Data deep dive: enterprise merchants

Strategic goals – and how to achieve them

PayPal

An enterprise snapshot

Commerce is evolving fast, and the pressure is on. Customers expect seamless digital experiences, secure transactions, and meaningful brand interactions. Internally, teams are juggling efficiency targets, compliance requirements, and ambitious growth plans.

In this environment, having a clear view of what really matters – and where your business stands – is critical. What are your peers prioritising? Where are the gaps in your strategy? And what are the high-impact areas to focus on if you want to strengthen trust, reduce risk, and stay ahead?

Drawing on data from the PayPal e-Commerce Index, this deep dive explores the priorities of enterprise merchants, some potential challenges around those priorities, and guidance for how to solve those challenges. Read on for a focused snapshot of where to invest your energy next.

Top priorities

Priority #1 Security

51% say 'safety and security' is their priority for the year ahead

Merchants are prioritising safety above all else. Robust security measures don't just prevent losses; they build trust and create customer loyalty. Solid security can reassure customers that their data and payment details are safe, in turn driving sales.

Priority #2 Customer experience

46% are investing efforts to improve online customer experiences

Merchants are doubling down on seamless digital experiences, because smooth journeys turn browsers into buyers, and one frustrating checkout can lose a customer for good. Unfortunately, experience and security don't always play nicely together. Tighter checks can mean more friction. Too much friction, and conversion rates take a hit.

Priority #3 Loyalty

44% are focusing on online loyalty and rewards programs

Loyalty schemes are key to building long-term customer relationships, deepening engagement, and encouraging repeat purchases. The best schemes slot seamlessly into the customer journey, offering timely rewards, personalised incentives and cashback offers.

Security, experience, and loyalty are all interconnected. Want to know how to strike the right balance?

Explore how to align safety, experience, and choice in our eBook:

Do more with enterprise payments

Download Now

Security challenges

Security might top the list of priorities, but merchants report some worrying gaps in terms of customer alignment, confidence, and capability.

The first major disconnect? Merchant perception vs customer reality. Most merchants feel confident in their security posture. In fact, 83% rate themselves at least 'quite good' at protecting customer data, and 76% say the same about securing online transactions.

Unfortunately, customers don't share that confidence. Only 24% of UK consumers say they trust businesses to keep them safe online – so while you might think you're ticking all the right boxes, the people who matter most aren't convinced. And in a market where trust directly impacts sales, loyalty and brand equity, that's a problem merchants can't afford to ignore.

83%

of enterprises believe they are good at protecting customers' personal information

76%

of enterprises believe they're good at keeping online transactions secure

24%

of consumers trust UK businesses to keep them safe and secure online

Dial up on customer education

The first step to closing the trust gap is education. You can’t always show security at the point of purchase – especially when a frictionless, high-converting checkout is the goal. But proactive security alerts, clear comms around account activity, and well-timed educational nudges help customers understand the risks, and the steps you’re taking to protect them.

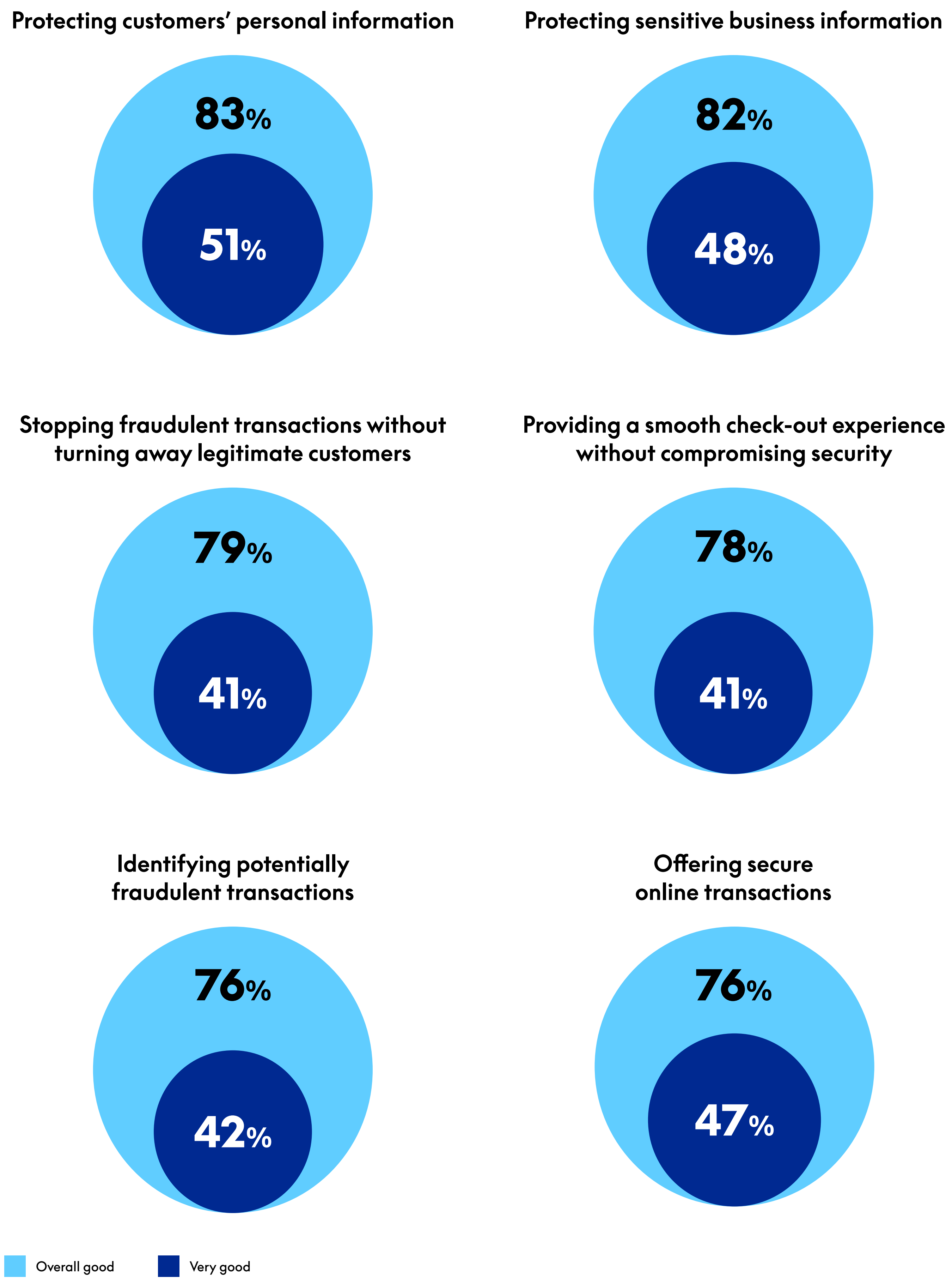
The good/great gap

The second step to genuinely improving customer perceptions? Closing the gap between doing an okay job, and a great one.

At first glance, the majority say they're doing at least a 'quite good' job across key metrics. But when we break it down further, a different picture emerges. Fewer than half rate themselves as 'very good' on key security measures like protecting sensitive business information (48%) or providing a smooth check-out experience without compromising security (41%).

This shows us that, while security is a mission critical business requirement, there's room for improvement to meet their own expectations of best practice.

How do merchants rate their security capabilities?



Protecting customers' personal information

Protecting sensitive business information

Stopping fraudulent transactions without turning away legitimate customers

Providing a smooth check-out experience without compromising security

Identifying potentially fraudulent transactions

Offering secure online transactions

How to close the good/great gap

Across the UK and Europe, merchants are required to meet strict security and privacy regulations – from GDPR and PSTI to Strong Customer Authentication (SCA). These are non-negotiable. But compliance with standards alone won't keep you ahead of threats – or truly convince your customers that your brand has security covered.

To genuinely strengthen your security posture, closing the gap between 'good enough' and 'exceptional', merchants need to go beyond the baseline. The strongest performers are embracing advanced capabilities that deliver both protection and peace of mind.

Here's what that looks like in action:

- **Predictive threat detection with machine learning:**
  Advanced algorithms now enable real-time pattern recognition and behavioural analysis. That means you can detect anomalies before they become incidents and stop fraud in its tracks.

- **Continuous monitoring, not occasional checks:**
  Real-time transaction monitoring ensures threats don't slip through the cracks. With 24/7 oversight, you can respond to suspicious activity the moment it happens, not hours later.

- **Increase authorisation rates with vaulting:**
  Vaulting enhances security by storing customer payment data using tokenisation. It ensures payment details remain current through real-time account updates, minimising declines due to expired or outdated cards – and it facilitates seamless repeat transactions, improving customer experience while safeguarding against fraud.

- **Geolocation and IP intelligence:**
  Knowing where a user logs in from, and whether it fits their usual pattern, helps catch credential stuffing, account takeovers and bot attacks early.

- **Chargeback control:**
  By using a PSP with chargeback protection and dispute automation, you can prevent fraud before it happens, reduce false declines, and fight disputes at scale. That means fewer fees, higher win rates, and more time to focus on growing your business.

The bottom line? Compliance keeps you in the game. Advanced capabilities help you do more – building customer trust, strengthening resilience, and staying one step ahead of increasingly complex threats.

Turn security into a strategic advantage

For enterprise merchants, strong security isn't just about reducing risk. It's a driver of trust, performance, and long-term value. Crucially, it protects what matters most: your customers, your reputation, and your bottom line.

But in today's sophisticated security landscape, doing the minimum won't cut it. Meeting regulatory requirements is essential, but it's only the starting point. To stand out and stay secure, you need to go beyond compliance and invest in capabilities that offer deeper protection, greater confidence, and a better customer experience.

That's where PayPal can help. Our value-added security services don't just safeguard your business – they support growth by cutting fraud losses, improving efficiency, and helping you build trust at every touchpoint.

PayPal

Ready to close the gap between good and great?

Download our latest eBook to see how to strengthen your security posture without compromising experience.

Download Now