Airwallex

Digital trust in online payments

Elliot Colquhoun
VP, IT & Security, Airwallex

Balancing convenience, customer experience, and payment security in online transactions

Trust, it turns out, is the silent deal-breaker or deal-maker in online transactions. While customers expect secure, seamless payments as a baseline, they also gravitate toward brands that signal credibility and reliability from the first click to final checkout. That expectation flows both ways – businesses, in turn, need to choose payment providers they can trust to deliver on those promises.

In fact, when selecting a global payment solution, businesses across markets consistently rank trust as a top priority[1]. After all, every glitch or security lapse reflects directly on the business itself. To earn and keep customer trust, businesses must first place their trust in the infrastructure powering every transaction behind the scenes.

What digital trust means – and why it varies around the world

Digital trust means different things to different people. For consumers, it might be the confidence that their credit card details won't be stolen during checkout. For businesses, it could be the assurance that a payment platform they use won't crash during a major sales event.

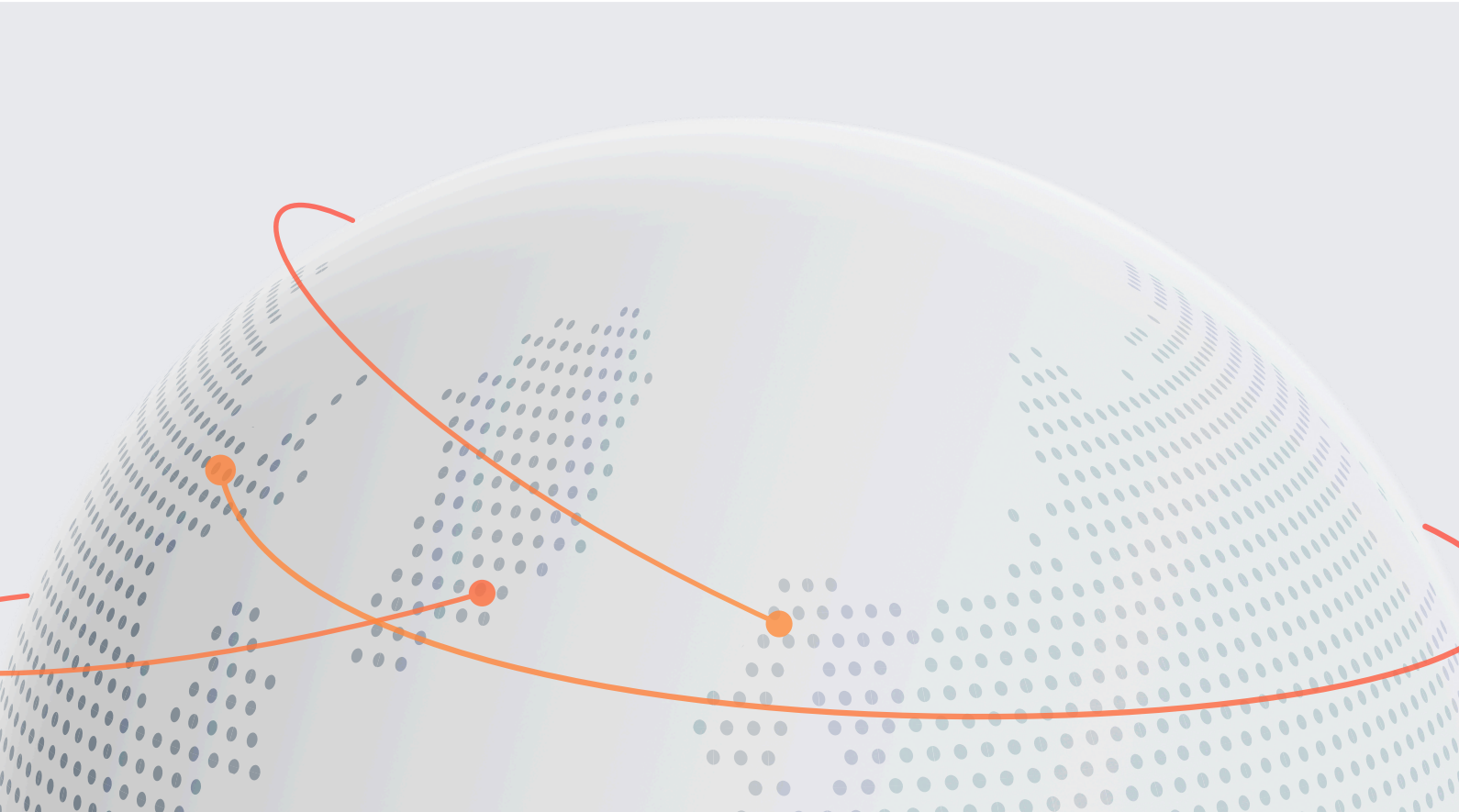
At its core, digital trust is about creating a foundation of confidence that underpins every online interaction customers have with a brand.

This happens through the proactive protection of sensitive data, ensuring reliability and consistency, so that every payment, every login, and every online transaction works seamlessly and without disruption. It's not just about preventing problems; it's about making sure customers never have to think about them at all.

What builds that trust, however, varies depending on where people are in the world. In the EU, stringent data privacy regulations like the General Data Protection Regulation (GDPR) have raised public awareness and expectations around how companies store and use personal data. Consumers are increasingly asking tough questions, and businesses are expected to offer transparency and control over personal information.

In the US, while privacy rules are more fragmented, trust is often established through third-party certifications and independent security audits – signals that demonstrate accountability and adherence to best practices. Meanwhile, in markets across Asia-Pacific, the rapid adoption of mobile and digital technologies has placed a premium on speed, uptime, and secure real-time transactions.

These differences reflect broader trends in regulation, cultural expectations, and technological maturity. Yet across all markets, one thing remains constant: digital trust is the foundation of every successful online transaction.

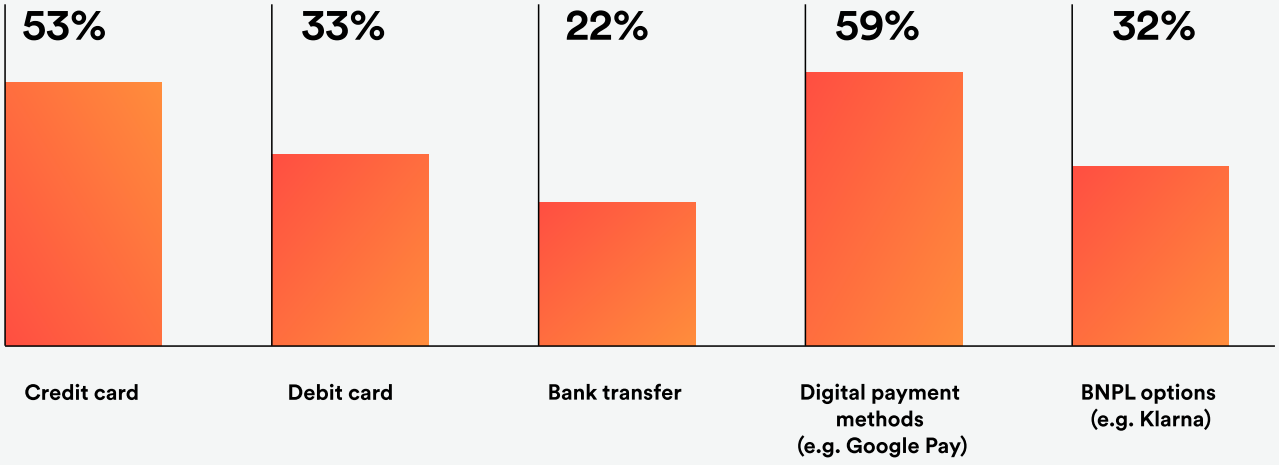


Payments are getting smarter, but more complex to trust

When it comes to trust in online payments, the stakes are especially high. Payments are often the most sensitive and high-risk part of any digital experience – where a single failure can mean lost revenue, broken customer confidence, or even reputational damage.

The challenge today is compounded by the sheer number of payment methods consumers now expect to use – credit and debit cards, digital wallets, bank transfers, buy now, pay later options, and more. Digital payments like Apple Pay and PayPal have almost become the world's default payment methods, with 59% of global consumers now regularly using them for online purchases.

Preferred payment methods when buying online from another country



But preferences aren't uniform across generations. The internet-savvy use digital wallets often and are comfortable with local payment methods. Others rely on physical credit cards, while some are still wary of online transactions in general. 68% of Gen Z and Millennials prefer digital payment methods like digital wallets, while 57% of Baby Boomers instead use credit cards regularly. Younger customers are more likely to use alternative options like Buy Now Pay Later (BNPL), with 41% of Gen Z and Millennials choosing these services[2].

No matter which payment method a customer chooses for an online transaction, from the consumer's perspective, the experience is the same. You're just paying someone money, right?

But the underlying way the payment is made, how the validation occurs, and what transaction type it is, is completely different. What feels familiar to one group may require very different controls behind the scenes. A biometric tap through Apple Pay is processed very differently to a card-not-present transaction through a browser. QR-code payments involve yet another model altogether. Each of these payment types adds layers of complexity, and businesses must ensure that every method works securely, instantly, and without error.

Global losses from online payment fraud are projected to exceed US$343 billion by 2027[3].

Juniper research projected global losses from online payment fraud to exceed US$343 billion by 2027[3]. But we're at a pivotal moment of innovation in online payments. There's an opportunity for businesses to harness new tools and technologies to stay ahead. So while consumers trust businesses to handle their transactions securely, businesses must find payment providers they trust to not let them down.

The business case for prioritising payment security

Businesses understand that the risks of choosing the wrong provider go beyond lost transactions. Trust is a fragile thing in online payments. Businesses invest heavily in attracting customers, improving conversion rates, and expanding into new markets, but all of that effort can be undone in an instant if customers don't feel safe when making a payment. Security failures, even minor ones, can have lasting consequences. A single instance of fraud, a vague security policy, or an unreliable payment experience is enough to make customers hesitate.

"Building trust with consumers is crucial to increasing customer conversion, especially as businesses are looking to grow in new markets around the world. If customers do not have full trust in your website/app or the goods/services they are looking at, they will be quick to abandon their purchase intentions."

Ivo Jenni
Product Director, Payments Platform, Airwallex

Your payment provider is now part of your brand

Every part of the online payment experience influences how customers perceive your brand. From authentication to fraud detection, cross-border transfers to chargeback handling, every touchpoint must function seamlessly and feel secure. Customers shouldn't have to question whether their money is safe or if a transaction will go through.

Trust is earned in those moments – and once lost, it can be hard to win back. Much of this trust depends not just on your business itself, but on the reliability of your payment processor, technology stack, and even the resilience of your wider supply chain.

Every part of your webstore's customer experience forms a part of your brand – including your checkout page and payments providers. From a consumer perspective, if the checkout page feels insecure, they're not going to think that the payment provider is insecure – it will directly reflect on your brand and they'll find another merchant. You have to consider your payment provider as a core part of your customer experience, who can help you build trust with your customers, and ultimately win sales.

This means looking beyond compliance certifications and asking critical questions. What fraud detection tools are in place? Does the customer experience feel secure? How quickly can the provider respond to a security threat?

A provider that doesn't innovate against emerging cyber attacks will leave your business exposed. If they don't instil confidence in customers, they're undermining your overall security.

From a consumer perspective, if the checkout page feels insecure, they're not going to think that the payment provider is insecure – it will directly reflect on your brand.

Our research shows that across markets, trust is the number one factor businesses consider when choosing a payments provider. Price and product features matter, but neither carries as much weight as confidence in the provider's ability to secure transactions, protect data, and respond quickly when issues arise. In many cases, trust isn't just a conscious choice – it's an unconscious bias shaped by everything from brand familiarity to perceived credibility. Businesses are more likely to lean toward providers they instinctively feel are reliable, even before diving into the fine print.

Elliot Colquhoun
VP of IT & Security, Airwallex

40%

of consumers stopped doing business with a company after learning it had failed to protect customer data[4].

53%

of consumers only purchase after confirming a company has a reputation for protecting customer data[4].

10%+

annual revenue growth for companies with strong digital trust framework[4].

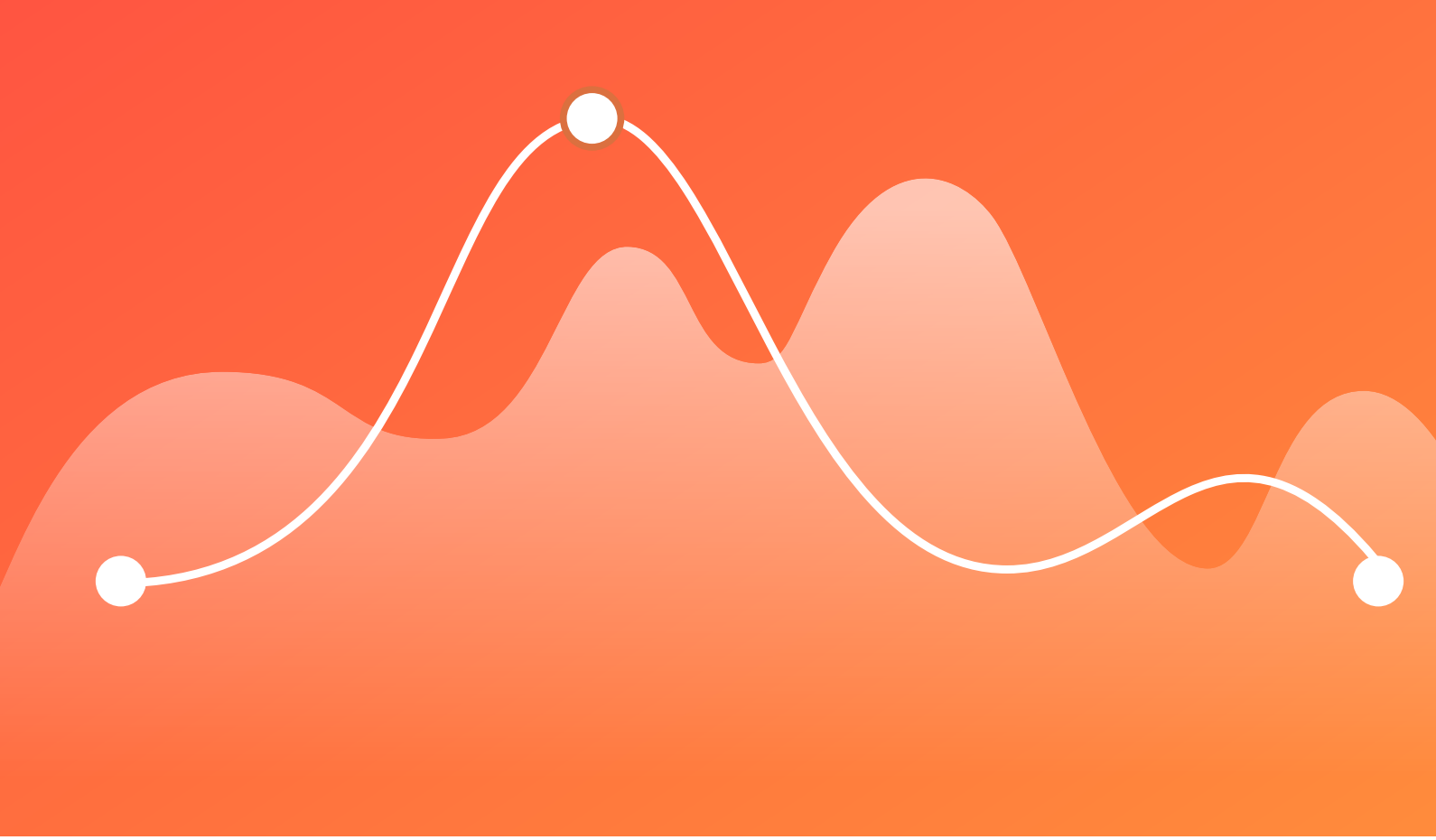
How digital trust fuels business growth

Customers rarely return to a business after a security failure, making trust one of the most valuable yet vulnerable aspects of online payments. The brands that succeed are those that proactively address security concerns before customers ever have to question them.

Investing in payment security can go a long way towards increasing customer confidence, improving conversion rates, and strengthening brand loyalty. While trust in payments is primarily about compliance and operational requirements, it's also a significant driver of customer retention and business growth.

McKinsey research found that companies with strong digital trust frameworks are more likely to see annual revenue growth of at least 10%[4].

When customers see that a business takes security seriously, they're more likely to buy. Conversely, the absence of trust signals has the opposite effect. Customers who don't feel secure will hesitate, abandon their carts, or switch to competitors that provide stronger security assurances. The question is no longer whether businesses should prioritise payment security. It is whether they can afford not to.



General tips for building trust with customers

Customers need tangible proof that their payment is secure. Airwallex research found that 91% of consumers are more likely to complete a purchase when security badges are visible at checkout[2]. But trust is not built on badges alone. Customers don't analyse encryption protocols or read privacy policies before making a purchase. They judge security by how a payment experience feels. Here's how businesses should approach building digital trust with their customers:

Choose a payment provider that prioritises security

Selecting a payment provider with robust security measures is essential. Compliance certifications like PCI DSS are a starting point, but businesses must look beyond basic requirements. Fraud detection capabilities, real-time threat response, and ongoing security updates are just as important. Payment security isn't static. It must evolve to keep pace with emerging threats.

> **"Security is built into everything we do at Airwallex. Our security program allows us to build new controls, and respond to new threats, faster than other providers."**
>
> Elliot Colquhoun, VP of IT & Security, Airwallex

Embed security into the customer experience

Customers expect security, but they also expect convenience and speed. A payment process should feel reliable, consistent, and seamless, without unnecessary friction. A check out that redirects users unexpectedly or introduces unfamiliar authentication steps can cause hesitation. If a transaction doesn't feel familiar or intuitive, customers may abandon their purchase.

Businesses must ensure that security measures enhance the customer experience rather than disrupt it. Features like biometric authentication, tokenization, and real-time risk assessment improve security without adding friction. The most effective controls are those that operate in the background, keeping transactions safe without interfering with usability.

> **"User experience is incredibly important to our customers, to be able to build trust with theirs. With Airwallex, you're able to define what the user experience for payments looks like – whether using redirects, embedding our components, or integrating directly via our API."**
>
> Elliot Colquhoun, VP of IT & Security, Airwallex

Conduct regular security reviews

Compliance with industry regulations is essential, but it doesn't guarantee that a payment system is fully secure. Fraud tactics evolve quickly, making it critical for businesses to conduct regular security audits to identify vulnerabilities before they can be exploited.

External security reviews provide an independent assessment of a business's security posture. Trusted third-party audits, penetration testing, and ongoing fraud analysis can help businesses ensure that their security systems remain resilient and adaptable.

> **"It's beneficial to obtain an independent review of your security setup. These reviews help ensure that your integration doesn't inadvertently introduce vulnerabilities to your platform. We've also found value in asking our customers for their perception of our security, to ensure our brand matches the quality of our security controls."**
>
> Elliot Colquhoun, VP of IT & Security, Airwallex

The next phase of digital trust in payments

Digital trust won't be defined by whether a business has security frameworks in place but by how well those measures evolve against emerging threats.

AI is making fraud tactics more scalable and cost-effective. As automation lowers barriers to cybercrime, security teams face increasing pressure to develop defences that aren't only effective but also economically viable. Staying ahead requires investment in real-time threat detection, adaptive fraud prevention, and security strategies that evolve as quickly as the threats themselves.

Traditional rule-based fraud detection is no longer enough. Businesses that rely on outdated fraud prevention models will struggle to keep up.

Outdated systems leave financial companies exposed, unable to keep pace with the speed and sophistication of today's cyber threats. Legacy infrastructure often lacks the agility to implement advanced fraud detection, respond to compliance changes, or patch vulnerabilities quickly. Meanwhile, attacks are becoming faster, more targeted, and cheaper to launch.

Without the ability to adapt in real-time, businesses risk falling behind – and losing the trust of their customers. Maintaining digital trust requires a modern security framework: one that can evolve rapidly, scale effectively, and respond decisively to emerging risks.

Payment providers and merchants need adaptive security models that use machine learning, real-time behavioural analytics, and biometric authentication to detect threats before they cause damage.

This is where modern fintech providers have the edge. Their infrastructure is purpose-built to respond at speed, with the flexibility to launch new controls and close vulnerabilities quickly. With continuous monitoring, frequent updates, and a tech-first approach to global compliance, they offer the kind of proactive protection that traditional systems simply can't match.

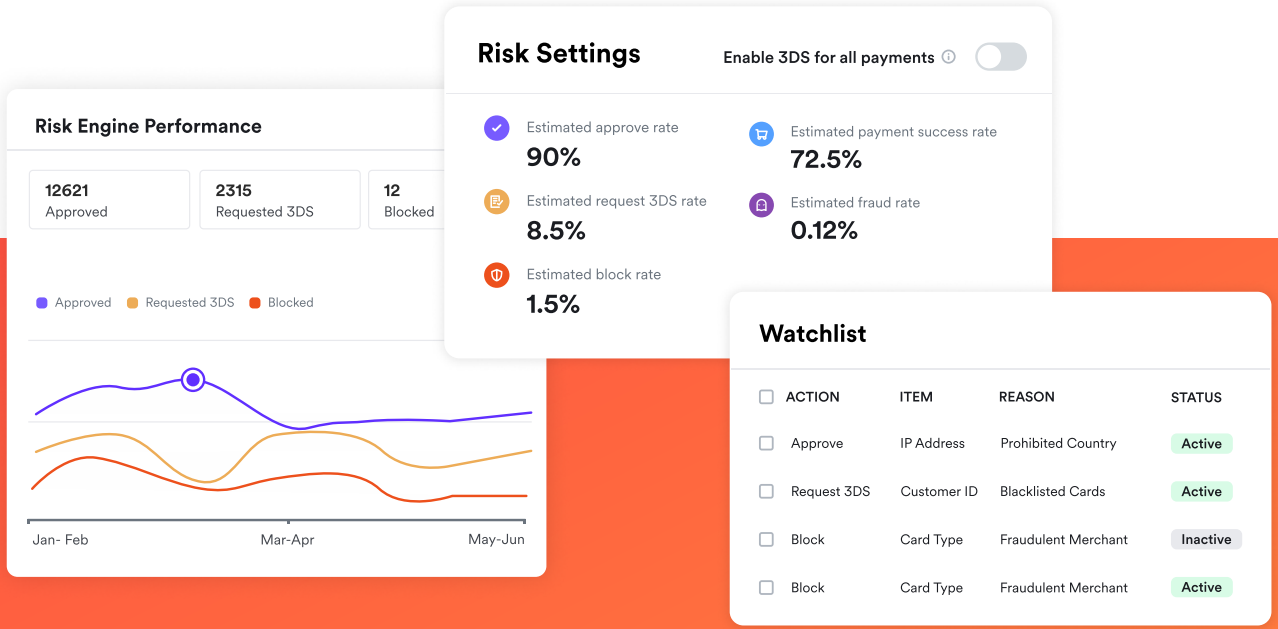
Airwallex's commitment to secure online payments

At Airwallex, security is a core pillar of our product, shaping how we design, build, and maintain our payments infrastructure. Businesses trust us to move their money securely, and we earn that trust through robust security controls, regulatory compliance, and transparency.

What sets us apart is our speed and modernity. We use the latest infrastructure to deploy new controls swiftly, addressing specific regional requirements more rapidly than our competitors. This agility helps us tailor our solutions to be both responsive and compliant across different geographies.

We're ahead of the curve when it comes to regulations, which allows us to help shape industry standards. With a world-class security team backed by leadership that prioritises quick, decisive action, we're equipped to tackle emerging threats faster than traditional financial institutions.

Security is embedded into every layer of our payments infrastructure. From encryption and compliance to AI-driven fraud detection and real-time monitoring, at Airwallex, we provide businesses with the confidence they need to process payments globally without security concerns.



Sources:
1. Airwallex brand survey, Q2, 2024 (GFK An NIQ Company)
2. Airwallex Cross-border payments survey, 2025 (Statista research)
3. https://www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-343bn/
4. https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters#/