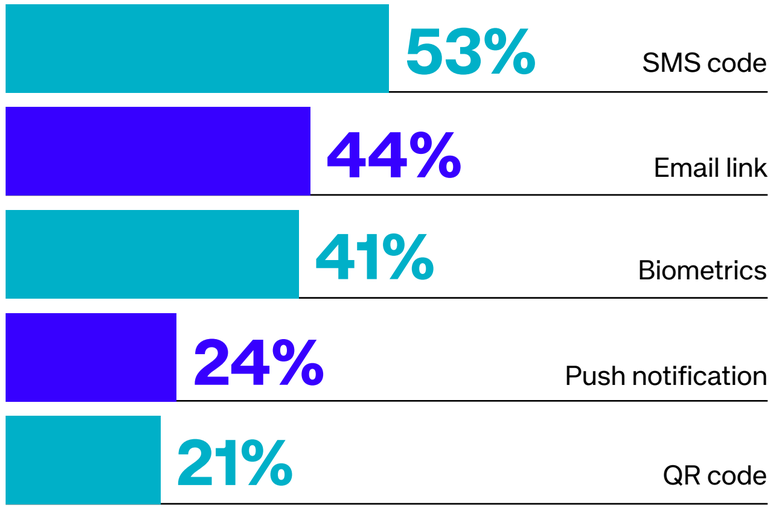
Precision screens transactions made with multiple different payment methods across web, mobile and at the call centre, in real-time so that travel companies can more accurately identify fraud. Using multiple technologies, the solution delivers a direct decision to either approve or decline a transaction or apply targeted 3D Secure Authentication, delivering a smooth payment experience for travelers by minimizing unnecessary authentication steps.

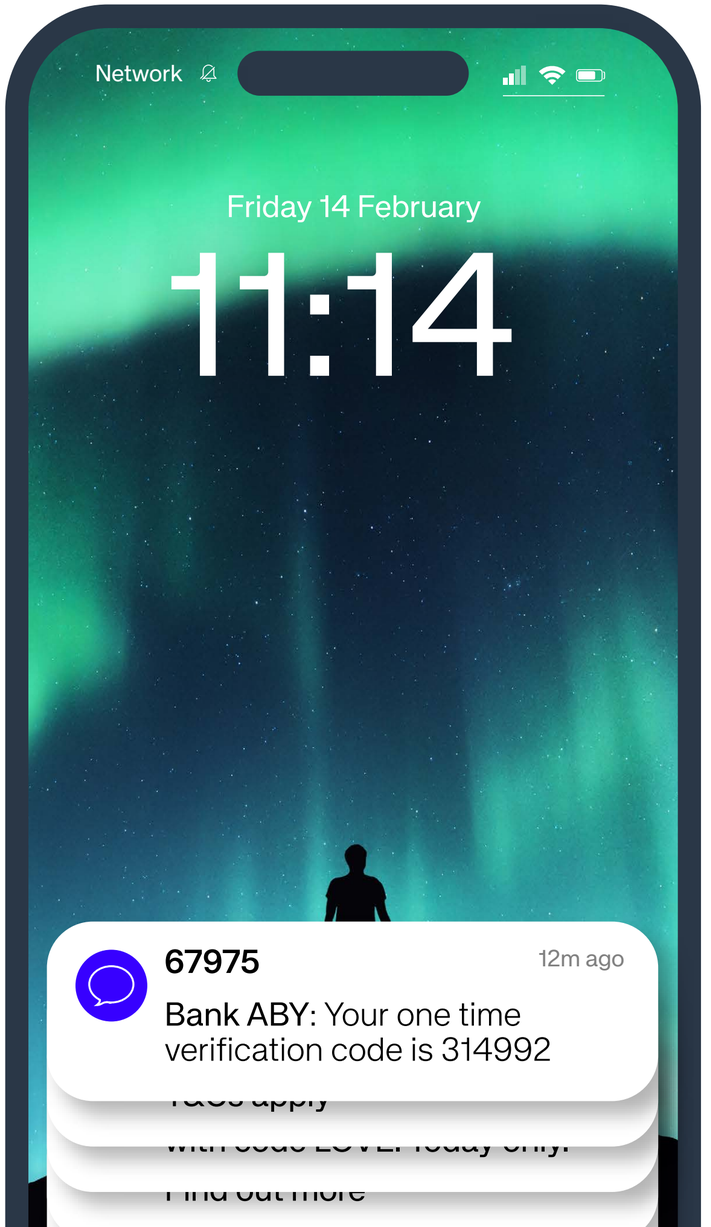


Update on strong customer authentication (SCA)

Another key tool in the fight against payment fraud is the Strong Customer Authentication check. Mandated in Europe on most high value card transactions by PSD2 regulations, SCA asks the payee to prove they are the rightful card holder by performing Two-Factor Authentication (2FA). Such checks typically involve the payee authenticating with a One Time Passcode, push notification, or perhaps with biometrics on their device.

Traveler preferences toward 2FA:





SCA came into force across Europe at the end of 2020 and has since been adopted in other parts of the world like Australia, India, Japan and Turkey, with plans for the introduction of similar requirements in the US market soon.

According to our survey with travelers, 85% have been asked to perform 2FA when buying travel with the majority confirming the 2FA process was easy last time they bought travel.

However, 48% have abandoned a travel purchase when asked to perform 2FA, which is higher than any other type of purchase.

Payments friction resulting from the introduction of this additional authentication measure remains a key concern across the industry, with travel merchants seeking to apply SCA exemptions where legitimately possible, and where their fraud management system provides the confidence to do so.

Outpayce has been working to support the introduction of SCA across travel in several ways, including making a significant contribution to EMVCo's* 3DS data exchange standard for specific travel use cases.

Today, merchant customers access 3DS 2 Travel, a specially designed authentication system, via the Outpayce platform. 3DS 2 Travel collects and sends more than 100 different payments and travel data points to help card issuers form a more complete judgement about whether the payee is the legitimate card holder, which in turn allows more transactions to be authenticated in the background, without the need for the traveler to perform 2FA.

*EMVCo is a company owned by Visa that sets industry standards for card payments.

outpayce from amadeus

Payments security as a business enabler

Many travel companies, like airlines, are increasingly focused on becoming effective retailers and growing their business across new geographies while selling new types of services. Payments plays a crucial role in the retailing transition, helping travel companies to convert more sales and create value in new ways.

An effective approach to payments security that prevents fraud and reduces risk is a fundamental enabler to digital retailing. It can provide the business confidence to sell and operate in regions of the world where fraud is high. It protects the brand from the significant risks associated with data breaches. It helps a travel company to accept more legitimate business, reducing traveler frustration from false-positive declines.

Perhaps most importantly, as this research demonstrates, security is now a concern for consumers. Taking a proactive stance helps travel companies to build trust, encouraging more travelers to store their payment methods, opening the door to a one-click payments experience.

About the research

The survey was conducted by independent research firm Opinium during Q4 2024 with 4,500 travelers from France, Germany, Singapore, the United Kingdom and the United States.

outpayce from amadeus

outpayce

from AMADEUS