2025 ELEPHANT REPORT

Identity crisis:
The invisible barrier to global ecommerce growth

elephant

Contents

Introduction

Ecommerce businesses are missing out on a potential $47 billion revenue opportunity because of a global identity crisis[1].

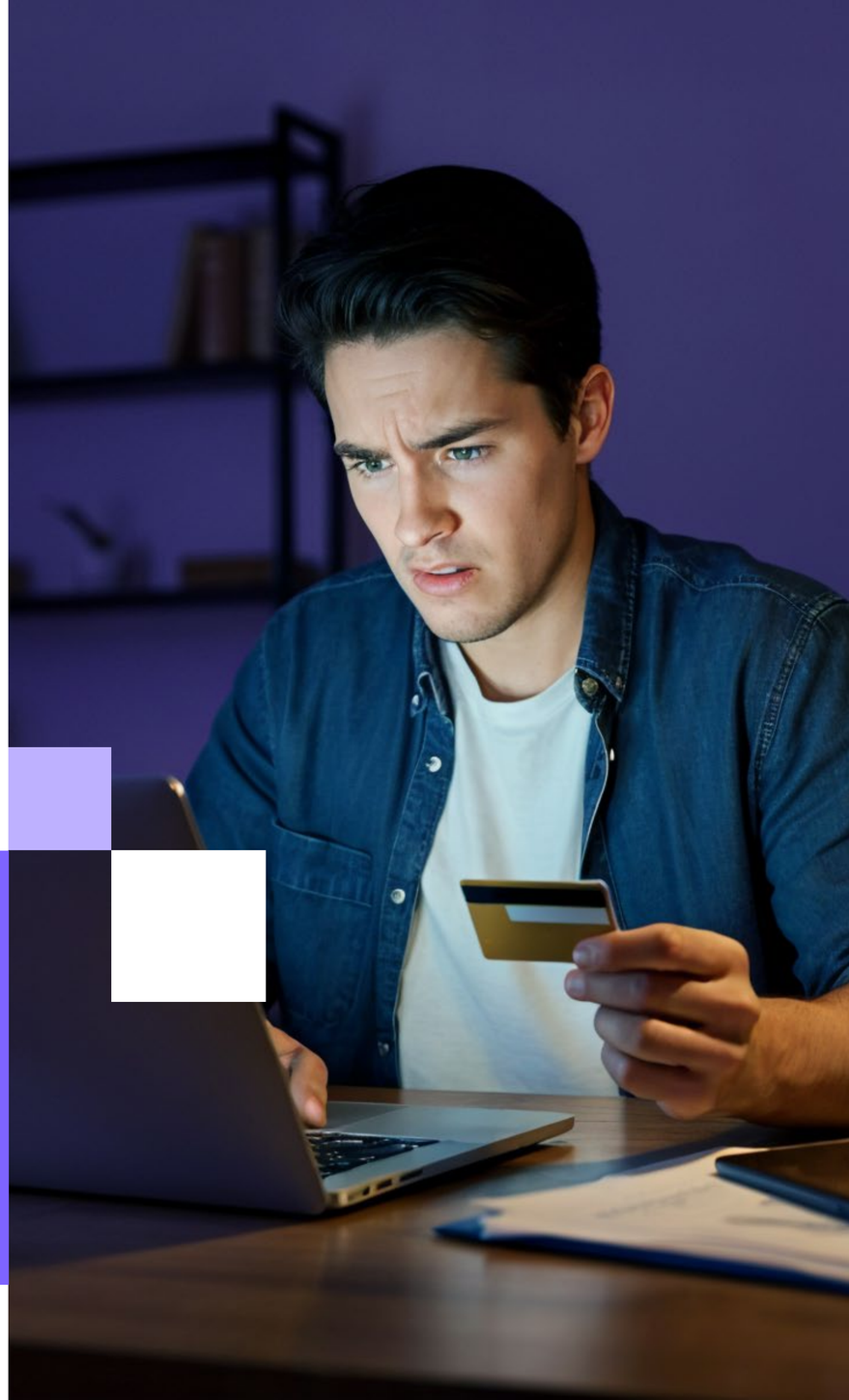
Cross-border revenue opportunities continue to grow. Worldwide ecommerce sales reached $5.6 trillion in 2023 and are projected to exceed $7.5 trillion by 2027. In many markets, ecommerce now accounts for more than 20% of total retail sales. But while consumer demand is rising, global scale is stalling because platforms don't have the tools they need to trust customers across borders.

The root of the crisis is a lack of information. Most ecommerce businesses simply don't know enough about their online users to trust them. This is particularly true in high-risk, low-data visibility markets that paradoxically show the highest opportunities for growth. Without that clarity, even normal customer behavior looks unfamiliar. And when platforms can't tell the difference between customers and fraudsters, they default to decline.

The breakdown is happening on both sides of the transaction. Consumers lose faith in global platforms that misinterpret them as fraudsters. Simultaneously, businesses lose trust in their ability to expand into new markets safely. What seems like risk is often just a lack of context, which causes the trust gap to compound.

International consumers have learned to adapt. Faced with rigid checkout systems, limited shipping options, and unsupported payment methods, they find workarounds. Switching wallets, using VPNs, or rerouting deliveries. Without the identity infrastructure to support them, companies misread these behaviors, and good customers are blocked.

Businesses already lose up to $600 billion globally from false declines. But the true cost is far greater. International consumers who feel untrusted permanently switch to competitors or find local alternatives.



1. Assume 1.15% of global ecommerce revenue ($6T) is up for grabs via optimized transaction flows. Apply a conversion opportunity rate based on survey data of ~68% of users switching platforms due to friction.

To understand the scale of this identity crisis, Elephant conducted a survey of 1,000 consumers across five key ecommerce markets—the United Kingdom, Brazil, Germany, France, and Mexico—to quantify the cost of broken trust and examine how it's reshaping consumer behavior, often driving consumers away from global platforms toward more local alternatives.

For leaders navigating the challenges of cross-border scale–maintaining consumer trust at the individual level while expanding into new, diverse markets–our findings reveal that the global identity crisis is more serious than most organizations realize:

- **Nearly 70% of consumers have switched to competitors** due to transaction barriers, suggesting permanent erosion of customer lifetime value
- **Over 30% of consumers would increase purchasing by 50% or more** if retailers resolved trust barriers, representing billions in untapped revenue
- In high-growth markets like Brazil, rigid trust models are sending **1 out of every 3 consumers** to more adaptive competitors

Companies no longer need to choose between growth and security. Recognition becomes a competitive advantage. With better global identity coverage, businesses can confidently distinguish real customers from those who are unknown–reducing friction, cutting false declines, and expanding into new markets without increasing risk.

The future of global ecommerce won't be won by those who try to stop the most fraud, but by those who have the most clarity about their customers. Today's consumers aren't behaving badly; they're just not being seen. And the cost of that invisibility is billions in missed revenue.

Participants

1,000 consumers across five markets


Brazil


France


Germany


Mexico


United Kingdom

Survey discovery

Nearly 7 in 10 global consumers have switched to a competitor after hitting a transaction barrier, clear evidence that today's trust systems are failing to recognize intent at scale.

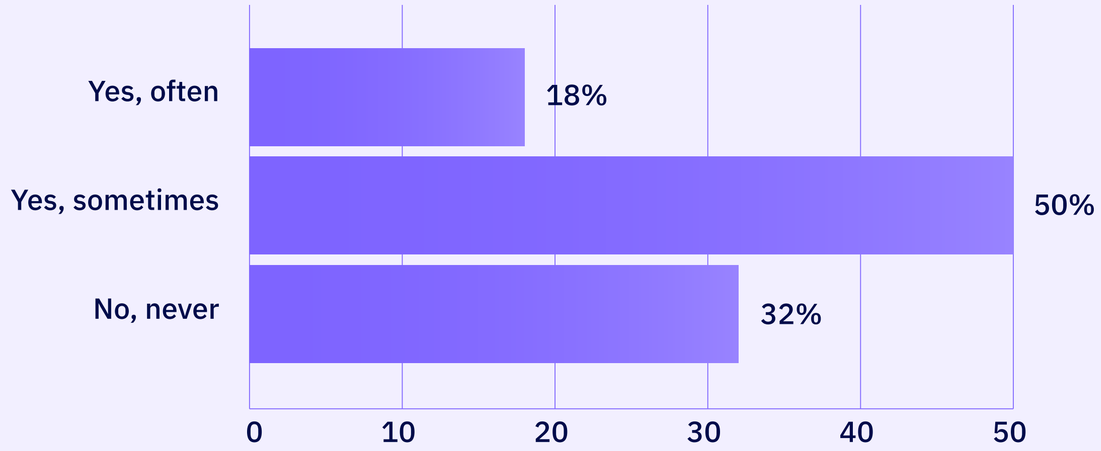
False declines cost ecommerce businesses up to $600 billion annually, but the real damage runs deeper when factoring in abandoned transactions, eroded trust, and loss of lifetime value.

To understand the impact of today's global identity gap, we asked consumers about their ecommerce experiences. **Nearly 60% reported failed purchases in the last six months due to transaction barriers, with 15% failing an alarming *five or more* times**.

The immediate revenue loss from this is damaging, but the long-term impact may be devastating.

When platforms lack the identity data to recognize who a customer is, they struggle to interpret behavior in context, leading to broken experiences, broken trust, and severed relationships. In the cutthroat world of digital commerce, consumers rarely give second chances.

To gauge the extent of this, we asked, *"Have you switched to a competitor or local alternative due to experiencing transaction barriers?"*



In response, **68% of respondents acknowledged switching, with 18% doing so *often***—a likely permanent erosion of lifetime value.

But this challenge is not confined to mature markets. In high-growth regions like Brazil and Mexico, where payment options are fragmented and logistical challenges greater, consumers are more likely to be flagged simply because identity coverage is weaker and insight is low.

Baymard Institute highlights the magnitude of this issue. The average large ecommerce site could gain a 35% increase in conversion rate through better checkout processes, including reducing barriers. For enterprise platforms across the US and EU, this translates to $260 billion in unnecessarily lost orders.

Baymard notes that **1 in 5 US shoppers will abandon orders** due to "too long or complicated checkout" processes.

Our survey reveals that this escalates globally, with **abandonment rates doubling to 2 out of 5 shoppers** across all five countries surveyed.

This is more than just isolated friction. It's a systemic identity failure. What begins as a single failed transaction quickly cascades into market-level abandonment, a visibility issue masquerading as fraud, and a trust fracture with macroeconomic implications.

Survey discovery

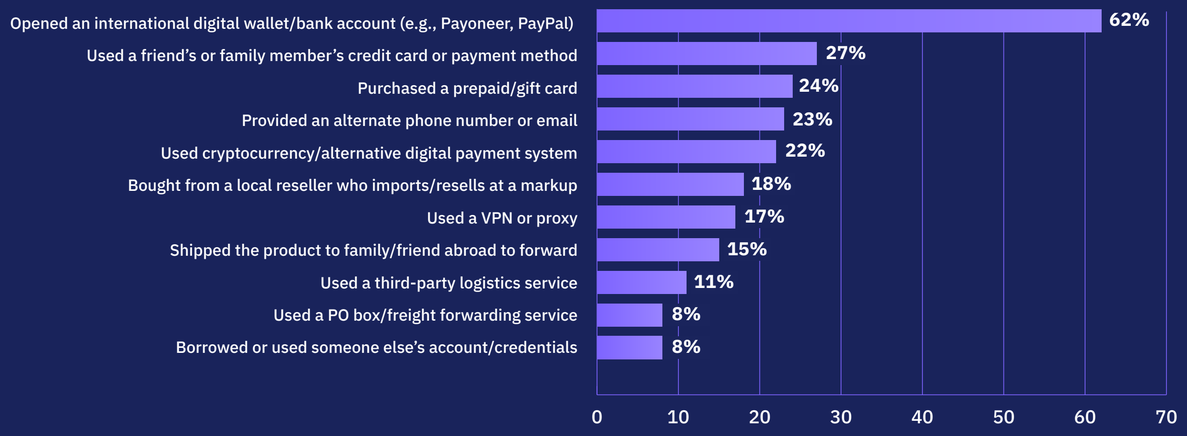
Platforms misread adaptation because they lack customer context.

At the heart of the global identity crisis is a fundamental misunderstanding of consumer behavior: an inability to interpret behavior without the underlying information that gives it meaning.

Consumers aren't abandoning ecommerce so much as they're adapting to survive it. When faced with transaction barriers, outdated verification steps, and rigid checkout systems, consumers respond creatively. But without customer context to understand these adaptations, platforms are defaulting to treating them as risk.

Our survey revealed just how widespread and varied these adaptive behaviors have become:

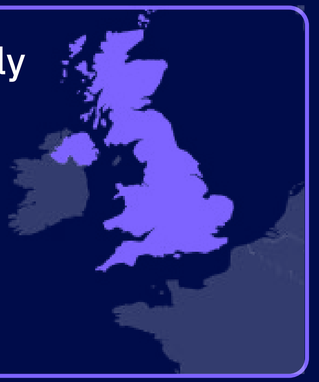
When you are shopping online and are faced with a transaction restriction such as your country or currency not supported, or you are required to provide additional identity verification, what workarounds have you used to complete your purchase?



These behaviors are no longer the fringe, they're the new normal. Without consistent recognition of who the customer is and what their situation requires, these adaptations get flagged because the system doesn't know how to read them.

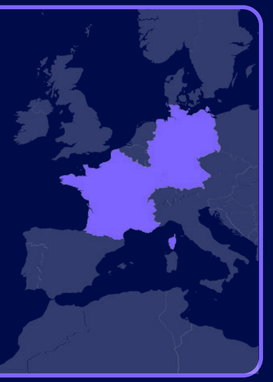
Don't assume they're evenly distributed across global markets, instead, they form a complex patchwork of trust challenges shaped by access, regulations, and infrastructure.

In the United Kingdom, nearly one-quarter of shoppers report using VPNs while shopping, often getting flagged automatically as suspicious.



In Mexico and Brazil, the widespread use of alternative payment systems and third-party logistics is often misclassified as high-risk by legacy fraud models.

In France and Germany, concerns around data privacy drive consumers toward alternate emails and privacy-first payment methods, again triggering status risk flags.



Each workaround represents both an individual act of resilience and a collective signal that current trust models are failing.

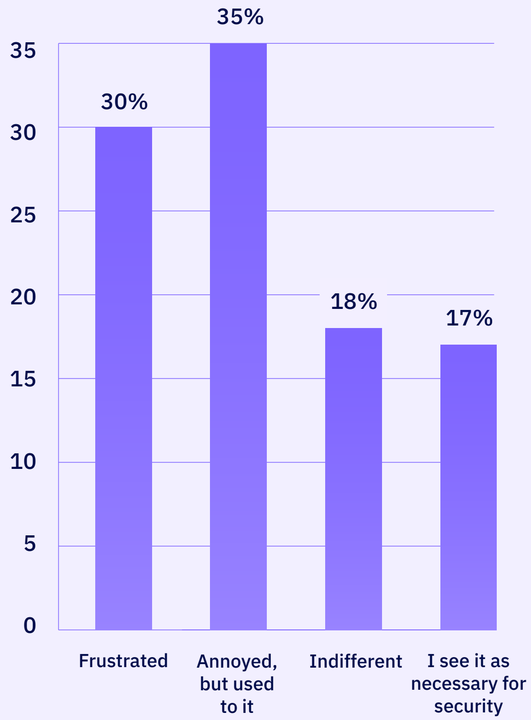
The impact is two-fold:

1. At the individual level, consumers experience broken trust, unnecessary friction, and abandoned transactions

2. At the macro level, invisible market barriers like these erode loyalty, suppress revenue, and gift market share to more insightful competitors

Resentment is building: **a combined 65% of our surveyed consumers expressed frustration about being forced into workarounds**, 35% saying that they're "annoyed, but used to it," and another 30% describe outright dissatisfaction. Rigid, one-size-fits-all fraud frameworks can't scale globally. Trust doesn't require perfection, it just needs clarity. When platforms have the right signals, they are capable of dynamically interpreting consumer behaviors not just at a global level, but at a regional, cultural, and even individual level.

How do you feel about the restrictions and workarounds required to shop online in your country?



Workarounds aren't fraud, they're signals of demand, resilience, and intent. But until businesses can recognize who their customers are, every adaptation will continue to be misread, and every misunderstood behavior will be another customer lost.

Survey discovery

In low-visibility markets, it’s uncertainty, and not fraud, that stalls scale and growth.

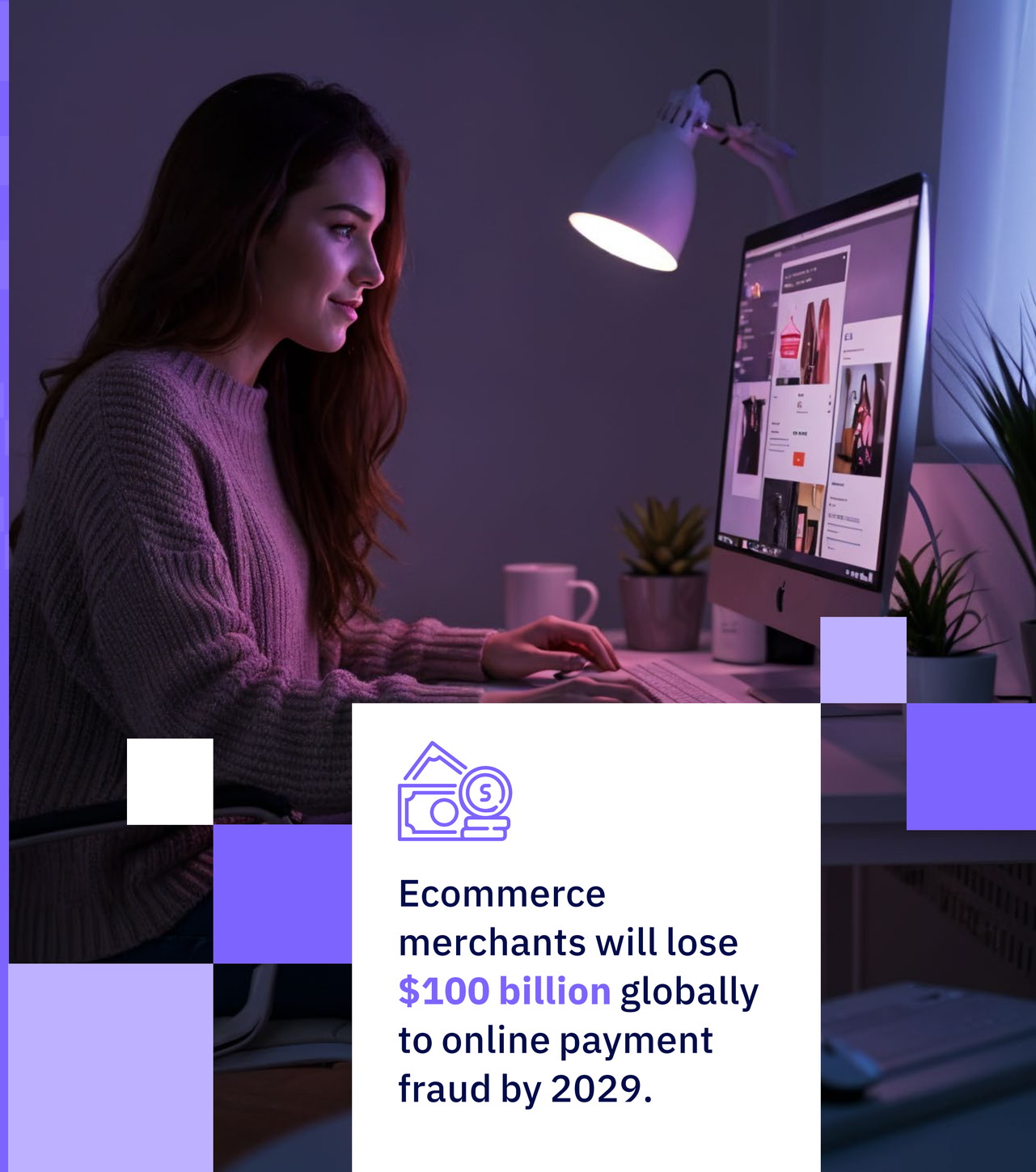
Without a full picture of the customer, businesses default to rigid rules or risky shortcuts, and often lose new customers in the process.

Ecommerce merchants will lose $100 billion globally to online payment fraud by 2029. Yet it's uncertainty driven by a lack of visibility about who is behind the transaction that prevents many companies from evolving their trust strategies—triggering a spiral of lost revenue, fraud exposure, and eroding consumer loyalty.

In high-potential but data-scarce markets like Brazil and Mexico, ecommerce businesses often face incomplete transaction histories, fragmented payment methods, and unfamiliar consumer behaviors. Without rich, predictable datasets available in more mature markets, most businesses are left to guess. And when businesses guess, they default to binary decisions: good or bad, safe or fraudulent, pass or fail.

But in a world of VPNs, cross-border orders, and decentralized consumer habits, binary trust decisions are no longer sustainable. When businesses can't see the full picture, even standard regional behaviors are treated as threats.

We need to solve the deeper problem: recognizing adaptive, legitimate consumers in real-world conditions, even when insights are limited. Solely focusing on fraud losses misses the larger systemic damage. In low-data environments, businesses aren't just losing transactions, they are forfeiting future market dominance.



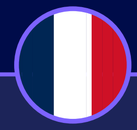
Ecommerce merchants will lose **$100 billion** globally to online payment fraud by 2029.

And in regions where digital adoption is still accelerating, these losses compound dramatically over time. Consider the markets we surveyed:

In **Brazil**, adaptive consumers are often flagged for risk when using alternative payments, VPNs, or reshipment services.

In **Mexico**, digital wallets and alternative banking solutions are common among legitimate buyers, yet are frequently misinterpreted by rigid verification systems.

In **Germany**, higher consumer sensitivity to privacy triggers false alarms when consumers use alternate email addresses, masked phone numbers, or VPNs to protect their data.



In **France**, consumer expectations for seamless, low-friction transactions clash sharply with models that believe adding verification hurdles improve security.

In the **United Kingdom**, nearly one-quarter of shoppers reported using VPNs regularly while shopping, a behavior that traditional fraud systems often automatically associate with risk.

Across all of these markets, trust is not eroding uniformly. It fractures in local patterns, invisible at first, but devastating over time for businesses that are unable to adapt. So the challenge is no longer simply preventing fraud, but instead enabling recognition to dynamically rebuild trust, region by region, behavior by behavior, transaction by transaction.

In data-scarce environments, it's a double-edged sword, either breaking good customer journeys or allowing real threats to slip through unchecked.

Both outcomes signal the same failure: the inability to fully and immediately recognize your global customers.

But top retailers are no longer guessing, they're investing in dynamic trust models that learn, adjust, and interpret behaviors in context, turning the ability to resolve uncertainty into a competitive advantage. There's no question that these markets will continue to grow; the real question is whether your systems will grow alongside them.

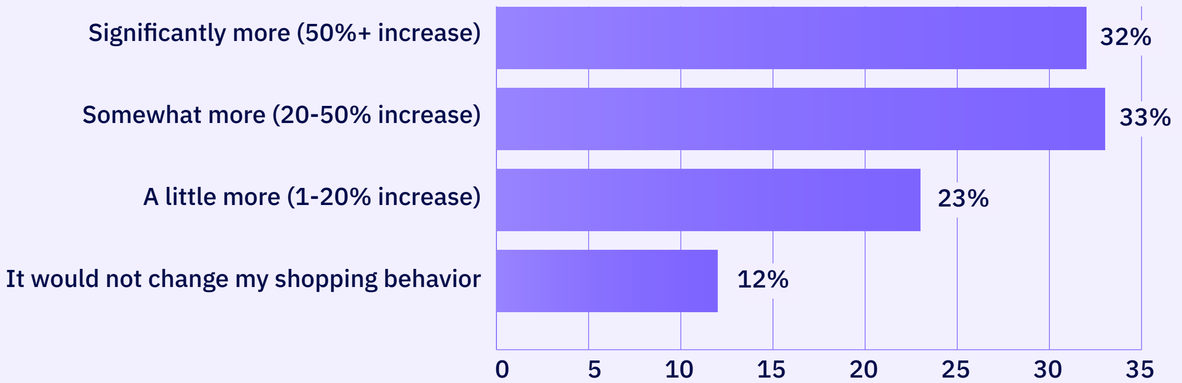
Survey discovery

When customers feel trusted, they spend more.

Consumers in high-growth regions are not leaving ecommerce–they are abandoning platforms that treat them like a risk.

Easier transactions lead consumers in high-growth markets to buy more—a lot more. According to our survey, **33% of consumers would increase their shopping by *20-50%* if transaction barriers were reduced. Another one-third of consumers would increase spending by *more than 50%*.**

If international companies could resolve transaction restrictions, how much more would you shop online?



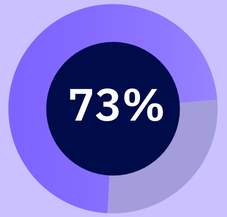
This latent revenue opportunity is most pronounced in markets burdened by fragmented financial infrastructures, such as Mexico and Brazil, where cash-based and alternative payment systems dominate. Consumers here often use third-party shipping addresses, alternate currencies, or digital wallets less familiar to international brands. While commonplace in these countries, global brands often misclassify this as suspicious behavior under more rigid, rule-based systems.

But even in highly structured markets like Germany, excessive verification can backfire. Our survey found that **18% of consumers have abandoned purchases when security steps felt excessive**, despite Germany's high trust standards for online ecommerce.

Across these markets, the message is clear: improving recognition at checkout, particularly for adaptive but legitimate behaviors, reduces abandonment, recovers lost sales, and drives incremental spend from existing customers. It also enables brands to take market share from competitors still relying on static, inflexible trust frameworks.

Of course, most of our respondents want reasonable transaction protection: 73% of consumers say they are *definitely* more willing to purchase from online retailers or marketplaces when they sense security safeguards in place. Additionally, less than 2% of participants said better safeguards *don't impact* their buying decisions.

73% of consumers say they are definitely more willing to purchase from online retailers or marketplaces when they sense security safeguards in place.



This offers an important insight into consumer psyches; what consumers are rejecting is not security, but distrust. When behavior is flagged not because it's risky, but because the platform lacks the clarity to understand who the customer is, trust erodes and revenue goes with it.

Ecommerce brands able to see the full picture, and not just the transaction, stand to unlock meaningful growth from customers who are ready to buy.

Survey discovery

Binary security forces unnecessary trade-offs between growth and protection. Trust scoring offers a third path.

Nearly 6% of all ecommerce orders are rejected due to suspected fraud, yet up to 80% of those rejections are false declines involving legitimate customers.

Across the global ecommerce landscape, traditional fraud detection systems are trapped in an outdated mindset: approve or deny. But the problem isn't the narrow rules, it's a failure of identity insights. In today's reality, where identity data is fragmented and customer behaviors vary widely by region, binary trust models no longer reflect how legitimate transactions actually happen across borders.

The results are eye-opening:

6% of global ecommerce orders are rejected due to suspected fraud

Up to 80% of these declined transactions are false declines from legitimate customers

Instead of evolving toward smarter, context-aware decisioning, many businesses have responded by layering more rigid control measures onto brittle frameworks. These additive layers may feel safer, but they only worsen the core issue: the system still doesn't know who is on the other side of the transaction.

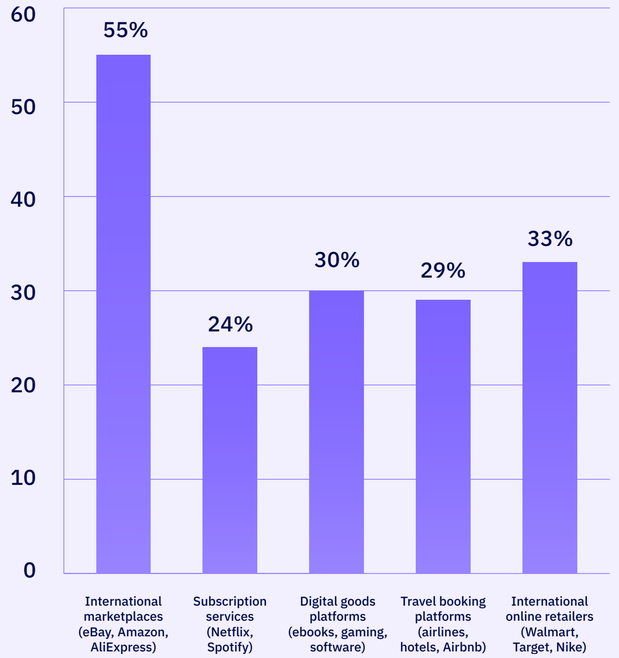
This lack of clarity leads to blanket decisions that frustrate legitimate consumers, especially in international markets. For example, in Mexico, 83% of surveyed consumers welcome additional verification, but only when it supports, not disrupts, their purchasing intent.

Rigid global systems fail precisely because they apply uniform logic to non-uniform markets. Instead of recognizing behaviors such as VPN usage, alternative payment behaviors, and localized shipping preferences, they treat any deviation from legacy norms as risk.

When we asked consumers about encountering transaction barriers, nearly 50% said they occasionally experience issues, while **20% said they face limitations *very often***. With respect to where restrictions occur, the top three cited areas include:

1. International marketplaces (e.g., Amazon, eBay, AliExpress) (55%)
2. International online retailers (e.g., Walmart, Target, Nike) (33%)
3. Digital goods platforms (e.g., eBooks, gaming, software) (30%)

What types of online platforms do you most experience transaction restrictions?



Perhaps most revealing: **8% of consumers report being blocked simply for being in a *high-risk region*—** the consequence of an identity trust failure, not risk management.

These are not isolated incidents, they represent a failure to separate real threat from a real customer, a blind spot that punishes the same consumers that global brands are trying to reach.

The visibility layer that global ecommerce is missing

For ecommerce businesses trying to grow globally, the problem isn't just shipping and payment methods; it's not having enough reliable insight into who their customers are. The result? Poor decisions, overcorrection, and missed opportunities.

Companies operating internationally typically have modern fraud solutions in place. Yet many are still defaulting to outdated logic because their systems fundamentally lack the global identity coverage needed to interpret signals in real time and at scale.

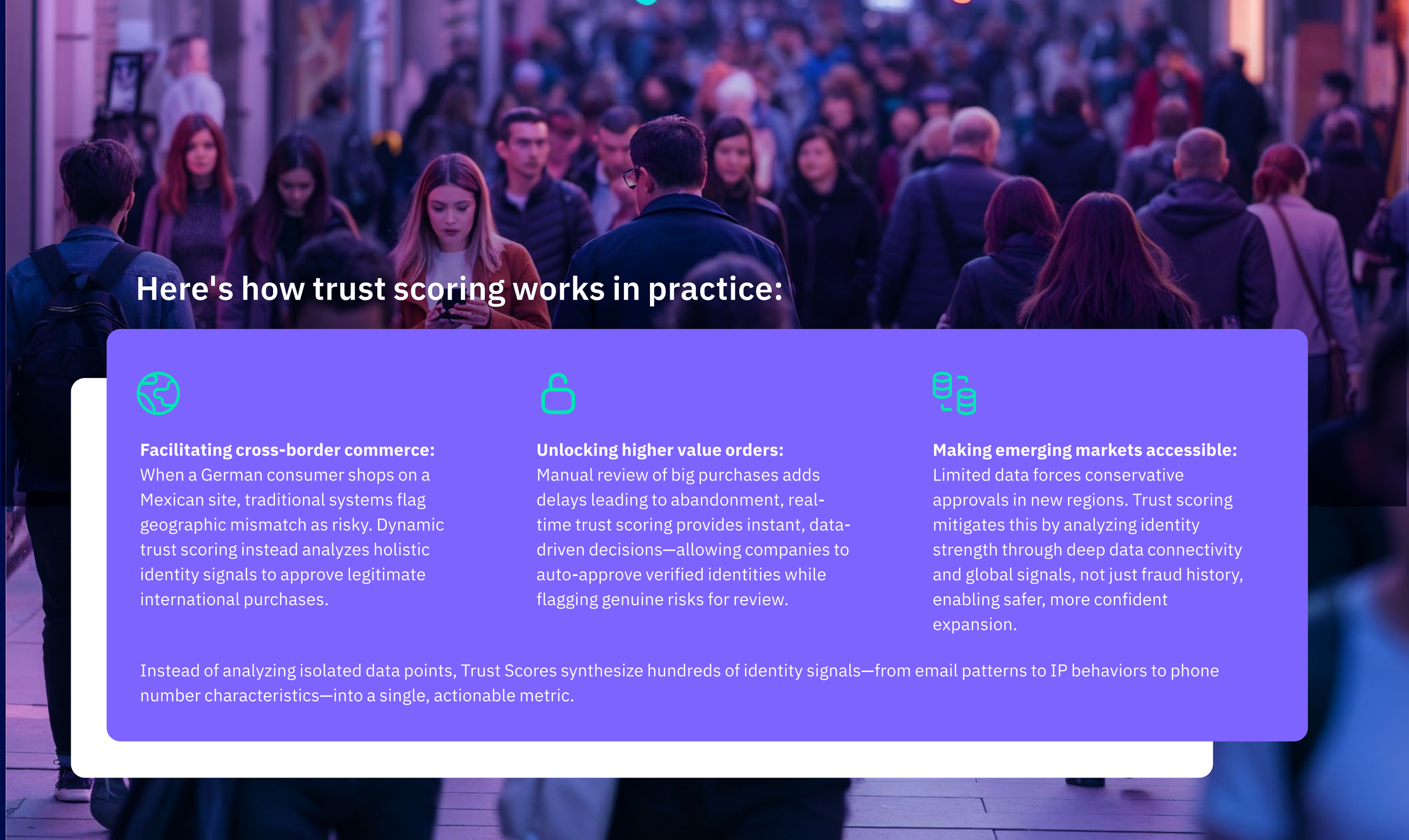
At Elephant, we solve this through global trust scoring, a framework built to provide ecommerce fraud solutions the global clarity they are missing.

Our global identity trust solution is powered by Elephant's continuously evolving identity graph, built from over 5 billion identities across more than 150 countries, with more than 2 billion updates processed daily. This ensures our trust scores are powered by consistent, compliant, and real-time data, even in regions where identity data coverage is traditionally limited.

Trust scoring brings an AI-powered approach to recognizing digital identities that analyzes hundreds of correlated identity signals in real-time. Unlike traditional rule-based systems (or single-point authentication methods), a platform built on trust scores examines the context and connections between various identity elements—email, phone, IP address, physical address, and more—to generate a comprehensive trustworthiness score. It's a way to see the whole customer, not just the transaction.

With global trust coverage, businesses can simultaneously reduce fraud exposure and increase approval rates for legitimate customers, without defaulting to excessive barriers, costly manual reviews, or rigid blocks that suppress revenue.

The strength of our model lies in its connectivity; examining both individual data points and the relationships between them, creating an identity graph that fraudsters find difficult to fabricate.



Here's how trust scoring works in practice:

Facilitating cross-border commerce: When a German consumer shops on a Mexican site, traditional systems flag geographic mismatch as risky. Dynamic trust scoring instead analyzes holistic identity signals to approve legitimate international purchases.

Unlocking higher value orders: Manual review of big purchases adds delays leading to abandonment, real-time trust scoring provides instant, data-driven decisions—allowing companies to auto-approve verified identities while flagging genuine risks for review.

Making emerging markets accessible: Limited data forces conservative approvals in new regions. Trust scoring mitigates this by analyzing identity strength through deep data connectivity and global signals, not just fraud history, enabling safer, more confident expansion.

Instead of analyzing isolated data points, Trust Scores synthesize hundreds of identity signals—from email patterns to IP behaviors to phone number characteristics—into a single, actionable metric.

Conclusion: Solving the global identity crisis

The findings of our survey reveal a global digital economy straining against its own limitations. While businesses continue to fight yesterday's fraud battles, a larger threat (and opportunity) has emerged: a global identity crisis, where the inability to distinguish legitimate customers from fraudsters is stalling growth at scale.

Across every market we surveyed, consumers sent a clear message:

They are ready to engage, they are eager to spend, but they will not wait for businesses to recognize them.

Rigid, outdated verification models, static risk signals, and one-size-fits-all frameworks are no longer sufficient. These aren't just legacy tools, they're active barriers to growth. So the challenge becomes not just simply stopping fraud, but learning how to trust better, faster, smarter, and at scale.

This is where the promise of Elephant's dynamic identity trust scoring comes into full view. You can have a model capable of providing global clarity by instantly recognizing consumers without misclassifying them. Of fully seeing each customer individually, holistically, across borders, devices, behaviors, and purchase patterns.

The businesses with this vision will unlock the potential $47 billion trapped in the global identity crisis. A lack of clarity may define today's ecommerce landscape–but it does not need to control its future. At Elephant, we believe that identity trust is the new frontier of global expansion. Businesses that invest in expanding their global identity coverage today will own the markets of tomorrow.

About

Elephant is the identity trust solution built for global scale. Powered by the world's largest network of over 5 billion identity profiles, Elephant delivers real-time trust scores that reduce manual reviews, prevent false declines, and unlock revenue across regions.

Only Elephant provides consistent, high-confidence identity insights anywhere you do business—so you can approve more real users, faster.

Visit **elephant.online**