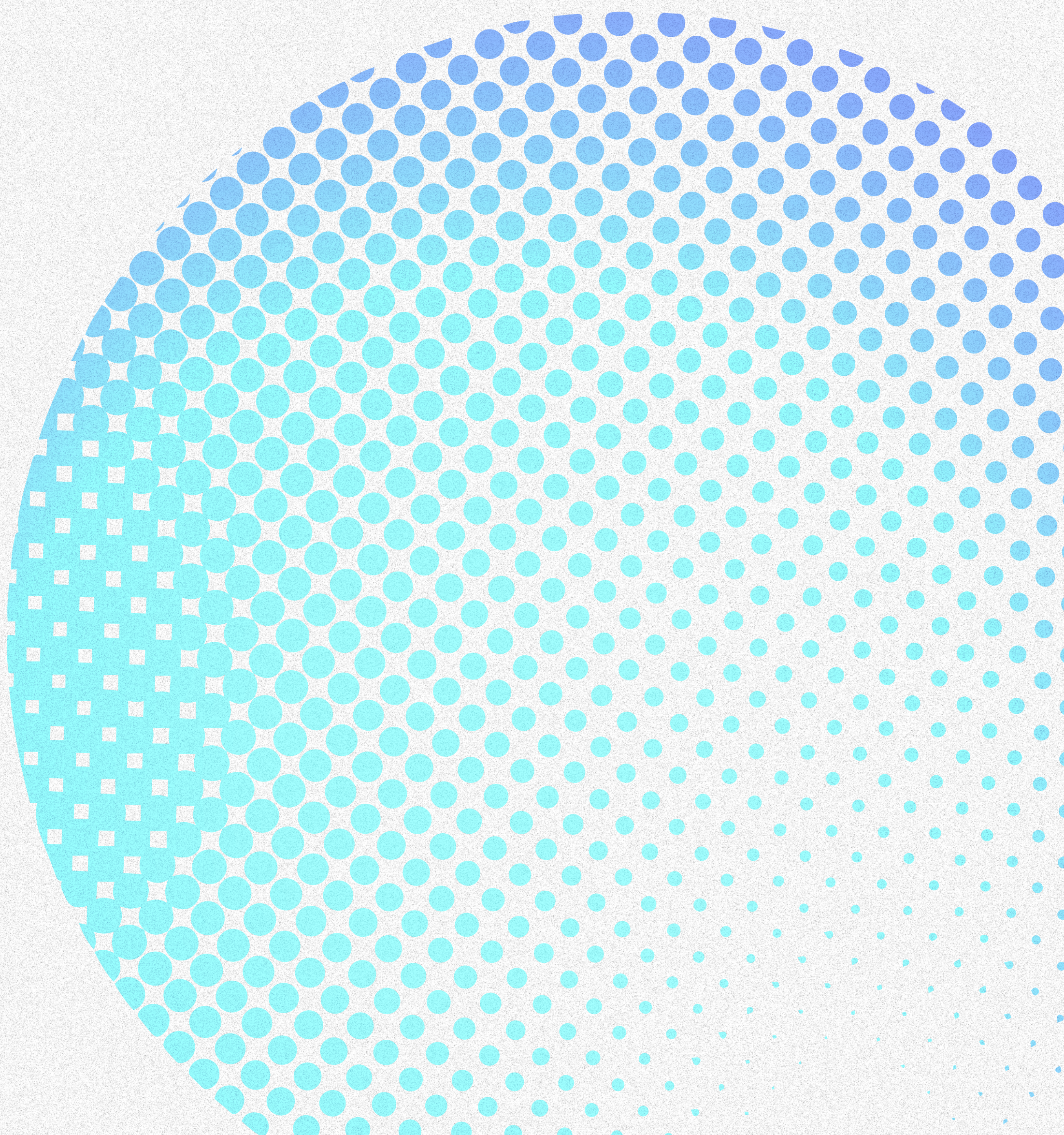
Liminal Research Report | November 2023

Transaction Fraud Prevention in E-Commerce

● Market and Buyer's Guide



Liminal™

Contributors

Travis Jarae
CEO

Will Charnley
Managing Director

Cameron D'Ambrosi
Senior Principal

Jonathan Gergis
Analyst

Jennie Berry
President

Stacy Schulman
Senior Vice President

Vatsal Jhawar
Senior Associate

Vivaan Jaikishan
Analyst

Table of Contents

Navigation – click the Liminal logo to return to this page.

Key Takeaways

The digital marketplace has grown substantially in recent years, with a notable shift towards e-commerce, mobile retail, and digital service delivery. This increasing reliance on digital transactions emphasizes the importance of ensuring efficiency and security while also enhancing the user experience. A seamless and positive user experience in legitimate digital transactions cannot be overstated, as it directly impacts customer satisfaction, trust, and revenue. The question that arises is whether there is a correlation between optimizing the user experience and improving the efficiency and security of legitimate digital transactions. To explore this, in October 2023, Liminal conducted research involving fifty B2B technology buyers across e-commerce and online retailers in five regions: North America, Europe, Latin America, Asia-Pacific, and the Middle East & Asia. The research findings were further validated through qualitative interviews with business executive leaders and industry experts. Here's what we uncovered:

- **The cost of solving fraud is on the rise, driven by elevated fraud risks and general price increases; this presents challenges for all buyers, with a particular impact on small and medium-sized enterprises:** Over the past twelve months, 54% of buyers have encountered price increases, and 66% anticipate paying more in the future. Smaller solution providers are especially vulnerable, with only 17% of buyers who serve fewer than 500,000 customers capable or willing to absorb price increases within their current budget allocations.[1]

- **While mitigating fraud is important, buyers increasingly seek solution providers who deliver a consistent, positive user experience and optimize the processing of legitimate transactions:** 62% of buyers placed a higher priority on minimizing false declines, even if it meant allowing some fraudulent transactions, rather than concentrating solely on reducing fraud rates. Merchants place a higher priority on minimizing false rejection rates, aiming to maintain a better customer experience, and they are prepared to tolerate a certain level of fraud on their platforms to ensure that legitimate customers are not accidentally blocked.

- **Generative AI has enabled the sophistication and frequency of fraud attacks, elevating the threat of financial losses and reputational damage:** 98% of buyers reported an increase in AI-enabled transaction fraud attacks on their platforms. To combat this risk, 73% of merchants currently rely on two or more risk-scoring vendors to better prevent fraud. This sheds light on the limitations of existing fraud models, emphasizing the urgent need for dedicated countermeasures and technologies designed to thwart AI-driven attacks.

- **Rising first-party fraud rates pose fresh challenges and threat vectors for solution seekers, necessitating additional product capabilities from technology providers:** As indicated by 66% of surveyed merchants, categorizing chargebacks and return fraud is a significant market pain point. Moreover, recent studies also indicate that 35% of consumers admitted that they've engaged in first-party fraud, with over 40% of them planning on committing first-party fraud again in less than 60 days after the first event. This increase in first-party fraud leads to massive financial loss, with annual first-party loss in the US totaling more than $100 billion.[2]

- **There is demand from buyers for more robust identity verification protocols at account opening as a tool for fraud prevention, as it enhances security by reducing the risk of identity-related fraud attacks:** 68% of surveyed buyers expressed confidence in the potential efficacy of identity verification for validating individuals' identities. Incorporating identity verification tactics could make it more challenging for fraudsters to impersonate others and potentially mitigate instances of friendly fraud.

Introduction

In recent years, consumers have become increasingly dependent on digital transactions, marking the onset of a new era in online commerce. Exponential growth in e-commerce transactions, both in terms of volume and value, has delivered convenience and accessibility to consumers worldwide. This meteoric rise in digital trade has not been without its challenges; digital transactions have been accompanied by a corresponding increase in fraud attacks. Between 2019 and 2022, fraud attempts have risen at an equivalent rate of 80%, mirroring the growth in digital transactions.[3] Liminal anticipates this trend to continue over the next five years.

The surge in fraud attempts is not the sole concern; the tactics employed by fraudsters are also becoming increasingly difficult to detect and thwart. By leveraging AI-enabled technologies, fraudsters have elevated the sophistication of their attacks across e-commerce platforms. These advanced and high-volume fraud attacks are inflicting substantial financial losses on online platforms. In response to this evolving threat, e-commerce merchants are acknowledging the urgent need for robust transaction fraud prevention solutions to curtail and prevent fraudulent transactions on their platforms.

In this report, Liminal conducted a thorough exploration of the market use case of transaction fraud prevention in e-commerce, offering an in-depth analysis from the perspective of buyers. Our research highlights the vital factors that buyers take into consideration when navigating the transaction fraud prevention landscape.

Liminal sheds light on the various fraud typologies frequently encountered by e-commerce merchants. We provide insights into recent market trends, clarifying the mechanisms and processes that enable fraud platforms to catch fraudulent transactions before they occur. The report also explores buyer demand for transaction fraud prevention solutions, the substantial challenges faced by buyers, the difficulties experienced when attempting to meet their demands, and a glimpse into future prospects for buyers in this dynamic landscape.

In this report, Liminal also presents market opportunities and drivers, including a calculation of the total addressable market (TAM) for transaction fraud prevention in e-commerce, which is projected to reach $7.9 billion by 2024 and is expected to grow to $12.4 billion by 2028, demonstrating a compound annual growth rate (CAGR) of 11.8% over this period.

The ever-evolving nature of fraud tactics underscores the need for proactive strategies to stay one step ahead of fraudsters. To support merchants in this endeavor, Liminal concludes its report with a comprehensive buyer's guide. This list of solution providers and questions that can be applied in a request for information (RFI), equips buyers with the information and resources to assess and select a fraud prevention platform that meets the unique needs of each organization. This guide serves as a valuable resource for those looking to implement transaction fraud prevention solutions to safeguard their digital platforms in the online marketplace.

Market Overview

Transaction Fraud Definition

Transaction fraud prevention encompasses various strategies and tools that businesses employ to shield themselves against fraudulent or unauthorized transactions. These approaches include behavioral analysis, risk scoring, geolocation signals, and real-time fraud monitoring, all crafted to detect and mitigate fraud while striving to minimize disruption to the user experience.

Behavioral analysis closely examines user patterns during transactions, allowing for the early detection of suspicious activity. Geolocation signals verify transaction legitimacy by tracking the user's geographic location. Simultaneously, real-time fraud monitoring employs sophisticated AI models to scan for warning signs, responding swiftly to prevent fraudulent transactions. A critical aspect of these strategies is maintaining a balance between robust security and a smooth, user-friendly online shopping environment.

While the capabilities of each fraud solution are unique, solution providers typically deliver a risk signal, a risk score, or a risk decision to the merchants they serve:

- **Risk Signal:** A signal typically comes from a specialist solution provider (e.g., geolocation provider) and is ingested into a larger fraud decisioning platform.

- **Risk Score:** A score can be calculated across different variable levels (i.e., 1-10, 1-100) and allows merchants to customize rules according to a specified risk threshold. In this model, some scores are 'passed', others are 'rejected', and some are escalated for manual review.

- **Risk Decision:** A risk decision platform delivers a yes or no answer to either validate the transaction or reject it. In these models, merchants may customize the underlying variables incorporated in the risk decision; however, the end result is typically authorizing or not authorizing the transaction.

Transaction Fraud Prevention in E-commerce

Transaction fraud prevention tools are critical safeguards for e-commerce platforms, designed to identify and mitigate potentially fraudulent actions. The overarching goal of transaction fraud prevention solutions is to allow all genuine transactions to be processed through the merchant platform successfully while minimizing fraud losses. Transaction fraud prevention vendors have the ability to adapt the risk thresholds, which determine whether a transaction is approved or denied, according to the merchant's risk tolerance levels and the nature or value of the items being offered for sale.

Preventing transaction fraud requires a multifaceted approach. One primary concern for merchants is the use of stolen or synthetic payment details and identity information, a common fraud tactic. By scrutinizing transactions for inconsistencies and anomalies, transaction fraud solutions can flag suspicious purchases and trigger an immediate response to mitigate the risk. Another critical capability of many transaction fraud prevention tools is to address fraudulent returns and chargebacks. Returning purchased items is a common practice within e-commerce; however, fraudsters often exploit the system by returning stolen or fictitious goods or making unwarranted chargeback claims. Fraud detection tools are crucial in distinguishing between genuine and fraudulent return requests, enabling merchants to minimize losses.

To bolster their efficacy in fighting fraud, e-commerce merchants frequently employ advanced systems, which can encompass rule-based algorithms and AI-powered risk-scoring mechanisms. Rule-based systems use predefined criteria to identify suspicious transactions, while AI-powered models leverage machine learning (ML) and real-time data analysis to adapt and evolve in response to emerging fraud patterns. Additionally, the incorporation of behavioral insights and device analytics into the fraud prevention process provides a deeper, more nuanced understanding of user behavior. This approach enhances the precision of fraud detection and enables a proactive response to potentially fraudulent transactions, effectively preventing them from being successfully executed.

The ultimate objective of transaction fraud prevention in e-commerce is to strike a delicate balance. On one hand, it aims to minimize fraud risks, safeguard merchants from financial losses, and foster consumer trust. On the other hand, it strives to ensure a seamless and secure shopping experience for legitimate users. By remaining at the forefront of evolving fraud tactics and adapting through innovation, these technology solutions play a crucial role in upholding the trust and confidence of both merchants and customers in the digital marketplace.

Importance of Transaction Fraud Prevention Solutions

Transaction fraud prevention is vital in e-commerce for various reasons. It provides a financial safety net for businesses by shielding them from potential monetary losses stemming from fraudulent transactions, unauthorized purchases, or chargebacks. It also reduces the operational costs of addressing fraud-related issues and disputes, enabling companies to allocate resources more efficiently. Ultimately, a focus on transaction fraud prevention ensures that legitimate transactions proceed smoothly and seamlessly on the merchant's platform, while risky or fraudulent transactions encounter additional hurdles and scrutiny.

Fraud Typologies

With the rapid growth of e-commerce transactions, fraud attacks can be broadly categorized into two main groups: first-party fraud and third-party fraud.

First-party fraud involves individuals attempting to commit fraud against an e-commerce platform by leveraging their own legitimately-opened accounts.

Common Examples of First-party Fraud:

- **Chargeback Fraud**: A customer initiating a credit card chargeback with their bank under false pretenses (e.g., claiming an item was damaged or defective when it was delivered in good condition).
- **Refund Fraud:** A customer requesting a refund directly from the merchant under false pretenses (e.g., claiming an item was not received when the package was properly delivered).
- **Return Fraud:** A customer initiates a return of a delivered item and requests a refund, but fails to mail the return or mails the box back empty.
- **Loyalty / Promo Fraud:** A customer abuses loyalty programs, coupons, or discounts to gain monetary benefit improperly (e.g., a customer falsely claims a military veteran discount).

Third-party fraud occurs when threat actors use compromised accounts belonging to existing, legitimate consumers or accounts created with falsified or stolen identity information to defraud an e-commerce platform.

Common Examples of Third-party Fraud:

- **Social Engineering Scams:** The use of manipulative techniques to convince a consumer to initiate a transaction from their account on behalf of the fraudster.

- **Account Takeover (ATO):** The unauthorized access of a legitimate customer account by a fraudster to initiate fraudulent transactions. ATO can be accomplished by several different unique threat vectors including:

  - **Phishing**: The extraction of a consumer's account credentials using a fake login page that tricks the user into sharing their password.

  - **Breached Credentials:** The procurement of account credentials via malware placed directly on a consumer's computer, or purchased from hackers selling account information on the black market.

  - **Credential Stuffing**: The use of account credentials obtained for an unrelated website, in an attempt to access additional accounts held by the consumer that use a shared password.

- **Payment Fraud:** The use of stolen payment credentials to purchase goods via an account created by the fraudster. This can include both credit/debit card numbers, or bank account/routing numbers.

How Solutions Work

While the specific product capabilities may vary among different fraud prevention vendors, they typically employ a combination of signals to score and/or make decisions regarding transactions. Moreover, these solution providers often assist merchants with chargebacks and disputes, and some may offer insurance to cover potential revenue losses. In general, transaction fraud prevention models follow a sequence of steps (see Figure 1, on page 9):

- **Step 1:** User visits an e-commerce website:

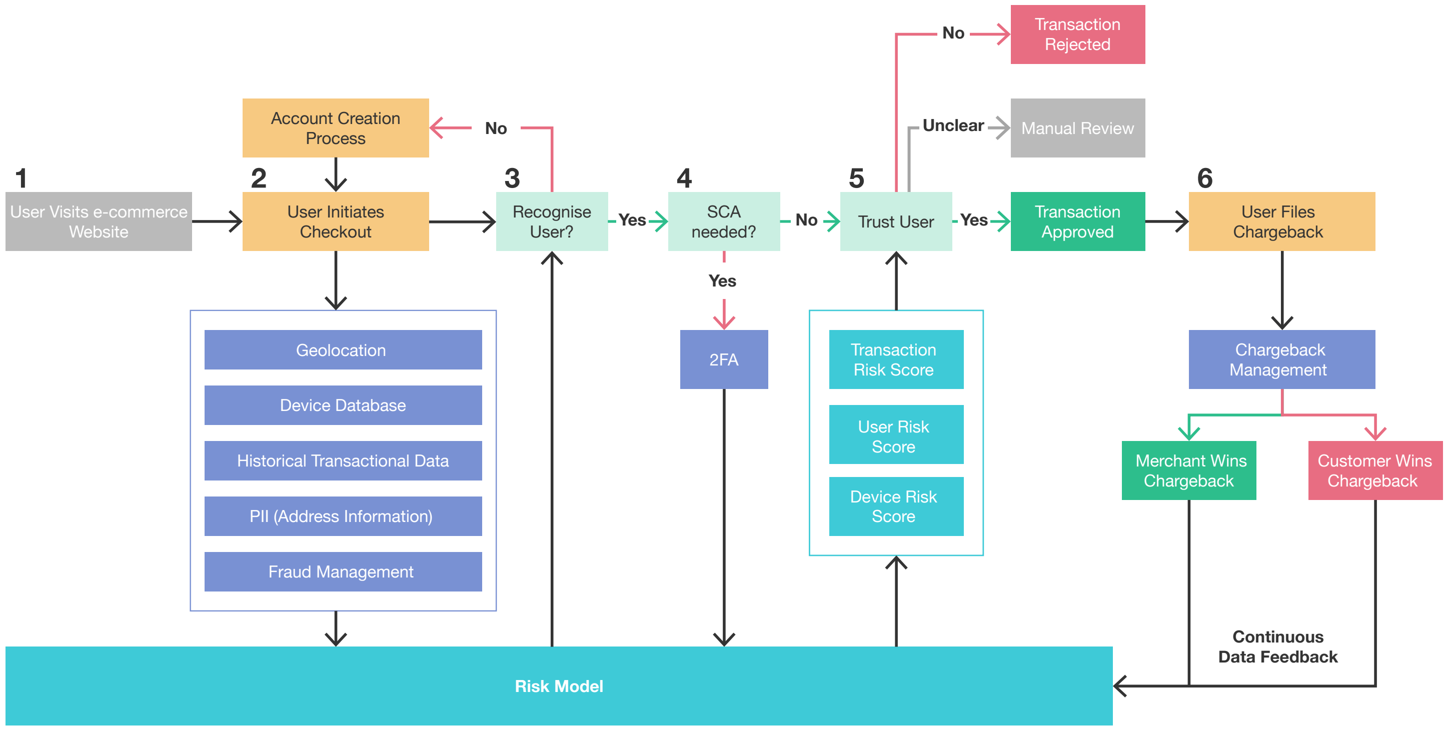
  - As soon as a user enters the e-commerce website, the fraud platform starts collecting behavioral signals that can be tracked and collected. Behavioral signals may include geolocation, IP address, device level signals (e.g., type of device, operating device), keystroke dynamics, etc. Data points like how users hold their device, mouse movements, and touchscreen pressure may also be collected. The fraud detection platform will track the user as they navigate through the website, all the way through checkout. This allows the platform to analyze how the user navigates through the website and whether the user is demonstrating bot-like or suspicious behavior.

- **Step 2:** The transaction is initiated, passing along key behavioral, transaction, and device information into the risk mode:

  - While the user initiates the checkout process, the fraud platform will continue operating in the background to analyze user behavior. For example, fraud platforms utilizing behavioral biometrics can determine whether users are being guided through the checkout process by a potential fraudster or if they are navigating through text boxes in an atypical manner, which could be an indication of a potentially fraudulent transaction.

- **Step 3:** The fraud platform determines if it has enough information to validate the user or not:
    - The risk engine will determine if it has enough information to validate the user based on the signals collected.
    - If there ***is not*** enough information to validate the transaction, the user may be tasked with either creating an account or validating additional information (e.g., address) to provide the merchant with more certainty.
    - If there ***is*** enough information to validate the transaction, the user will be evaluated based on the amount of risk they pose.
- **Step 4:** The policy engine will determine whether Strong Customer Authentication (SCA) is required for a particular user:
    - Certain geographical concerns and internal risk policies may require merchants to conduct a second form of authentication in order to prevent fraud. This is required in some regions (i.e., Europe) and generally viewed by fraud prevention practitioners as a best practice.
    - If there ***is*** a requirement for SCA, the user will be prompted to provide a second form of authentication. This may include providing additional user information, conducting in-app authentication, and in some cases, authenticating via a one-time passcode (i.e., SMS OTP).
    - If there ***is no*** requirement or need for SCA, the user will skip this step and be evaluated based on the risk model.
- **Step 5:** The transaction is either approved, rejected, or escalated for manual review based on the risk model's calculated score:
    - The risk score is then integrated into the e-commerce platform's decision engine. Depending on the platform's risk tolerance level, the transaction can be approved, denied, or escalated for manual review.
    - For instance, if the collected IP address has been previously flagged for multiple fraudulent attempts, the user displays bot-like behavior, and the device status is identified as jailbroken, the AI/ML model could generate a high-risk score, leading to an automatic rejection of the transaction.
    - If the device's IP address is detected in a different country from the delivery address provided, the risk score may fall within the moderate range, prompting a manual review of the transaction.
    - Fraud platforms offer merchants the flexibility to establish risk thresholds in accordance with their risk tolerance. Furthermore, these risk thresholds can be adapted based on the value of the items or goods being purchased.
- **Step 6:** Post-purchase, if a customer initiates a chargeback, a fraud prevention solution will help the merchant understand the validity of the claim and in some instances, fight the chargeback:
    - Although the specific strategies employed by different solution providers can vary considerably, vendors typically utilize similar models in conjunction with transaction history data to ascertain the validity of a disputed transaction or chargeback, discerning whether it is genuine or potentially fraudulent. In such cases, solution providers may assist merchants in challenging the disputed transaction, provide case management tools, or offer a level of chargeback insurance to reduce the risk of potential losses.

Figure 1: Model of an Example Transaction Fraud Prevention in E-commerce Platform



Necessary Product Capabilities

Liminal conducted market research on the fraud typologies associated with first-party and third-party fraud to gain an understanding of the approaches employed by leading solution providers.

The following scale was used to prioritize product capabilities (see Table 1):

- **Must-Have:** These capabilities are essential to solve the market use case
- **Nice-to-Have**: Helpful capabilities, but not a requirement
- **Differentiator**: Unique product capabilities that not many solution providers have today
- **Not Necessary**: Capabilities that are not a priority when evaluating solution providers

Table 1: Importance of Product Features to Combat Third-Party and First-Party Fraud

Product Capabilities	Third-party Fraud Importance	First-party Fraud Importance
Chargeback Management	🟢	🟢
Device Risk Scoring	🟢	🟢
Proxy and VPN Detection	🟢	🟢
Transaction Risk Scoring	🟢	🟢
User Risk Scoring	🟢	🟢
Real-time Fraud Monitoring	🟢	🔵
Automated Transaction Monitoring	🟢	🔴
Chargeback Protection (Liability Shift)	🔴	🟢
Rules-based Transaction Monitoring	🔵	🔵
Merchant Monitoring	🔵	🔴
Behavior Profiling	⚪	🔵
Signal Sharing Network	🔵	⚪
Social Engineering & Scam Detection	🔵	⚪
Bot Detection	🔴	🔴
Location Intelligence	⚪	🔴
Device Fingerprinting	⚪	⚪
Dynamic Friction	⚪	⚪

🟢 Must have

🔵 Nice to have

🔴 Differentiator

⚪ Not necessary

Market Dynamics

Market Challenges

When engaging with buyers in the market, we discovered a multitude of challenges affecting their businesses today. While these challenges vary based on factors such as business size, geographic focus, and the nature of the goods sold, these specific challenges consistently emerged as both prevalent and severely impactful for buyers seeking to address e-commerce transaction fraud.

These three challenges include:

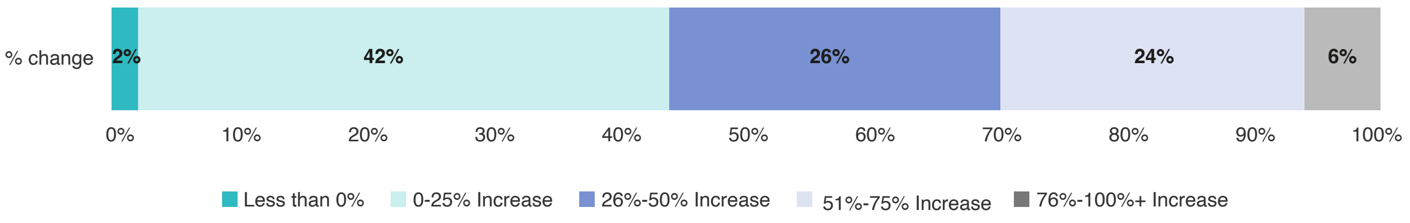
1. Fraudsters are using generative AI to increase the sophistication and scale of their attacks, which exposes e-commerce merchants to serious vulnerabilities.
2. While the risk of fraud continues to rise, e-commerce merchants are cautious about adopting solutions that introduce friction for end users. This caution poses challenges for vendors striving to enhance fraud prevention measures without disrupting the user experience.
3. Both the cost of fraud losses and the expenses associated with fraud prevention solutions are increasing, presenting challenges for buyers seeking to implement cutting-edge solutions within constrained budgets.

Fraudsters are using generative AI to increase the sophistication and scale of their attacks, which exposes e-commerce merchants to serious vulnerabilities.

The increased accessibility of generative AI technology has empowered fraudsters to orchestrate sophisticated, large-scale, automated fraud attacks. Automated AI-driven attacks can inundate the fraud prevention measures adopted by merchants due to the sheer quantity of simultaneous attacks. Furthermore, generative AI is being harnessed to enhance the effectiveness of specific fraud schemes, such as phishing. Fraudsters can manipulate models to craft emails and SMS messages that mirror the language and phrasing commonly used by merchants in their customer communications, making these fraudulent attempts more convincing.

98% of e-commerce merchants identified AI-enabled fraud attacks as significantly impacting the level of fraud their businesses have encountered. Among that 98%, 30% reported a surge in fraud losses exceeding 50% in the past two years (see Figure 2, on the next page). As fraudsters become more adept at harnessing generative AI, Liminal anticipates this trend to persist, putting both merchants and customers at a heightened risk of fraud attributed to generative AI. To counter increased fraud attacks, numerous merchants are turning to the use of multiple vendors, with the expectation that at least one of them will detect and thwart fraudulent activities before they inflict harm on their business. For the merchants who have experienced the greatest increase in fraud (50%+), 73% of them currently rely on two or more risk-scoring models to mitigate fraud risk. This sheds light on the limitations of existing solutions and emphasizes the urgent need for dedicated countermeasures designed to thwart AI-driven attacks.

Figure 2: In the last 2 years, have you witnessed a change in the number of AI-enabled transaction fraud attacks on your platform?

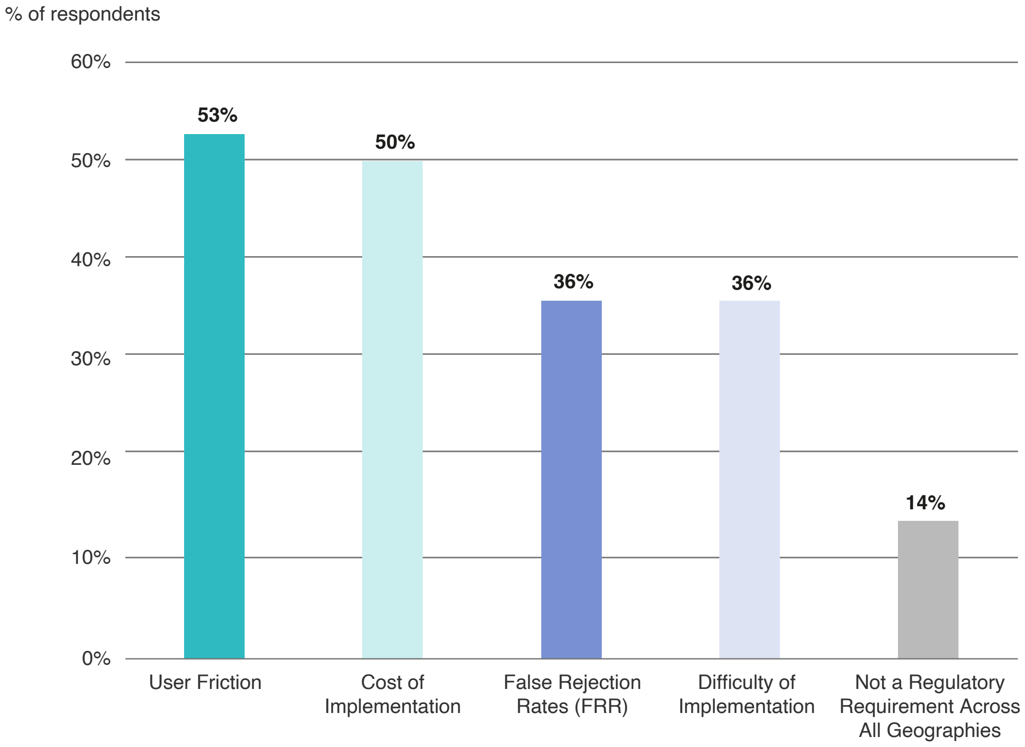


While the risk of fraud continues to rise, e-commerce merchants are cautious about adopting solutions that introduce friction for end users. This caution poses challenges for vendors striving to enhance fraud prevention measures without disrupting the user experience.

Despite the ongoing prevalence of fraud attacks, many merchants remain cautious about embracing more robust fraud prevention solutions, such as 3D Secure 2 (3DS2). In Europe, based on the Payments Services Directive 2 (PSD2), retailers and merchants are required to implement Strong Customer Authentication (SCA) measures like 3DS2; however, outside of that region, adoption of these technologies is limited. Safeguards like 3DS2 enhance customer protection against fraud by introducing a second layer of authentication, and they also bring advantages to merchants by triggering a liability shift for fraud. The liability shift entails that any fraud-related losses borne by the merchant are covered by the card networks, such as Mastercard and Visa.

Despite these benefits, there is hesitancy among merchants to adopt this solution, with only 28% presently incorporating 3DS2. The reluctance among merchants to adopt 3DS2 becomes more apparent when delving into the reasons underpinning this restraint. 53% of merchants who have not implemented 3DS2 identified user friction as a contributing factor, while 50% of buyers cited the high cost of implementation as a critical concern (see Figure 3, on the next page). These apprehensions underscore the pressing need for fraud prevention solutions that balance efficacy and user experience, ensuring that security measures do not inadvertently impede the seamless flow of transactions. The reluctance to implement stronger fraud prevention solutions not only exposes merchants to continued vulnerabilities but also reflects the existing gap in the availability of solutions that effectively mitigate fraud without imposing excessive friction on users. In an ever-evolving digital landscape, finding the right balance between security and user convenience remains a challenge for e-commerce merchants seeking to safeguard their interests and foster trust among their customer base.

Figure 3: If you have not implemented 3DS2 as a defense against transaction fraud, which factors contributed most to your decision?



Both the cost of fraud losses and the expenses associated with fraud prevention solutions are increasing, presenting challenges for buyers seeking to implement cutting-edge solutions within constrained budgets.

Escalating financial losses suffered by merchants in the wake of large-scale fraud attacks are not the only challenge when it comes to weighing the cost of fraud; the cost of procuring effective fraud prevention solutions has risen over the last several years, and many merchants expect a continued increase. 54% of buyers have reported either a slight or substantial increase in the pricing of their chosen fraud prevention solutions (see Figure 4, on the next page). This creates major pain points for merchants, as cost is the second highest rated key purchasing criteria (KPC) for buyers today, with over 32% citing it as one of their top three evaluation metrics for a vendor. As the financial impact of fraud attacks continues to grow, it emphasizes the pressing need for merchants to discover cost-effective yet robust fraud prevention solutions. These solutions should effectively reduce losses and uphold a seamless user experience without imposing excessive financial burdens on merchants.

Figure 4: How has pricing for your fraud vendor trended historically?

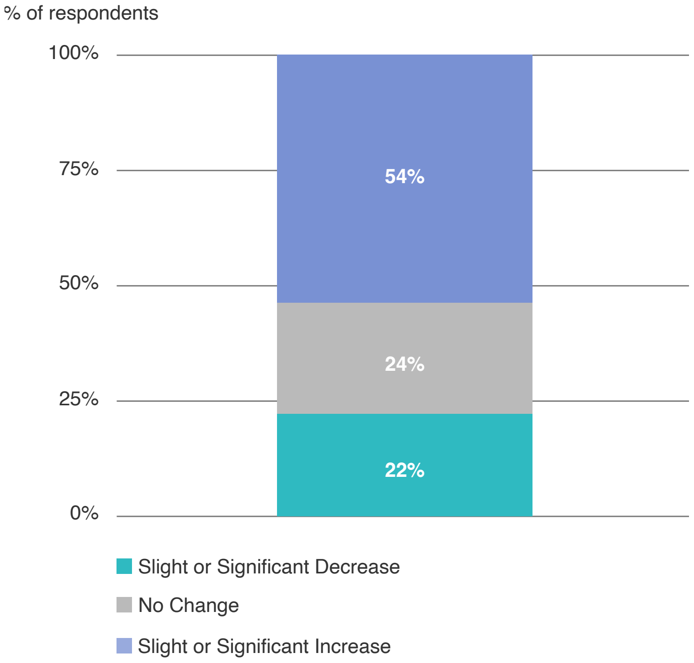
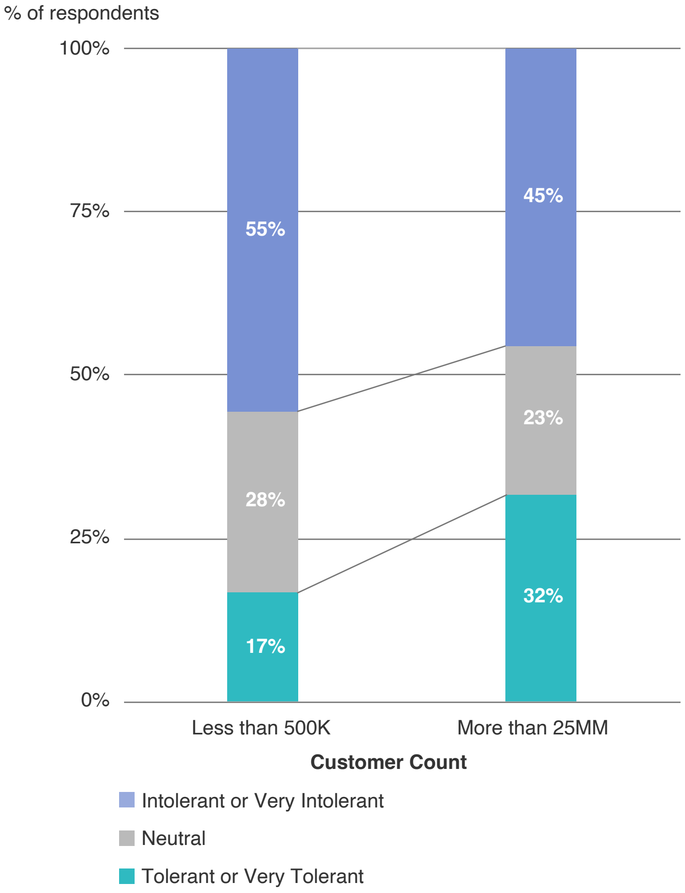


Figure 5: How tolerant are you of price increases for fraud solutions?



The sensitivity to pricing concerns becomes even more pronounced when assessed on a scale that considers the size of the merchant. Out of buyers serving customer bases of fewer than 500,000, only 17% are willing to accept price increases, in contrast to the more price-flexible 32% of buyers serving customer bases of over 25 million (see Figure 5). Consequently, buyers are confronted with a complex challenge as they strive to strike a delicate equilibrium between their cost considerations and the rising necessity of safeguarding their platforms.

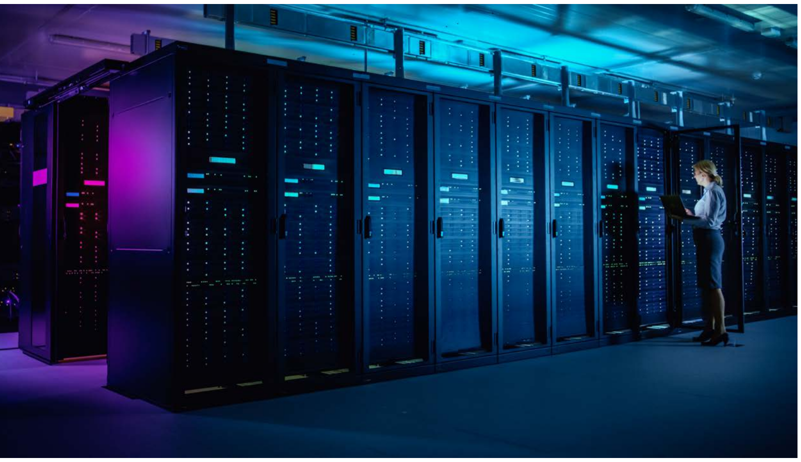
Market Demands

To solve existing market challenges, e-commerce merchants are demanding more robust product capabilities to solve transaction fraud:

1. Buyers want solutions that incorporate AI/ML models alongside traditional rules-based transaction processes to counter the growing threat posed by generative AI-driven fraud attacks.

2. When faced with the choice between introducing friction to transactions and mitigating fraud, buyers prioritize fraud prevention. Solution providers must be cautious not to adopt models that overly reject legitimate or 'good' transactions.

3. The increasing sophistication and volume of first-party fraud is prompting buyers to seek capabilities like chargeback management to better prevent first-party attacks.

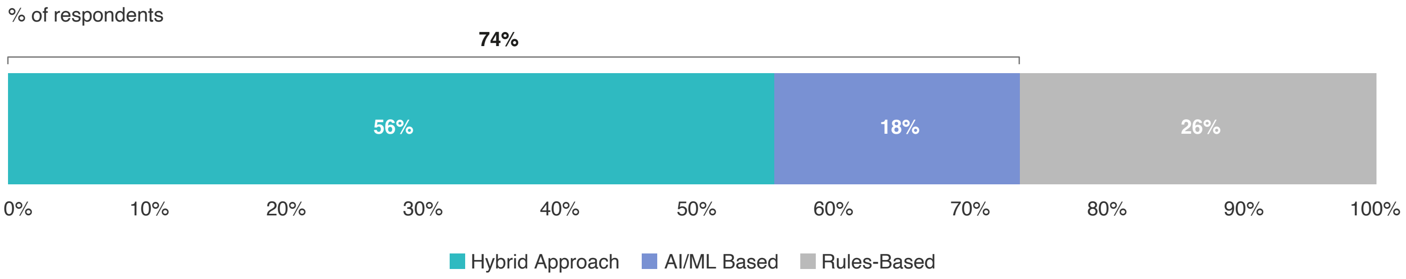


Buyers want solutions that incorporate AI/ML models alongside traditional rules-based transaction processes to counter the growing threat posed by generative AI-driven fraud attacks.

While fraudsters have a head start in harnessing generative AI to amplify the volume and sophistication of their fraudulent activities, solution providers are also embracing fraud prevention solutions that employ AI and ML technologies to maintain a competitive edge in the ongoing battle against fraud. To combat AI-generated attacks, buyers want AI/ML-driven fraud technologies, either as standalone solutions or to enhance existing rules-based risk models. A substantial 74% of buyers desire fraud solutions that leverage AI, and the majority of buyers, accounting for 56%, prefer a hybrid solution that allows them to retain their own rules-based approach while benefiting from enhanced AI/ML scoring signals (see Figure 6, on the next page).

Regarding the development of robust AI/ML models, buyers overwhelmingly emphasize the importance of models capable of assimilating a variety of signals. 85% of buyers highlighted the significance of device, behavioral, transaction data, and user data signals as important capabilities within their transactional fraud prevention solutions. In response, solution providers need to ensure that their models not only utilize AI/ML for generating comprehensive risk scores but also incorporate a wide array of signals as part of a strong defense.

Figure 6: When selecting a transaction fraud management solution, which of the following approaches aligns most closely with your preference?

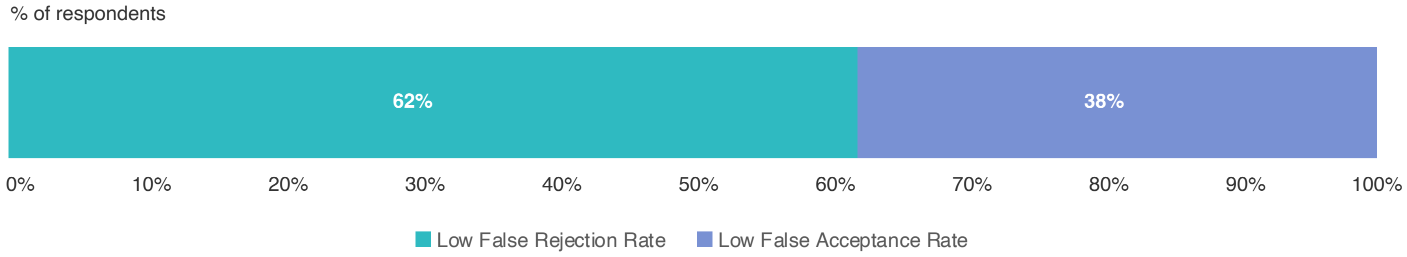


When faced with the choice between introducing friction to transactions and mitigating fraud, buyers prioritize fraud prevention. Solution providers must be cautious not to adopt models that overly reject legitimate or 'good' transactions.

As e-commerce solidifies its position as a staple for online shoppers, merchants face the crucial challenge of striking a delicate equilibrium between minimizing user friction and enhancing fraud prevention. The implementation of more robust fraud prevention measures has given rise to another significant concern for merchants: the issue of false positives. According to JP Morgan, while actual fraud losses accounted for an estimated 7% of the overall cost of fraud, a staggering 19% of losses could be attributed to false positives.[4]

The increased risk of incurring losses by inadvertently rejecting legitimate users has led to merchants being more inclined to accept some degree of fraud in order to facilitate the successful passage of genuine users. When asked to choose between favoring a low false rejection rate or a low false acceptance rate, 62% of merchants favored a low false rejection rate, indicating that merchants prefer solutions that avoid turning away good users (see Figure 7, on the next page). Merchants place a higher priority on minimizing false rejection rates, aiming to maintain a better customer experience, and they are prepared to tolerate a certain level of fraud on their platforms to ensure that legitimate customers are not accidentally blocked. Therefore, striking the right balance between fraud prevention and user experience remains paramount for merchants, allowing them to optimize revenue while minimizing fraud losses.

Figure 7: When assessing the accuracy of a transaction fraud vendor, which is more important to you?

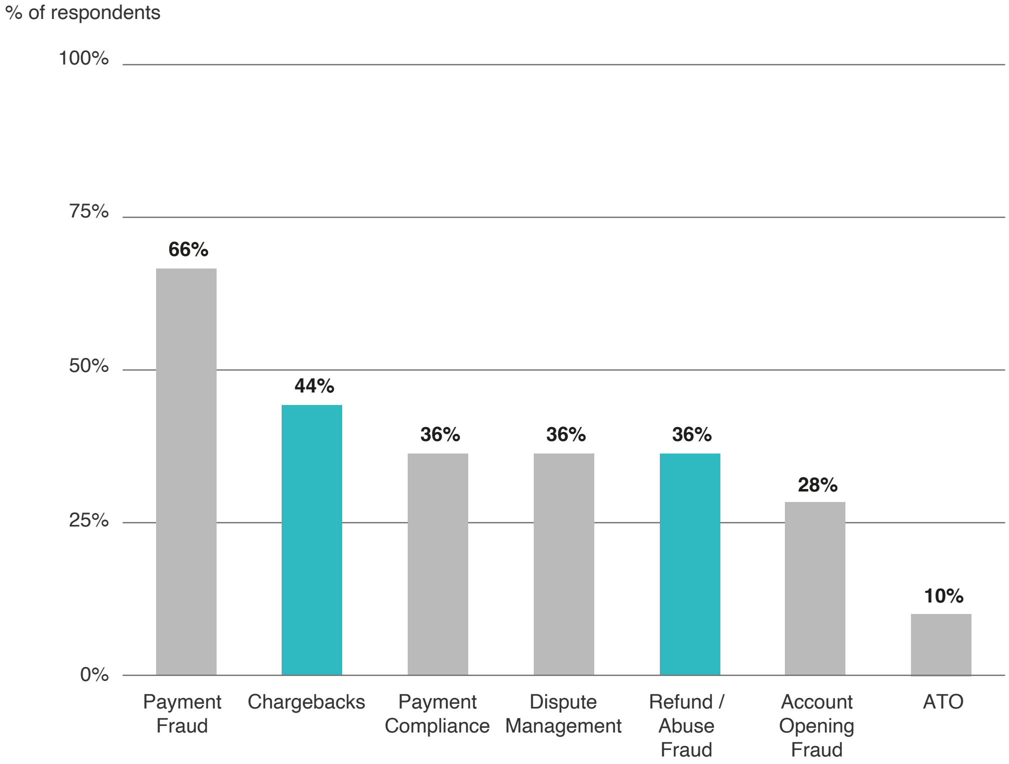


The increasing sophistication and volume of first-party fraud are prompting buyers to seek capabilities like chargeback management to better prevent first-party attacks.

Unlike conventional fraud attacks, friendly fraud is perpetrated by legitimate users who have successfully received the goods but dishonestly assert that they did not make the purchase or did not receive the products. Friendly fraud can present itself in various ways, with some common categories including chargeback fraud, return fraud, and refund fraud. Recent studies reveal a concerning trend: 35% of consumers admitted that they've engaged in first-party fraud, with over 40% of them planning on committing first-party fraud again in less than 60 days after the first event. This increase in first-party fraud leads to massive financial loss, with annual first-party loss in the US totaling more than $100 billion.[5]

This creates a major challenge with 44% of merchants citing chargeback fraud as one of their biggest market pain points, while 36% noted refund fraud as a significant pain point in their business operations (See Figure 8, on the next page). The repercussions of friendly fraud are multifaceted and extend beyond financial losses. Merchants also face heightened risks from card networks, as a rising chargeback ratio could result in the suspension or termination of their accounts, potentially leading to significant revenue losses. In the fight against friendly fraud, e-commerce merchants are actively seeking solutions that aid in the management and contesting of chargebacks. Presently, 78% of buyers employ third-party solutions to assist with chargeback management and 64% cite chargeback management as a critical product capability when assessing solution providers. Vendors specializing in transaction fraud must adapt their product roadmaps to incorporate features that assist merchants in addressing friendly fraud and if necessary, mitigating losses by providing tools for managing and contesting chargebacks.

Figure 8: What are the biggest market pain points?



Market Opportunity and Drivers

Solution providers who are able to meet buyer demands will unlock a strong overall market opportunity. Liminal projects a total addressable market (TAM) for transaction fraud prevention solutions of $7.9 billion in 2024 (see Figure 9, on the next page), increasing at a compound annual growth rate (CAGR) of 11.8% to reach $12.4 billion by 2028.[6] The market for transaction fraud prevention in e-commerce has experienced significant growth due to the expanding number of internet users, the increasing reliance on online shopping, and the widespread adoption of digital transactions, with a five-year growth rate reflective of this transformative shift (see Table 3, on page 20).

Figure 9: Transaction Fraud Solutions in E-commerce Market Size

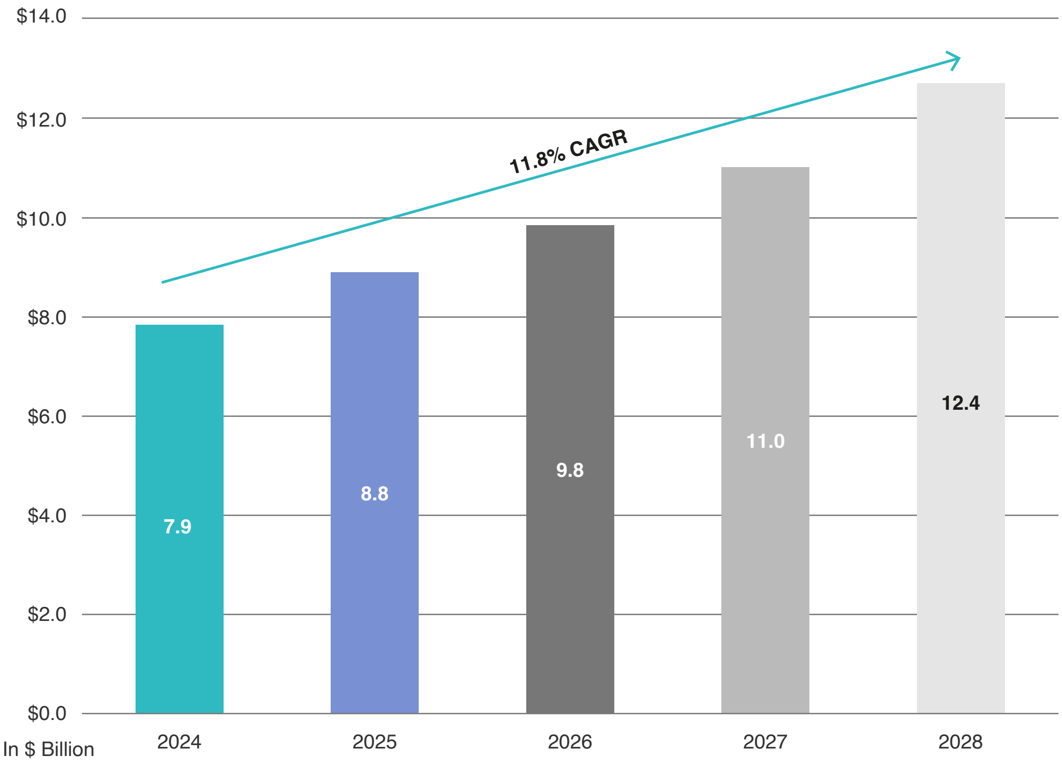


Table 3: Transaction Fraud Solution Market Drivers

Market Drivers	'24-'28 CAGR	Comments
Total Internet Users The number of internet users is increasing along with global digitization	6-7%	Growth in overall internet users is expected to increase 28% from 2024 to 2028 which will propel growth for e-commerce merchants. Growth in online consumerism is directly related to growth in fraudulent activity, which will continue to drive the market for transaction fraud prevention solutions.
New Digital Accounts Users will be creating more e-commerce accounts over time	2-3%	As various services continue digitizing, existing e-commerce users will increasingly open and manage additional accounts. The expansion of account usage heightens the potential for fraud attacks, such as account takeover fraud, which can exploit the growing digital footprint of users.
Increased Penetration of Fraud Platforms Merchants who are not presently utilizing fraud solutions are expected to in the future	1-2%	As the complexity and frequency of fraud attacks persist, merchants who have not yet embraced solutions to address loyalty/promo abuse and social engineering scams are expected to shift towards adoption.
Net Adjustment for Pricing Various factors can affect overall pricing and reflect buyer expectations	2-3%	54% of solution seekers have experienced pricing increases over the past twelve months and continue to expect to pay more in the future. In other markets, we have typically seen a 2-3% pricing increase on top of inflationary expectations.
Total	11-15%	Global accessibility to e-commerce is poised to propel digital transactions, creating an imperative for transaction fraud solutions. The escalating sophistication and prevalence of fraud attacks will potentially empower vendors to consider price increments for their solutions, further fueling overall market growth. As a result, the market is expected to grow at a CAGR of 11-15% over the forecast period.

Future Outlook

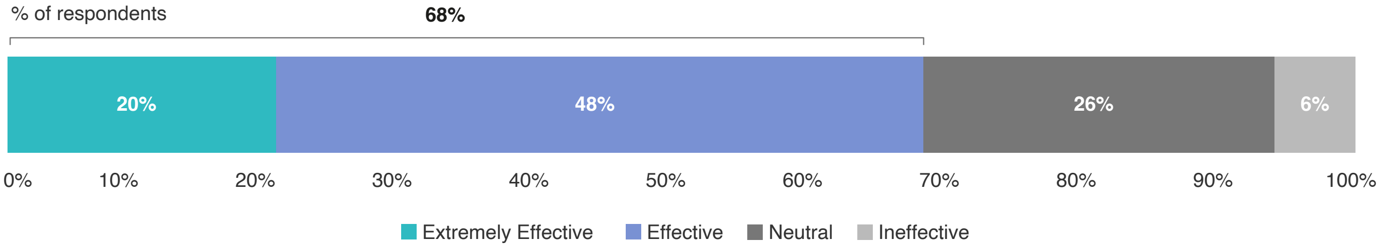
As e-commerce merchants and fraud prevention vendors look towards the future, there are several key and emergent trends that can enable buyers to obtain better solutions that combat fraud, without dramatically impacting the end-user experience.

Solutions capable of performing identity verification during onboarding not only mitigate the risks of fraud but also deliver immediate value to e-commerce merchants.

Merchants are introducing more rigorous onboarding checks, recognizing the effectiveness of identity verification procedures at the point of account creation to mitigate transaction fraud further down the customer lifecycle. 68% of buyers believe that implementing identity verification for transaction fraud prevention can be effective or extremely effective, while only 6% consider it ineffective (see Figure 10, on the next page). This data underscores the attractiveness of vendors providing platform solutions with a diverse range of capabilities, presenting a holistic approach to combating fraud.

Despite the potential impact of identity verification on preventing fraud in e-commerce, it is imperative for vendors to consider its effects on the user experience. Buyers remain cautious of solutions that add friction and may lead to cart abandonment. Hence, vendors must carefully evaluate the modalities and methods they use to conduct verification. Specifically, merchants should explore passive verification methods, such as behavioral analytics and device and location intelligence, to minimize manual data entry from end users.

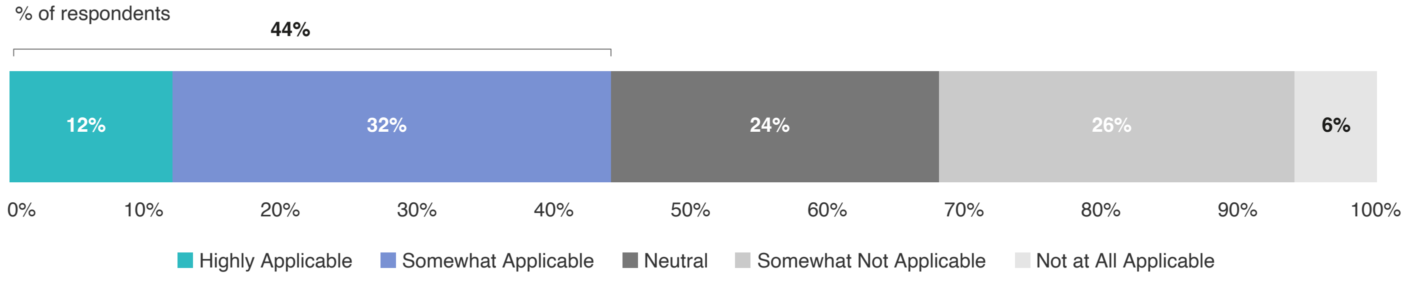
Figure 10: How effective do you feel identity verification processes are in combating transaction fraud?



While not a necessity in the majority of cases, buyers are recognizing the growing relevance of Language Learning Models (LLMs) when providing real-time customer service.

Language Learning Models (LLMs) are types of ML models like chatbots and virtual assistants that merchants can use to enhance their fraud detection and prevention strategy. LLMs detect suspicious and fraudulent data by analyzing text data, scanning emails and messages, and powering chatbots to interact with users and identify potentially fraudulent behavior during online transactions. 44% of buyers responded that LLMs can be somewhat or highly applicable to fraud prevention solutions, while only 6% feel LLMs do not apply to their fraud detection strategies (see Figure 11, on the next page). The integration of LLMs when offering real-time assistance may not only reinforce fraud detection and prevention capabilities, but it also furnishes users with around-the-clock support without necessitating additional employees. A reduction in headcount requirements can help merchants realize savings on employee costs while concurrently enhancing the efficiency of their customer service.

Figure 11: How applicable are large language models (LLMs) to your fraud prevention strategy, such as for the use of chatbots and virtual assistants?



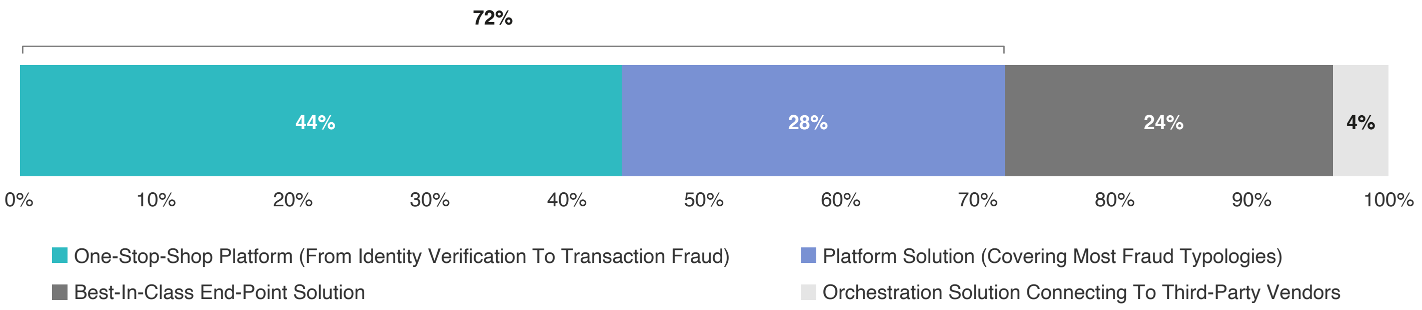
Buyers are looking for consolidated solutions rather than one best-in-class endpoint solution, underscoring a need for vendors to create more robust fraud detection platforms that span the customer journey.

Merchants have two primary approaches to fraud prevention solutions: opting for a single best-in-class endpoint solution or aggregating various solutions. On average, they engage with approximately 1.95 vendors for each fraud prevention use case. Consequently, a single buyer may need to integrate more than ten different vendors to combat the spectrum of fraud typologies effectively. Integration is seen as a major pain point for 52% of buyers, highlighting the demand for solutions that can amalgamate fraud prevention capabilities across the entire customer lifecycle.

There is strong demand for an all-in-one platform, with 72% of buyers expressing a preference for bundling a combination of solutions to create a more comprehensive array of fraud prevention options (see Figure 12, on the next page). Buyers are already making a shift, as 67% of buyers have plans to adopt an Integrated Identity Platform (IIP) within the next year. Integrated Identity Platforms (IIPs) are comprehensive digital identity solutions that orchestrate technologies and network data sharing to streamline processes across the consumer lifecycle.

Consolidation yields numerous advantages for buyers, including the ability to diversify their fraud defense strategies, the potential for tailored or specialized solutions, and the flexibility to add or adjust their fraud prevention models. This approach ultimately results in enhanced fraud detection, reduced dependency on a singular solution, and offers customization and scalability options to buyers.

Figure 12: What do you value most in a transaction fraud solution?



Buyer's Guide

The market for fraud prevention solutions is rapidly expanding, leading to the emergence of new vendors and existing vendors developing new solutions. Selecting the appropriate anti-fraud system for merchants is a crucial yet time-intensive undertaking. This decision has far-reaching business impacts, affecting fraud rates, conversion rates, revenue, and the overall user experience. Before engaging with potential vendors and evaluating their solutions, it is imperative that buyers establish a clear understanding of their implementation strategy. Buyers should outline their goals, set realistic timelines, establish a budget, and prioritize requirements before obtaining buy-in from key stakeholders. Here are some key questions to consider before proceeding (Tables 4-14):

Questions to Ask Internally

Table 4: Questions to Ask Internal Stakeholders

Objective	Example Question
Gain internal alignment with key stakeholders	What are our objectives for implementing a transaction fraud solution?
Gain consensus among the team on how to evaluate potential solutions	Rank the importance of the business requirements the solution should satisfy
Conduct a current state assessment of current solutions in place	What teams, processes, and technologies enable our fraud prevention capabilities today?
Understand what is going well and what is not for the current solution in use	What are the strengths and weaknesses of the current solution being used?
Consider the implications of altering the tech stack on other departments or teams	What teams, processes, and technologies will be impacted by the proposed solution?
Establish realistic expectations of what the solution can provide	What does success look like?
Establish a budget to allocate towards a solution	What budget are we able to allocate YoY towards a solution?
Establish a realistic timeline for the process of identifying, evaluating, and selecting a solution	What is the purchasing cycle for this solution?
Establish a team that will identify, evaluate, and select a solution	Who will be responsible for making a purchase decision?

Once internal alignment has been reached, here are some additional questions to consider when evaluating vendor solutions:

Questions to Ask Vendors

Solution Overview

Objective: The goal of asking these questions is to get an overall understanding of the product and solution offered by the vendor. This includes understanding the functionality of the solution, its main market use cases, and what sets it apart from competitors.

Table 5: Overview Questions to Ask Vendors

Objective	Example Question
Gain a baseline understanding of the product's capabilities	What are the core functionalities of this product, and how do they cater to various user needs?
Understand how the solution differentiates itself from competitors	What features set this solution apart from other competitors?
Evaluate whether the key verticals align with your business needs	What industries or verticals has this solution proven to be most effective in?
Evaluate how the platform stays ahead of the curve	How does the platform address emerging trends and industry shifts to ensure its relevance and competitiveness in the market?

Technical Capabilities

Objective: The goal is to establish the product's efficacy in addressing fraud. Additionally, it aims to gauge the effectiveness and comprehensiveness of the product in preventing fraud, along with the quality of explanations and analysis it provides.

Table 6: Questions to Ask Vendors to Understand Technical Capabilities

Objective	Example Question
Understand the real-time capabilities of the solution	How does the system's real-time transaction monitoring technology contribute to its fraud prevention strategy, and what advantages does this approach offer in mitigating fraud?
Evaluate different models and how they detect hidden patterns in transactions	What models (e.g., ML, rule-based systems) are utilized in this solution, and how do they uncover patterns indicative of fraud in transactions?
Explore the potential for utilizing the company's existing data	How can a company's existing data be leveraged within the solution to enhance fraud detection, and what types of data are most beneficial?
Obtain clarity on the solution's decision-making process	How does the solution provide transparency in its decision-making process to ensure trust in the fraud detection mechanisms?
Analyze reporting and analytics tools	What reporting and analytical tools and dashboards are available to provide insight into trends and performance?
Improve performance of existing fraud detection capabilities	Are there any supplementary features or strategies beyond our key requirements that help mitigate various fraud risks effectively?
Understand how AI/ML are leveraged to identify fraud behavior	Can you explain the role of ML and AI in detecting and adapting to transaction fraud?
Demonstrate practical examples of fraud detection rules	Can you provide examples of how fraud detection rules have successfully identified and prevented fraudulent activities?

Performance Metrics

Objective: The goal is to assess the solution’s effectiveness in identifying potential fraud, its speed, and its performance relative to established KPIs.

Table 7: Questions to Ask Vendors to Assess Performance

Objective	Example Question
Assess the overall effectiveness of the solution	How does the solution measure its overall effectiveness in preventing fraud, and what key performance indicators are considered in this assessment?
Evaluate the solution’s effectiveness in minimizing false positives and false negatives	How does the solution optimize the balance between minimizing false positives and false negatives, and what impact does this have on fraud detection efficiency?
Evaluate the solution’s ability to provide real-time analysis while delivering against established service-level agreements (SLAs)	How does the solution ensure real-time analysis on transactions without compromising on low latency?
Understand the speed at which solutions can process transactions	What is the typical transaction processing speed of the solution, and how does it accommodate high transaction volumes without sacrificing accuracy?
Identify the primary performance metrics to demonstrate the success of a solution	What are the key metrics that showcase the effectiveness of your fraud detection solution in preventing and detecting fraudulent activities, and how are these metrics monitored and reported?

Integration and Scalability

Objective: The goal is to determine how seamlessly the solution can be integrated within an e-commerce platform and to assess the solution’s ability to accommodate growth and increased transaction volumes.

Table 8: Questions to Ask Vendors to Assess Integration and Scalability Requirements

Objective	Example Question
Understand the ease and compatibility of integration	How seamlessly does the solution integrate into existing systems, and what level of support is offered for integration with a company’s existing infrastructure?
Assess the solution’s ability to accommodate growth	How does the solution adapt to the changing needs and growth of an organization, in terms of transaction volume, customer base, and user base?
Understand the time and effort needed for integration	What is the typical timeframe and level of effort needed for organizations to successfully integrate this solution into their existing infrastructure?
Establish nuances of supervised vs. unsupervised ML models	Does the solution require ongoing model training and maintenance to identify fraud patterns effectively?
Establish integration capabilities via APIs or SDKs	Does the solution provide integration options through APIs or SDKs, and what kind of customization do they offer?

Customization and Flexibility

Objective: The goal is to assess the solution's capacity for customization to meet unique e-commerce requirements, including the ability to define risk tolerance thresholds. It is also important to evaluate the solution's adaptability in identifying and responding to emerging fraud tactics.

Table 9: Questions to Ask Vendors to Assess Customization & Flexibility

Objective	Example Question
Determine whether the solution can be customized to unique business needs	How customizable is the platform, and can we tailor the solution to our specific fraud detection requirements?
Define risk thresholds in line with organizational risk tolerance	Can businesses establish and adjust their own risk limits?
Customize alert thresholds based on user profiles	Can the solution be customized to adjust alert thresholds for individual user profiles

Data

Objective: The goal is to evaluate the security and compliance standards of the solution to ensure data privacy, reliability, and adherence to leading practices.

Table 10: Questions to Ask Vendors to Assess Data Security

Objective	Example Question
Assess the measures in place to safeguard customer data	What are the security measures and protocols implemented by the solution to safeguard sensitive data and ensure compliance with data protection laws and regulations?
Verify whether the solution meets industry certifications and standards	Which industry certifications and standards has the solution attained, and how do these certifications validate its adherence to security benchmarks?
Identify the data sources used for model training	What are the primary data sources that the solution utilizes for training these models, and how are these sources selected and maintained?
Evaluate the expertise of the team in ML	Do you have in-house ML specialists or do you leverage third parties, and how does this contribute to the development and improvement of the fraud detection models?

Support and Updates

Objective: The goal is to evaluate post-integration support and the ongoing commitment of the solution provider to fulfill expectations over time.

Table 11: Questions to Ask Vendors to Assess Post-Integration Support

Objective	Example Question
Assess the level of support and assistance provided post-integration	How do you offer support and assistance to businesses after integration, and can you provide specific examples of post-integration support services?
Understand the solutions' commitment to stay up to date with fraud techniques	What strategies and mechanisms does the solution employ to continuously adapt to evolving fraud techniques, and how frequently are these tactics reviewed and updated to stay responsive to the changing threat landscape?

Pricing and Contractual Terms

Objective: The goal is to evaluate the pricing structure and contract terms associated with the solution in order to make informed decisions and plan effectively.

Table 12: Questions to Ask Vendors to Assess Pricing Structure and Contract Terms

Objective	Example Question
Understand the pricing structure	Can you provide a detailed breakdown of the pricing structure and model for this solution, including pricing tiers and cost factors?
Identify additional hidden costs beyond the base pricing	Are there additional costs that are not included in the base price, and what scenarios or circumstances may lead to these additional costs?
Gain clarity on the contract terms and duration of the solution	What is the standard contract duration, and what are the terms for renewal or termination?

Roadmap

Objective: The goal is to gain insight of the solution provider's strategic roadmap, with a focus on ensuring alignment with business needs, technological advancements, and customer requirements.

Table 13: Questions to Ask Vendors to Assess Their Strategic Roadmap

Objective	Example Question
Gain insights into the solution provider's product roadmap and plans for the future	What are the key features, enhancements, or developments planned for the future, and how do these align with evolving customer needs and industry trends?
Understand the vendors' strategy and commitment to innovation	What are key milestones on your product roadmap for the next two years?

References

Objective: The goal is to obtain references from current or previous customers who have utilized the solution, with the aim of confirming both the achievements and limitations linked to the solution.

Table 14: Questions to Ask Vendors to Assess References from Current/Previous Clients

Objective	Example Question
Gather evidence of the solutions' effectiveness and real-world impact	Can you share specific case studies from businesses that have implemented your solution, highlighting how it has effectively reduced fraud, improved security, and any measurable outcomes achieved?
Identify challenges or limitations associated with the solutions	Are there any known challenges or limitations current clients have faced with your solution, and how do you address or mitigate these issues?

Notable Vendors

The vendors included in the list encompass a range of providers in the transaction fraud prevention market in e-commerce. This includes well-established players as well as newer entrants, particularly those with distinctive features that set them apart and enable them to cater to evolving buyer demands. Each vendor in the list exhibits leading product capabilities aligned with those found in the Product Capabilities section (page 10).

Company	Product(s) Name	Brief Product Description
Accertify	Accertify Chargeback Management	Accertify offers a comprehensive fraud management and chargeback management product to assist businesses in preventing and managing fraud effectively. Their solutions aid large global merchants in handling millions of disputes while offering a wide range of tools to identify and prevent various forms of fraud, including account takeover, account origination schemes, and payment fraud.
ADVANCE.AI	ADVANCE.AI Fraud Intelligence	ADVANCE.AI's Fraud Intelligence tool provides continuous monitoring and analysis of network-based fraudulent activities, using AI technologies like text analytics and ML to offer data-driven approaches for fraud prevention, regulatory compliance, and security. It aids in devising effective risk management strategies by integrating multiple AI techniques, ensuring reliability in fraud prevention efforts.
Apruvd	ApruvdComplete, ApruvdRevive, ApruvdCustom	Apruvd offers three solutions: ApruvdComplete for chargeback protection, ApruvdRevive to minimize false declines and improve customer experiences, and ApruvdCustom for tailored order review. These solutions help businesses effectively manage order assessments and maintain secure transactions.
Bolt	Bolt Platform	Bolt focuses on reducing checkout friction to boost conversion rates and encourage repeat purchases through a one-click checkout option. They provide tailored solutions for both mid-market businesses and enterprises, aiming to simplify the purchasing process and enhance the checkout experience for customers.
Castle	Castle Rules, Castle Analytics, Castle Scoring	Castle offers a suite of fraud prevention solutions, including Castle Rules for real-time responses to account abuse and Castle Analytics for centralized activity monitoring. Castle Scoring employs ML to detect and prevent account fraud, collectively bolstering security and safeguarding user accounts against potential threats.
Chargeback Gurus	Chargeback Gurus Platform	The Chargeback Gurus platform provides a range of services, including chargeback protection, alert management, chargeback management, and social engineering and scam detection. It uses a combination of human expertise, AI, and white-glove service to fight chargebacks, recover revenue, and obtain data-driven insights that improve customer satisfaction and retention.

Company	Product(s) Name	Brief Product Description
ClearSale	ClearSale E-commerce Fraud Protection	ClearSale provides an E-commerce Fraud Protection platform with a focus on chargeback management, offering reliable security solutions. In collaboration with industry leaders, ClearSale aims to deliver technology-driven solutions that enhance fraud detection and prevention while maintaining customer trust in e-commerce operations.
Covery	Covery Card-Not-Present Fraud Protection, Covery Account Takeover Fraud Protection	Covery provides fraud protection solutions, including Card-Not-Present Fraud Protection to reduce risks like chargeback fraud and account takeovers, enhancing customer security. Additionally, their Account Takeover Fraud Protection solution safeguards against reputation damage, and bank account takeover at every stage of the customer journey.
Cybersource	Cybersource Decision Manager	Cybersource Decision Manager is a fraud detection system that employs ML to score transaction risks, allowing businesses to swiftly identify legitimate, suspicious, and novel transactions. Leveraging insights from Visa's vast transaction network, it continuously refines its models, enabling businesses to efficiently enhance transaction security, strengthen fraud prevention measures, and streamline their operational processes.
DataDome	DataDome Bot & Online Fraud Protection	DataDome's Bot & Online Fraud Protection service, powered by AI and ML technology, efficiently addresses fraud with its high data processing capacity and a low false positive rate. Its user-friendly dashboard enables performance monitoring and response customization, making it a valuable solution for fraud detection and prevention.
DataVisor	DataVisor Platform	DataVisor provides a comprehensive and user-friendly ML driven fraud platform that integrates with various data sources, including a knowledge graph feature that visually represents fraud-related insights by connecting data points from internal and external sources, uncovering relationships between entities, events, financial transactions, and geographical locations.
Deep Labs	Deep Labs DeepRisk	Deep Labs' DeepRisk is an advanced financial transaction risk identification solution that uses predictive capabilities to proactively prevent losses and maintain a strong reputation. It focuses on persona and signals-based intelligence, providing comprehensive insights beyond standard fraud detection, and is trusted for its robust risk assessment and prevention.
Entersekt	Entersekt 3DSecure	Entersekt's 3DSecure solution enhances payment authentication with risk-aware technology and the Transakt suite, which establishes a secure link between a customer's digital identity and their mobile app or web browser. This unique device token ensures security across multiple services.
Eye4Fraud	Eye4Fraud Platform	The Eye4Fraud platform utilizes advanced ML technology with persona and dynamic scoring to assess customer profiles and enhance security, effectively detecting irregularities in customer data and adapting to evolving threats for continuous protection.

Company	Product(s) Name	Brief Product Description
Fingerprint	Fingerprint	Fingerprint utilizes a combination of advanced techniques, including browser fingerprinting, IP/URL analysis, and ML, to accurately identify nearly 99.5% of unique visitors while countering tactics like incognito browsing and VPN usage. It generates unique visitor IDs, links fraud patterns to individuals, and offers crucial detectors for hardware signal spoofing, browser feature masking, and user-agent deception identification, providing granular probability scores for precise threat detection and improved data quality.
Forter	Forter Platform	Forter is an advanced fraud prevention platform designed for online retailers to enhance transaction security, reduce false declines, and optimize customer conversion rates. Leveraging technologies like the identity graph, network effects, and an AI/ML-driven decision engine, it offers real-time assessments of identity trustworthiness to ensure a secure online shopping experience.
Fraud.net	Fraud.net Transaction AI, Fraud.net Application AI	Transaction AI and Application AI by Fraud.net are robust tools for financial institutions and digital merchants to strengthen fraud prevention. Transaction AI offers real-time monitoring and actionable insights, while Application AI provides real-time risk assessment, collectively delivering a comprehensive approach to reduce fraud by validating legitimate customers and blocking fraudulent ones.
FraudFix	FraudFix Platform	FraudFix is an AI-driven online fraud protection platform that enhances security by utilizing AI algorithms and ML to create custom fraud rules for accurate detection. Its customizable APIs allow seamless integration with diverse platforms, offering businesses a versatile and comprehensive solution to combat fraudulent activities.
FraudLabs Pro	FraudLabs Pro Fraud Prevention Solution	FraudLabs Pro's Fraud Prevention Solution is designed to safeguard online businesses from card-not-present (CNP) fraud, helping to minimize chargebacks and losses while ensuring smooth transactions for legitimate customers. It provides comprehensive fraud reports and is particularly useful for businesses operating in the Asia Pacific region, offering reliable and robust fraud prevention measures.
HUMAN	HUMAN Bot Defender	HUMAN Bot Defender is a bot management solution that utilizes behavior-based technology to safeguard websites, mobile apps, and APIs from automated attacks, enhancing operational efficiency while reducing the risk of data breaches.
IDMerit	IDMTrust, IDMkyc, IDMaml	IDMerit offers three key solutions to reinforce security and regulatory compliance: IDMTrust provides risk scores based on email, phone, and IP address factors, IDMkyc provides identity verification and fraud detection with data from over 400 official sources across 178 countries, and IDMaml that empowers organizations with compliance programs, fraud reduction, and real-time risk mitigation, featuring profile matching and media screening capabilities. Collectively, these solutions enhance security and regulatory compliance efforts.
Justt	Justt Platform	Justt utilizes artificial intelligence to assist global merchants in combating false and fraudulent chargebacks. Their customized AI system integrates with each merchant's card processor, gathers evidence to counter unwarranted chargeback claims, and submits this information to credit card companies, relieving businesses of the burden of handling such disputes independently.

Company	Product(s) Name	Brief Product Description
Konduto	Konduto Performance, Konduto Complete	Konduto Performance and Konduto Complete are fraud prevention solutions tailored for e-commerce, retail, and payment providers. They utilize real-time user behavior tracking, ML algorithms, and device fingerprinting to detect and prevent fraud effectively, with Konduto Complete providing risk scoring and detailed reporting for manual and automated reviews.
Kount	Kount Dispute and Chargeback Management, Kount Central	Kount offers a comprehensive fraud detection and prevention suite that enhances the security of digital payments and accounts. Their solutions, such as Kount Dispute and Chargeback Management and Kount Central, streamline inquiry management and provide proactive fraud prevention, respectively, using AI-driven technology to detect high-risk behaviors and improve revenue streams and value-added services for payment service providers and merchants across various vertical markets.
LexisNexis Risk Solutions	LexisNexis Dynamic Decision Platform, LexisNexis RiskNarrative	The LexisNexis Dynamic Decision Platform provides a unified gateway for delivering fraud and identity solutions through a single API integration, empowering clients to make precise trust and risk management decisions. In addition, within the LexisNexis Risk Solutions ecosystem, the TruNarrative Platform, now known as LexisNexis RiskNarrative, offers advanced features for managing financial crime workflows, orchestration, and decision-making processes.
Mastercard	Ethoca, ekata, nudata	Mastercard utilizes Ethoca, ekata, and nudata fraud solutions to bolster fraud prevention and dispute resolution. Ethoca's Fraud Insights for Merchants gives merchants a holistic perspective on fraud, chargebacks, and declines within their Mastercard portfolio. Ekata uses global identity data for smarter identity verification in reducing friction and combatting fraud. Lastly, nudata helps solve fraud within use cases such as account creation, account access, and digital transactions in financial institutions and e-commerce.
MaxMind	minFraud by MaxMind	minFraud by MaxMind is a data return service that assists businesses in combating online fraud by providing risk scoring and transaction data insights. It leverages ML, human expertise, and data from the minFraud network to offer fraud detection for online transactions.
Netacea	Netacea Platform	Netacea uses a server-side approach to bot management, employing their Intent Analytics engine to assess requests, signals, and patterns, and offering a risk-based scoring system with real-time blocking, redirection, or challenge options. It also provides threat alerts and data-rich dashboards, systematically enhancing web traffic security and mitigating automated threats for websites, mobile apps, and APIs.
Nethone	Nethone KYU	Nethone's proprietary fraud prevention platform employs the KYU approach to create comprehensive user profiles by collecting over 5,000 attributes per session, including device details, network characteristics, and user behavior. Using AI and ML models, Nethone generates user risk profiles, assesses transactions, and offers recommendations through a user-friendly dashboard, utilizing data from its KYU profiler, client sources, and third-party providers to enhance fraud prevention efforts.
NoFraud	NoFraud Protection, NoFraud Checkout	NoFraud provides a comprehensive suite of solutions to improve e-commerce security and enhance the shopping experience, with NoFraud Protection offering real-time, accurate fraud screening to increase approval rates and provide financial guarantees for effective fraud prevention. In addition, NoFraud Checkout aims to reduce cart abandonment and improve the shopping experience, making it more convenient, particularly for first-time shoppers.

Company	Product(s) Name	Brief Product Description
nSure.ai	nSure.ai Platform	nSure.ai leverages advanced AI technology to offer insurance-backed fraud detection services designed for merchants dealing in digital goods, particularly high-risk items such as electronic gift cards, airline tickets, and event tickets.
Nuvei	Nuvei Payment Platform	Nuvei's payment platform offers a range of fraud and risk management tools, such as identity manager, smart 3DS2 service, tokenization, PCI management, and chargeback management, alongside a global payment gateway connecting businesses to banks worldwide. Nuvei maintains PCI Level 1 service provider standards, ensuring robust security and risk mitigation for businesses.
Outseer	Outseer Fraud Manager	Outseer Fraud Manager is a transactional risk management platform that employs ML and a robust policy engine to secure customer accounts at every digital journey stage, effectively evaluating and mitigating risks. With advanced data science technology and unique consortium data, it enables clients to combat the latest fraud trends with risk models trained on billions of transactions, making it a reliable solution for enhancing security.
Radial	Radial Fraud Protection	Radial Fraud Protection provides a full-service solution designed to protect businesses from e-commerce fraud throughout the transaction process, ensuring efficient detection and prevention of fraudulent activities to enhance the overall security and integrity of online operations.
Ravelin	Ravelin Platform	Ravelin is a flexible fraud detection and prevention platform that utilizes user PII and behavioral data to identify suspicious patterns, effectively reducing false positives and mitigating chargebacks. It offers a high degree of customization which allows businesses to adapt the platform to their specific needs, and it detects fraud signals while offering insights into customer behavior and network activities.
Riskified	Riskified Platform	Riskified offers an advanced AI platform that specializes in e-commerce fraud prevention, utilizing ML algorithms to differentiate between legitimate and fraudulent customers, offering a 100% chargeback guarantee.
Sardine	Sardine Platform	The Sardine platform provides a versatile solution that includes fraud prevention, KYC, and AML regulatory compliance for financial services, crypto, and NFT-related transactions. It offers pattern monitoring and irregularity detection, providing a comprehensive payment protection suite with fraud indemnification, instant bank ACH fund settlement, and fast bank ACH to crypto on-ramp functionality, empowering businesses to navigate complex financial landscapes with confidence.
SEON	SEON Platform	The SEON platform is a powerful AI-powered fraud management system designed to decrease fraud rates and offers an intuitive admin panel for easy operation. It features various integrations, device fingerprinting, behavioral analytics, access to a shared data pool, custom rule configurations, advanced analytical tools, and a user-friendly graphical interface, making it a comprehensive solution for fraud prevention.

Company	Product(s) Name	Brief Product Description
SHIELD	SHIELD Device Intelligence, SHIELD ComplianceAI	SHIELD offers two solutions for businesses: Device Intelligence profiles devices in real-time to enhance fraud prevention and build trust without inconveniencing customers, while ComplianceAI is an enterprise-grade fraud prevention solution powered by AI technology.
Sift	Sift Platform	Sift's platform provides protection against a wide range of fraud types, utilizing real-time ML models and a vast global data network processing one trillion events annually. With the ability to assess 16,000 signals, it excels in fraud detection, offering both a global model and custom model creation to meet specific business requirements.
Signifyd	Signifyd Commerce Network	Signifyd provides a commerce protection platform that helps businesses minimize chargeback losses, prevent incorrect declines, and reduce the costs of manual transaction investigations and fraud-related operations. It leverages adaptive AI and ML, along with the Signifyd Commerce Network's extensive data, to identify anomalies, offer actionable insights, and prevent policy abuse for merchants across the globe.
Stripe	Stripe Radar	Stripe Radar provides an advanced fraud detection and prevention solution that utilizes ML to identify and stop suspicious transactions.
Sumsub	Sumsub Transaction Monitoring	Sumsub's solution empowers companies to establish a comprehensive AML and anti-fraud transaction monitoring process, ensuring ongoing security and compliance beyond the initial onboarding process.
TransUnion	TransUnion TruValidate	TruValidate by TransUnion offers a comprehensive solution for businesses by connecting proprietary data, personal information, device identifiers, and online behaviors to detect anomalies, evaluate risks, and confidently identify genuine consumers. It enables businesses to prioritize personalized customer experiences while maintaining robust protection against fraudulent activities.
Vesta	Vesta Platform	Vesta Platform is a global transaction guarantee solution that uses advanced AI and ML to streamline online purchases, ensuring high approval rates for a smooth customer experience while reducing false declines and increasing valid approvals. The platform also provides fraud protection, particularly against common fraud attacks like chargebacks.

Appendix

Definition of Terms

Account Takeover Fraud	The unauthorized access of a legitimate consumer account by a fraudster, to initiate fraudulent transactions
Automated Transaction Monitoring	Process of computerization of monitoring of consumer transactions to provide a complete picture of consumer activity
Behavioral Profiling	The practice of analyzing patterns of behavior to identify and categorize individuals or groups of people
Bot Detection	The process of analyzing traffic to a website, mobile application, or API to detect and block malicious bots
Breached Credentials	The procurement of account credentials via malware placed directly on a consumer's computer, or purchased from hackers selling account information on the black market
Chargeback Fraud	A consumer initiating a credit card chargeback with their bank under false pretenses (e.g., claiming an item was damaged or defective when it was delivered in good condition)
Chargeback Management	Tools that enable merchants to manage chargeback-related workflows and successfully win chargeback disputes
Chargeback Protection	Services used to reduce chargeback rates or provide reimbursement for the costs associated with a chargeback
Credential Stuffing	The use of account credentials obtained for an unrelated website, in an attempt to access additional accounts held by the consumer that use a shared password
Device Fingerprinting	Process of combining specific attributes of a device to create a unique device identity. Attributes may be derived from software and hardware and include device type, operating system, IP address, language settings, and more
Device Risk-Scoring	A subcategory of risk scoring that assesses the trustworthiness of a device
Dynamic Friction	Adjusts verification based on a user's trustworthiness. As a user progresses, each action is assessed for risk. High-risk interactions trigger added verification, while trustworthy ones streamline the experience without any needed additional verification steps (e.g., 3DS2)
First-Party Fraud, Friendly Fraud	Fraud committed against an e-commerce platform by a consumer, from their own account
Location Intelligence	Analysis of an electronic device's physical location to identify potential risks

Merchant Monitoring	Active analysis of merchant behavior, sales, chargeback, and other patterns that may fluctuate after initial onboarding
Payment Fraud	The use of stolen payment credentials to purchase goods via an account created by the fraudster. This can include both credit/debit card numbers or bank account/routing numbers
Phishing	The extraction of a consumer's account credentials using a fake login page that tricks the user into sharing their password
Proxy and VPN Detection	Proxy/VPN detection identifies if an IP address is either a VPN or proxy
Real-time Fraud Monitoring	The surveillance and analysis of networks, accounts, and transactions to identify potentially fraudulent activity in near-real time for automated fraud decisioning
Refund Fraud	A consumer requesting a refund directly from the merchant under false pretenses (e.g., claiming an item was not received when the package was properly delivered)
Return Fraud	A consumer initiates a return of a delivered item and requests a refund, but fails to mail the return or mails the box back empty
Rules-based Transaction Monitoring	Detecting suspicious consumer transaction activity based on a predefined set of rules and conditions
Signal Sharing Network	Networks that enable communication between organizations to share information regarding trusted users and bad actors
Social Engineering & Scam Detection	Rules-based or ML models configured to identify consumer behavior indicative of social engineering – a user being manipulated to approve or initiate a fraudulent transaction using valid login credentials
Social Engineering Scams	The use of manipulation techniques to convince a consumer to initiate a transaction from their account on behalf of the fraudster
Third-Party Fraud	Fraud committed against an e-commerce platform by threat actors using the compromised accounts of an existing, legitimate consumer, or accounts opened using faked or stolen identity data
Transaction Risk-Scoring	Transaction risk scoring is the process of assessing the riskiness of a transaction. Risk scores are calculated by inferential statistical models based on established rulesets
User Risk-Scoring	Assessing the riskiness of an individual user and the likelihood of fraud, chargebacks, or other undesirable behavior

Survey Response Appendix

Survey Demographics: E-commerce Respondents

Figure 13: Survey Respondents by Role

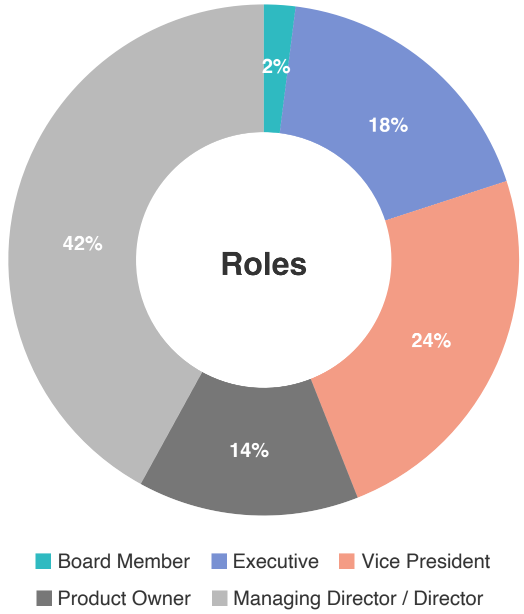


Figure 15: Survey Respondents By Company Size (Total Number of Customers)

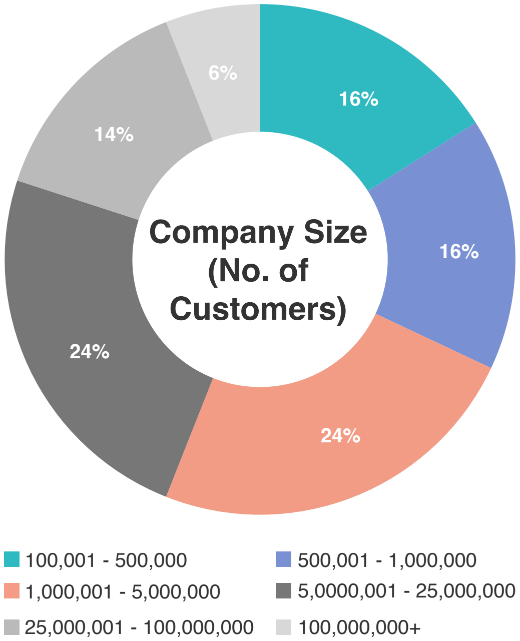


Figure 14: Survey Respondents by Geographic Region

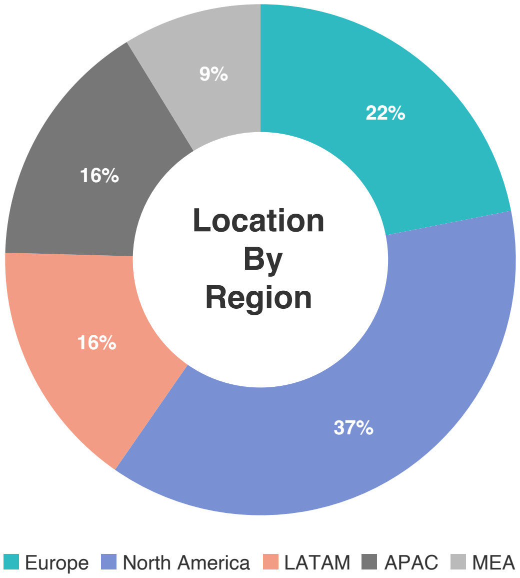
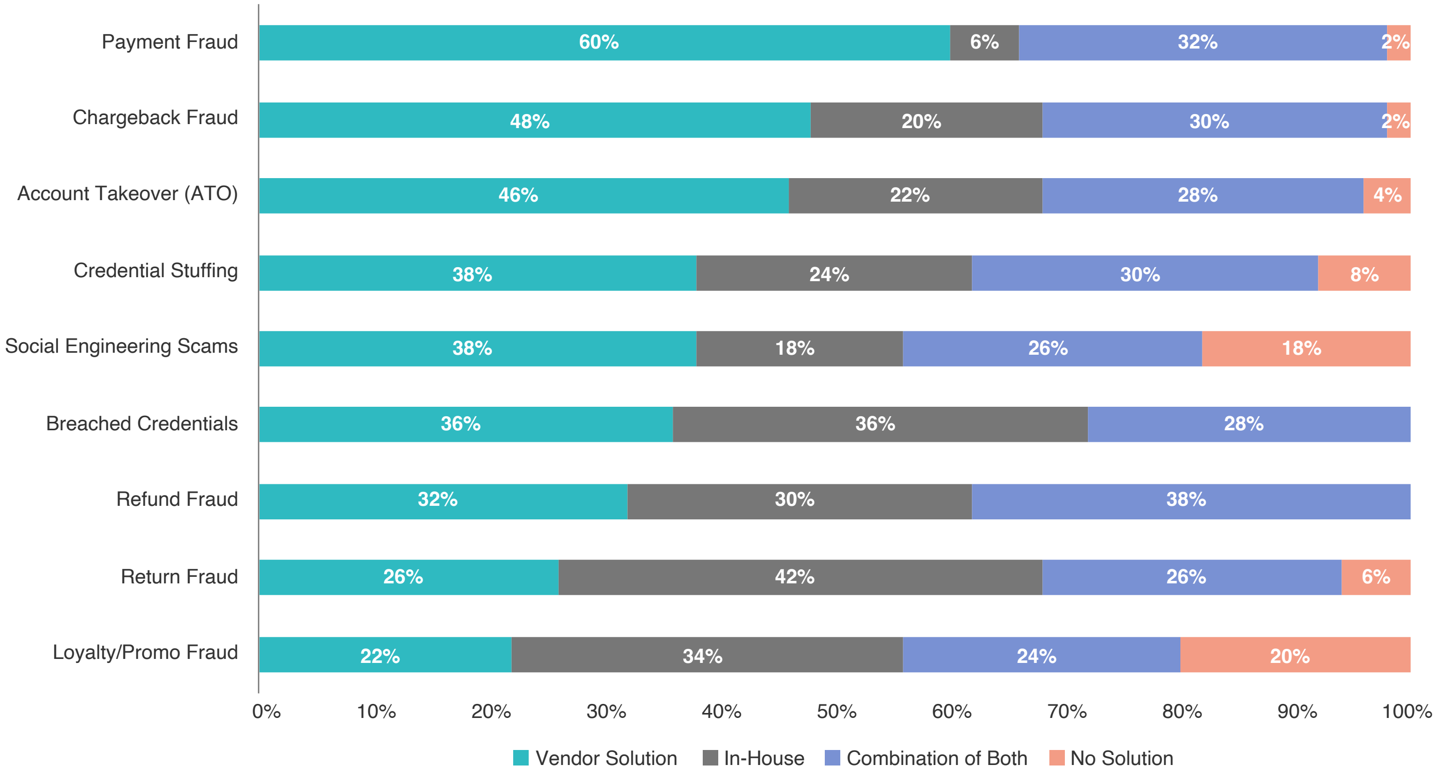


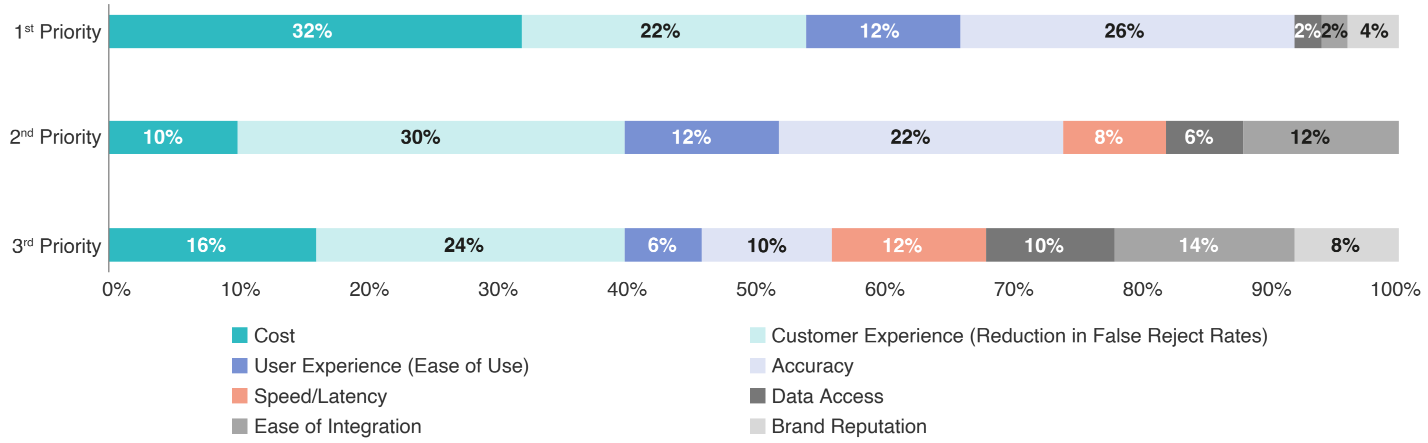
Figure 16: Based on each of the fraud typologies below, please specify whether you mainly solve for fraud with in-house solutions or vendor solutions?



Key Findings:

When examining different fraud typologies, return fraud is primarily addressed using in-house solutions. On the other hand, for third-party fraud such as payment fraud, buyers tend to rely more on vendor solutions. For refund fraud, buyers often adopt a combination of both in-house and vendor solutions. Merchant preferences indicate an inclination towards in-house or combination solutions to combat first-party fraud like return fraud, refund fraud, loyalty fraud, promo fraud, and chargeback fraud. In contrast, merchants overwhelmingly rely on third-party vendor solutions to combat third-party fraud such as payment fraud. It is worthy to note that all survey respondents have a solution in place to combat refund fraud, emphasizing the prominence of this fraud typology in the e-commerce marketplace.

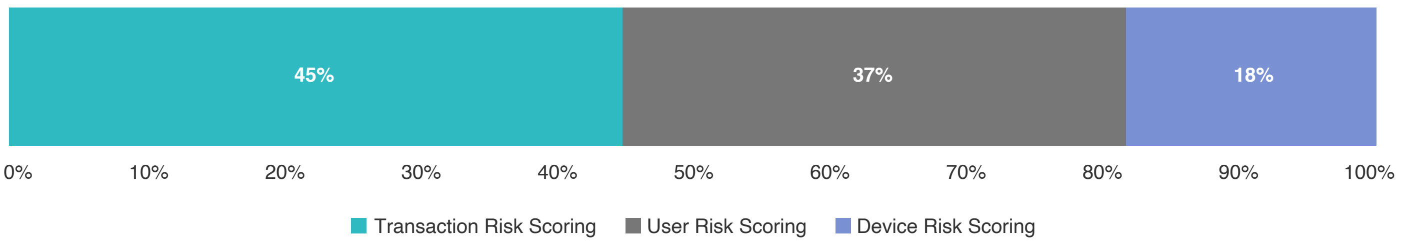
Figure 17: What are your most important key purchasing criteria (KPCs) for selecting a transaction fraud vendor?



Key Findings:

Cost and accuracy emerged as the top two key performance criteria (KPCs) for buyers, indicating that buyers prioritize solutions that offer the best return on investment. Additionally, a combined preference for customer experience (i.e., reduction in false reject rates) and user experience (i.e., ease of use) underscores a profound concern for how their customers interact with their platforms and the efficiency of their transaction processing.

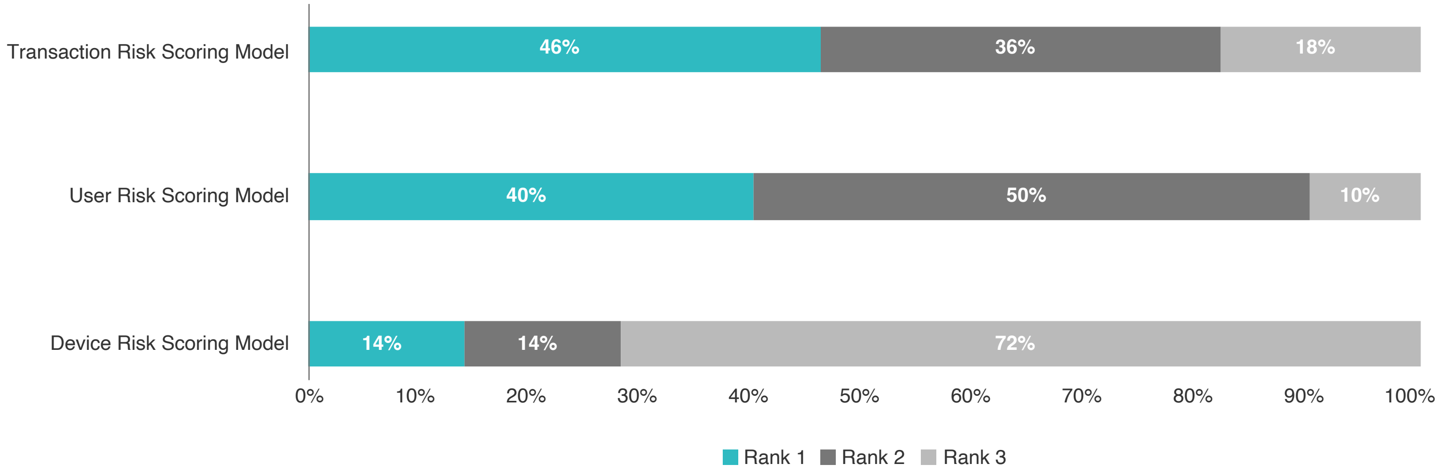
Figure 18: What risk-scoring models do you use during checkout?



Key Findings:

Most respondents employed two out of three models (user risk scoring, transaction risk scoring, or device risk scoring), during the checkout process. Transaction risk scoring, which evaluates transactions and assigns a risk score based on available data signals, was the most widely used model. Given the prevalence of guest checkout options and the ability to shop across multiple devices, merchants tend to favor using transaction-level data. While additional data signals like user risk scoring can be beneficial, stronger privacy regulations may make it more challenging for fraud platforms to utilize user-level PII to assess transaction legitimacy.

Figure 19: Rank the risk-scoring models by their efficacy in stopping transaction fraud



Key Findings:

In terms of effectiveness for preventing transaction fraud, transaction risk scoring models were ranked the highest, while device risk scoring models were rated the least effective. This ranking reflects a reduced reliance on device-level data. Customers often shop using multiple devices, some of which merchants may recognize, while others may be unfamiliar. Relying solely on device risk scoring models would provide an incomplete view of the transaction, as the device could be new or used by a different user. In contrast, by incorporating transaction and user risk scoring models, merchants can analyze the actual transaction activity and make informed decisions regarding user behavior during the transaction, leading to a more comprehensive assessment.

Bibliography

1. Liminal Market Study, September 2023, surveying 88 e-commerce and online retail buyers across North America, Europe, LATAM, APAC, and ME&A.

2. Liminal Market Study, October 2023, surveying 50 e-commerce and online retail buyers across North America, Europe, LATAM, APAC, and ME&A.

3. TransUnion. (October 2023). "2023 State of Omnichannel Fraud Report." Transunion Resources.

4. J.P. Morgan. (March 6, 2023). "False Positives & Fraud Prevention Tools." J.P. Morgan Resources.

5. Socure. (October 2023). "Identity Risk Insights: Defining and solving the elusive challenge of first-party fraud." Socure Resources.

6. Liminal's proprietary market sizing model, constructed using a bottoms-up approach, grounded in a comprehensive assessment of the total potential demand for solutions.

Contact Information

Liminal is a market intelligence and strategic advisory firm specializing in digital identity and cybersecurity solutions within the fintech and payments sector while also catering to the private equity and venture capital community. Since 2016, Liminal has offered strategic and analytical services supporting executive decision-making at all stages of product or business lifecycles. We advise some of the world's most prominent business leaders, investors, and government officials on building, acquiring, and investing in the next generation of digital identity solutions and technologies.

Liminal Strategy, Inc.
825 Third Avenue, Suite 1700
New York, NY 10022

For information about our advisory services, market intelligence platform, or memberships, **sales@liminal.co**

For citations and media inquiries, **media@liminal.co**

Visit **Liminal.co**

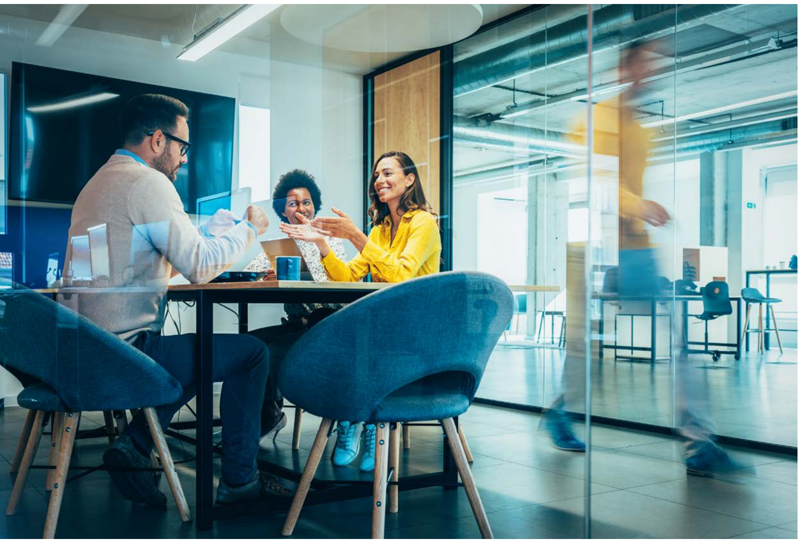
Looking for more insights?

With the Link™ platform, you can access the latest industry trends and research, tools that enable you to benchmark and compare company profiles, and explore features that will inform your next strategic move to gain an unfair competitive advantage.

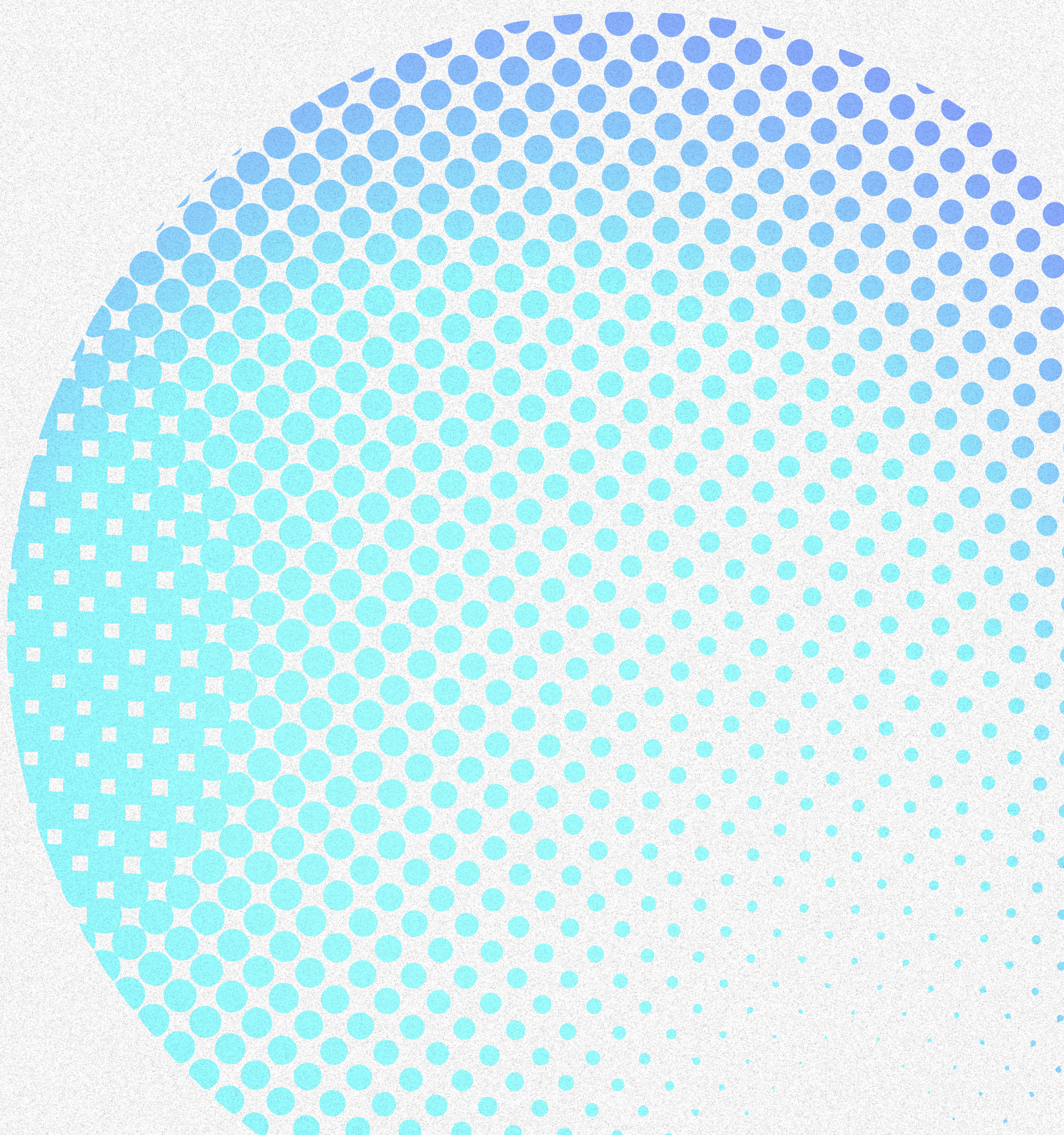
If you're an existing customer, log into the Link platform **here**.

If you're curious about Link, visit our website and sign up for a free **trial**.

To receive updates on new Liminal research, events, and thought leadership, **subscribe to our Newsletter**.



liminal.co



Liminal™