# PayPal

The pressing impact of fraud on the travel industry

After a challenging few years, Europe's travel industry is finally on a strong recovery trail. Intra-European travel has increased by 250% since the pandemic, and summer holiday bookings are also on the rise.[1]

But underscoring this optimism, businesses in the travel sector continue to be challenged by the ever increasing threat of fraud.

Let us examine the impact fraud has had on the travel landscape so far and explore how travel operators can safeguard themselves.
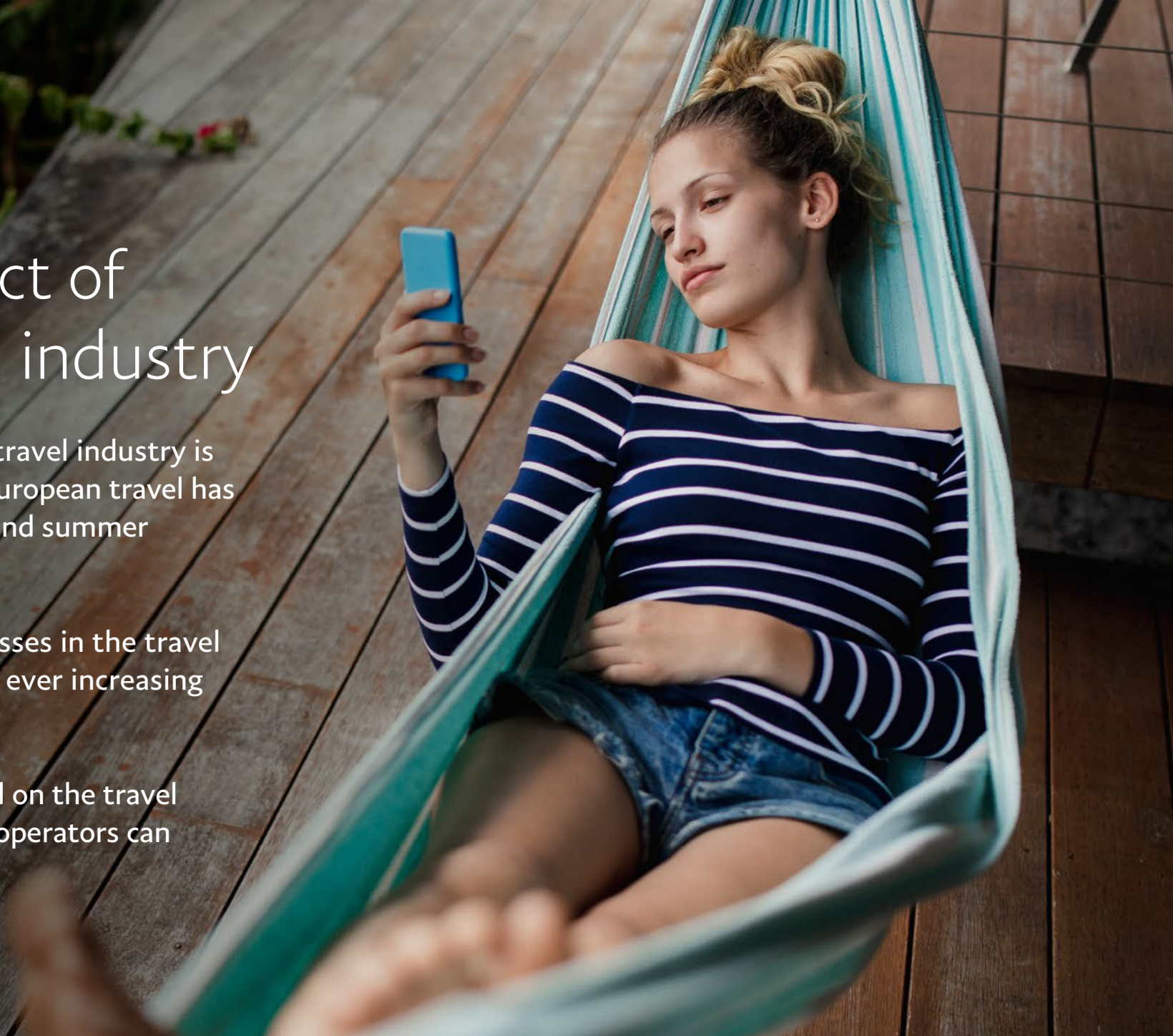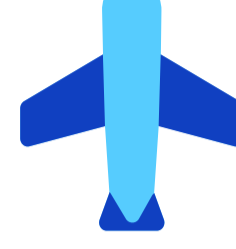

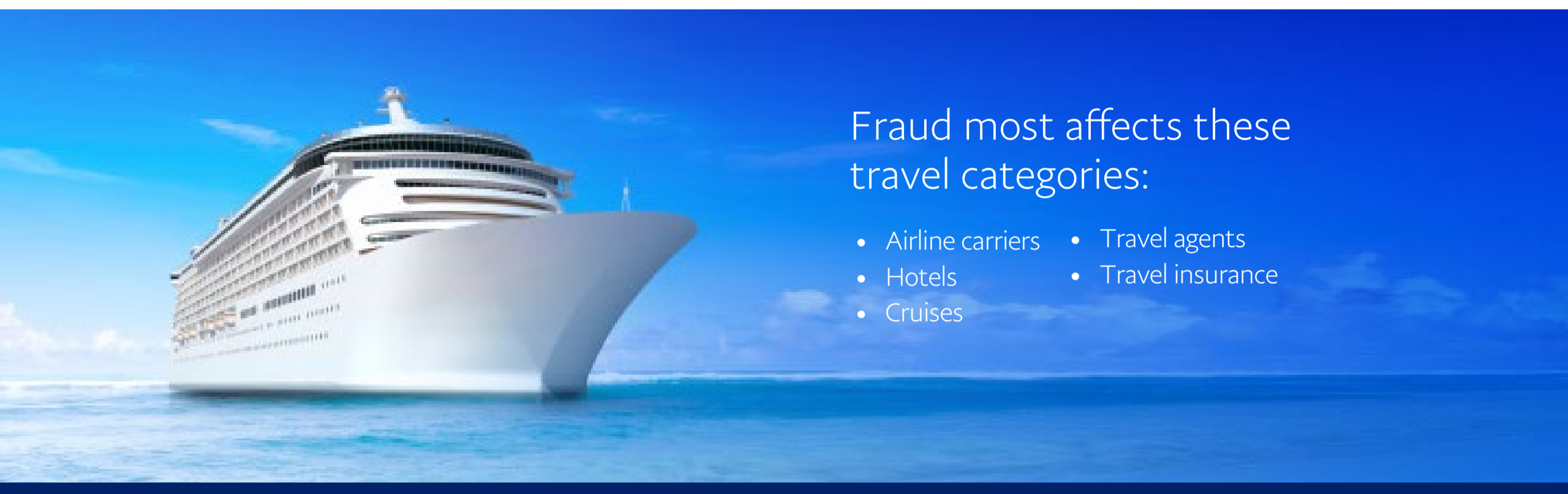## The travel industry is the second-most fraud-prone sector after retail.[2]

On average, hotels lose **5-6%** of their annual revenue to fraud.[3]

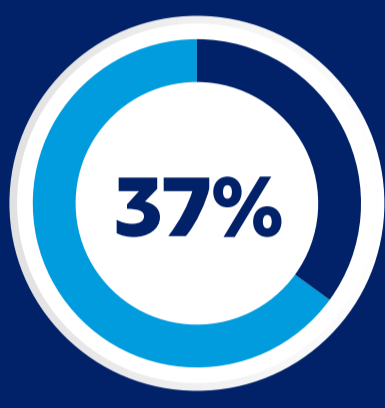In 2021, travel and leisure industry fraud rates soared to **155.9%.**[4]

Fraud costs the International Air Transport Association (IATA) **US$858M a year.**[5]

Fraud most affects these travel categories:

- Airline carriers
- Hotels
- Cruises
- Travel agents
- Travel insurance

37%

Major airlines are targeted **37%** more than lower-cost carriers.[6]

Credit card fraud

One third of all credit card fraud cases come through the hotel industry. These can be perpetrated by employees, guests or third-party vendors.

Common credit card fraud schemes include false account credits, use of skimming devices and fraudulent credit cards.

Data breaches

Several high profile data breaches have shaken the travel industry in the past few years. Such cyberattacks can lead to loss of reputation and consumer trust, as well as hefty fines from information rights organisations.[8]

Staggering amounts of client information are leaked during a data breach, from personal details to payment data.

Booking frauds

Holiday booking fraud has increased for both travel companies and consumers since 2020.[9]

Fake booking websites, bogus travel agents and active false marketing has become more sophisticated, making this type of fraud harder to detect.[9]

---
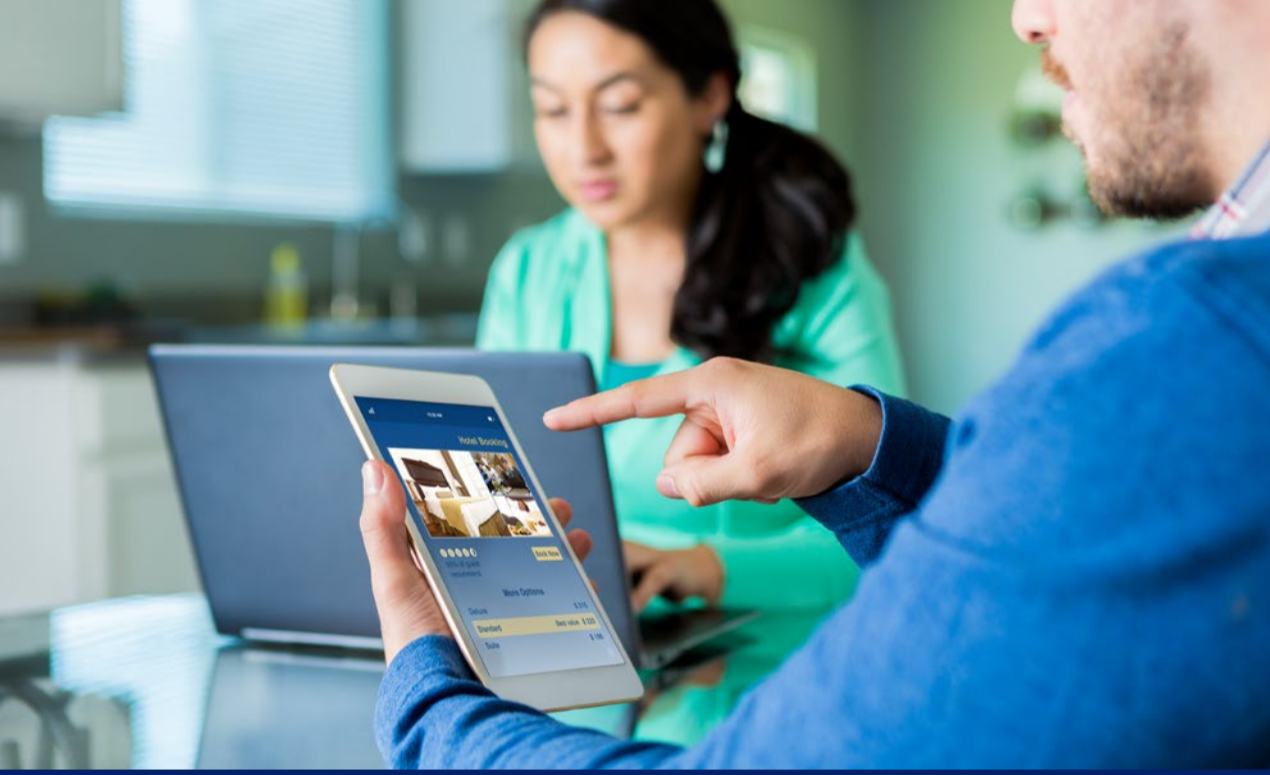
2 ways to minimise fraud in the travel sector

1. Improve cybersecurity measures

Routinely ensure your operating systems are updated. Strong firewalls, data backup practices, anti-malware software and ad-blockers should be enforced.

Employees across the organisation should also undergo training to ensure they are able to detect and avoid phishing.

2. Choose the right payments partner

The right payments partner can help you manage risk and security challenges to mitigate fraud. PayPal's proprietary mix of data, models and tools help keep your business and consumers safe.

Our security measures are:

Available 24/7, with real-time transaction monitoring

Compliant with national and international laws

Easily integrated into your e-commerce site

PayPal's fraud protection gives you insight and control to help minimise chargebacks and fraudulent activity. We combine extensive intelligence from our two-sided network with advanced machine learning and analytics to adapt as your business and fraud evolve.

With PayPal, payments are processed more securely and successfully.

Dynamic routing, retries, and granular data analysis enable legitimate transactions to be approved at a higher rate and more often on the first try.[9] You can also test and deploy rules in real-time, adapting to fraud patterns as they evolve, without creating friction at checkout.

Find out how PayPal can help grow and protect your business.

[Find out more]

---

[1] Schengen Visa Info, 'WTTC Foresees Strong Recovery of European Travel & Tourism in 2022', 21 January 2022
[2] WEX Inc, 'Travel Industry One Of Most Targeted For Fraud', 20 May 2019.
[3] Bender LLP, 'Is The Hospitality Industry Revisos, Expect Fraud To Follow, 7 January 2021.
[4] CNBC, 'Cyberfraud shifts to gaming, travel and leisure, report finds', 11 August 2021.
[5] SIfL 'Fraud in the Travel Industry', 29 January 2018.
[6] Travelpulse, 'Tips for Avoiding July 4 Travel Fraud', 24 June 2019.
[7] Data Breach Lawyers, 'Travel industry data breaches', 21 June 2021.
[8] ITIJ, 'Preventing and detecting travel insurance fraud', 5 October 2021.
[9] PayPal Internal Data, June 2019. Methodology: Benchmarked against MasterCard auth data set for the month of June 2019. There is no de-duplication for any of the numbers (removing duplicates will give us higher auth rates in the range of 95%+)