datos INSIGHTS

May 2024

E-Commerce Fraud Landscape and Trends: Merchants Seeking to Adapt

David Mattei and Gabrielle Inhofe

May 2024

E-Commerce Fraud Landscape and Trends: Merchants Seeking to Adapt

David Mattei and Gabrielle Inhofe

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

E-commerce merchants in the U.S. and U.K. navigate a complex landscape of competing priorities, including evolving regulatory requirements, increasingly sophisticated fraud, growing consumer demands for a frictionless experience, and a variety of different types of consumer abuses. As e-commerce fraud continues to grow, e-commerce merchants are refining their approaches to fraud loss prevention. The key findings from this report follow:

- **A robust e-commerce market has fueled rising fraud:** As consumers increasingly transact online and the use of payment cards accelerates, criminals have taken advantage of this landscape to perpetrate more fraud attacks. Datos Insights estimates net fraud losses for e-commerce merchants will reach US$43 billion by 2027.
- **Growing false declines are a major pain point for e-commerce merchants:** The average false decline rate (i.e., the fraudulent decline of a valid transaction) is 1.51% of e-commerce sales, representing lost e-commerce revenue of nearly US$265 billion by 2027. Larger merchants (those with US$1 billion and more in revenue) tend to have lower false decline rates compared to their smaller counterparts.
- **Authorization approval rates have dramatically increased:** While historically stuck in the low-to-mid 80% range, nearly 60% of merchants report approval rates above 90%.
- **E-commerce merchants rely on a suite of anti-fraud tools:** Merchants use a multiprong strategy to mitigate fraud losses by leveraging a suite of tools. Merchants are especially eager to deploy fraud alert management systems to gain a better handle on fraud and harness artificial intelligence (AI) and machine learning (ML) to strengthen accuracy, tamp down on false positives, and boost operational efficiencies.
- **Outsourcing fraud management is growing in popularity:** As fraud becomes more complex for e-commerce merchants, an increasing number have outsourced fraud loss prevention management to third parties that are better equipped to navigate the complex fraud landscape. Of those who currently outsource fraud management, many plan to outsource fraud liability responsibility to their third-party fraud providers.

Introduction

In most white-collar crime investigations, the adage is "follow the money." Fraudsters are very good at this, too; they follow consumers wherever they are spending money. It is no surprise that fraudsters have gone online as consumers continue to spend on e-commerce purchases and use cards to pay for them. Since consumers generally have zero-dollar liability for fraudulent card transactions and merchants bear the liability for fraudulent online purchases paid with a card, merchants have been actively building fraud controls to mitigate their losses.

Merchant fraud control strategies have evolved over the years as online spending has increased and fraudsters have launched more sophisticated fraud attacks. In this complex environment, merchants have faced a delicate balancing act of maximizing authorization approval rates while also minimizing fraud losses and false declines. Card-not-present (CNP) authorization approval rates continue to lag card-present (CP) authorization approval rates, much to the dismay of merchants, consumers, and card brands. Both merchants and consumers are frustrated by the wasted efforts by merchants to attract and retain customers who are then declined at the time of checkout.

This report examines how e-commerce merchants are faring in their efforts to balance competing operational objectives of maximizing authorization approval rates while also minimizing fraud losses and false declines. It provides insights into the tools merchants use in their fraud-fighting arsenal, the progress they are making in lowering their fraud losses, and the cost they bear related to false declines.

Methodology

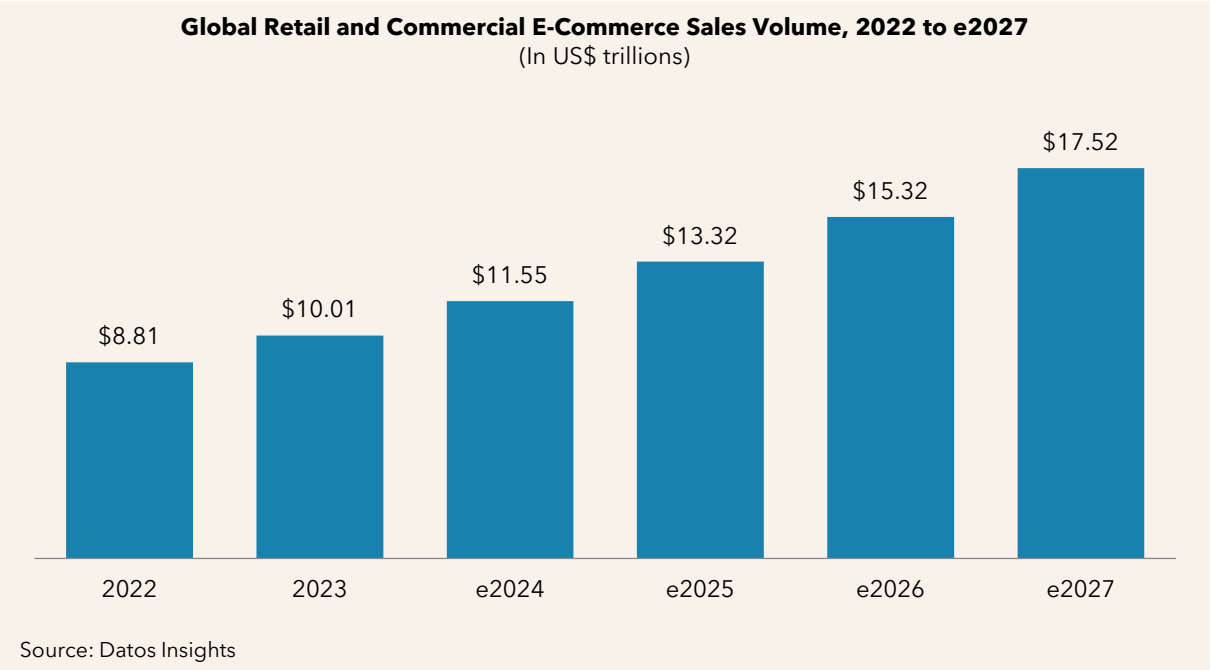
Datos Insights interviewed 200 e-commerce merchants in the U.S. and U.K. between July and September 2023. Interviewees hold senior positions at the director, vice-president, or higher levels in their companies. Fifty-four percent of the merchants have annual sales of US$1 billion or more, while 46% have annual sales between US$100 million and US$1 billion. On average, 57% of the merchants' total annual transaction volume is performed in a digital channel such as online or via mobile app.

The total sample has a margin of error of seven points at the 95% level of confidence. Statistical tests of significance were conducted at either the 90% or 95% level of confidence, depending on the sample size.

The State of E-Commerce

E-commerce is alive and well. Global sales across consumers and businesses are forecasted at US$11.55 trillion for 2024, growing to US$17.5 trillion in 2027 (Figure 1). Given the sheer scale of online spending, e-commerce remains a breeding ground for opportunity—and for fraud.

Figure 1: Global Retail and Commercial E-Commerce Sales, 2022 to e2027



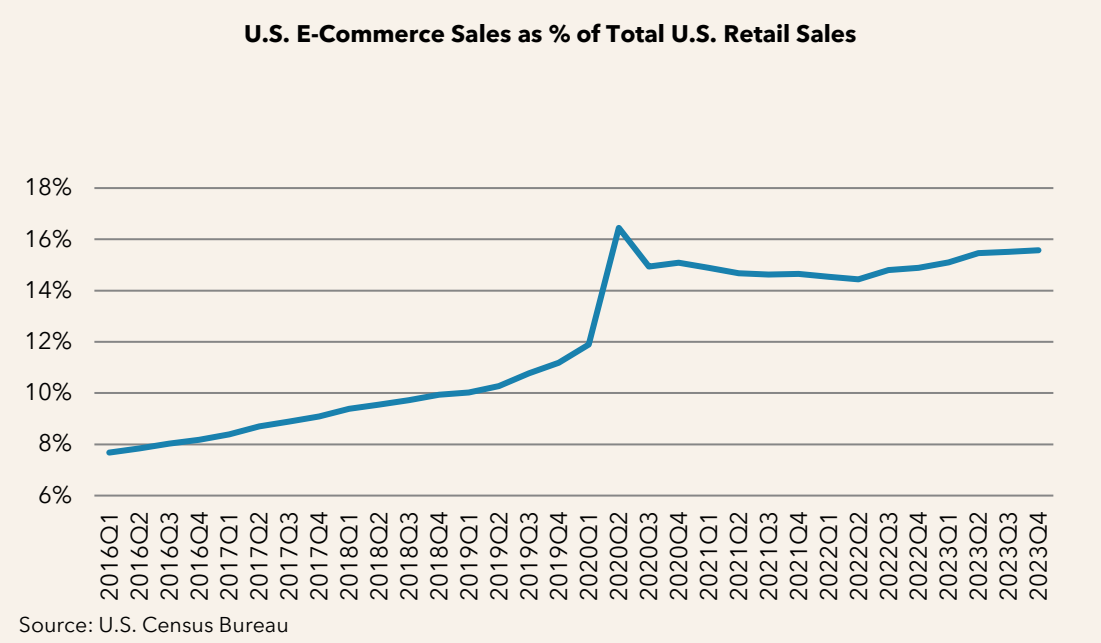
Source: Datos Insights

There are several key regional differences in e-commerce sales. The e-commerce markets in countries such as China and across Europe are more established and have higher existing penetration rates among consumers. There, online shopping is already fairly widespread; year-over-year e-commerce growth rates are in the high single-digit range. In contrast, e-commerce is still relatively nascent in emerging markets such as Latin America and the Asia-Pacific. A larger proportion of consumers in these regions are only recently gaining access to affordable internet, smartphones, and digital payments infrastructure. This allows for faster adoption as first-time online shoppers are brought into the e-commerce ecosystem, resulting in year-over-year growth rates in the mid-teens to low 20% range.

U.S. e-commerce sales in 2023 were US$1.1 trillion—15.4% of overall consumer retail spend. Still, annual growth rates have slowed considerably in the post-pandemic world

(Figure 2). Before the pandemic, U.S. e-commerce sales had healthy double-digit quarter-over-quarter growth rates, but those growth rates have moderated since Q4 2022 to approximately 7.5%.

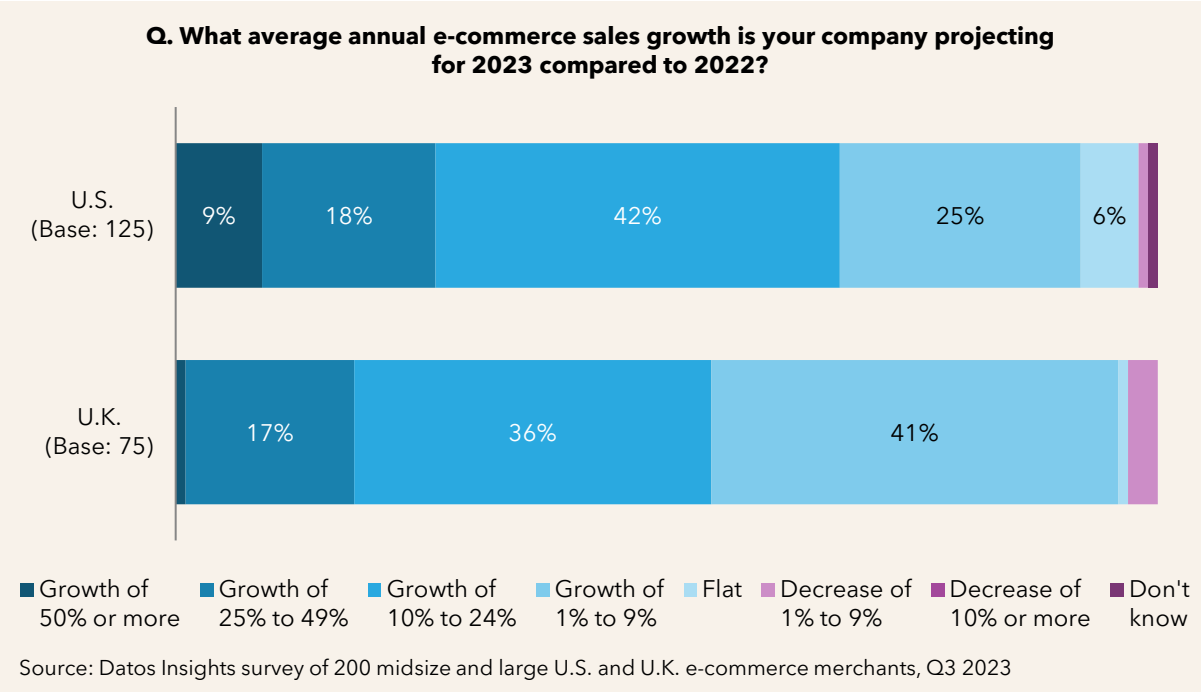
Figure 2: U.S. E-Commerce Retail Sales Statistics



Source: U.S. Census Bureau

Ninety-four percent of U.S. and U.K. merchants report their e-commerce sales are growing, which is a strong indicator of the health of e-commerce sales (Figure 3).

Figure 3: E-Commerce Merchant Sales Growth Rates, 2022 vs. 2023



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

However, upon closer examination of the data, there are signs that the sales growth rate is slowing.

When Datos Insights surveyed U.S. merchants in 2022, nearly half of them (48%) reported sales growth rates of 25% or higher compared to the prior year.[1] In the 2023 survey, only 26% of U.S. merchants reported growth rates of 25% or higher compared to the prior year. This data reflects the maturing market for e-commerce sales in the U.S.

Growth rates may be slowing, but the amount of online retail spend is substantial and remains an attractive target for fraudsters.

[1] See Datos Insights' report The E-Commerce Fraud Enigma: The Quest to Maximize Revenue While Minimizing Fraud, July 2022.

The E-Commerce Fraud Market

Datos Insights estimates global e-commerce fraud will cost merchants nearly US$29 billion in 2024 and grow to US$43.6 billion in 2027 (Figure 4). This increase represents a significant cost to merchants to sell goods and services online. It also drives the multiprong suite of fraud mitigation solutions deployed to protect e-commerce merchants.

Figure 4: Global E-commerce Gross and Net Fraud Losses 2022 to e2027

Source: Datos Insights

E-commerce merchants contend with a host of competing priorities in a complex landscape that often pits regulatory requirements against consumer demands. Table A outlines market trends and implications affecting how e-commerce merchants navigate fraud loss prevention.

Table A: The E-Commerce Fraud Market

Trends	Implications
Fraud volume and sophistication are rising	The pandemic spurred an incredible acceleration in global digitalization, and fraudsters took advantage of increased online activity to perpetrate more attacks. Meanwhile, emerging technologies facilitated a rise in the volume and sophistication of fraud. E-commerce merchants have had to refine their fraud controls in response.
Regulatory requirements are evolving	In the EU, the Second Payment Services Directive (PSD2) requires e-commerce merchants to institute strong customer authentication (SCA), which many e-commerce merchants were initially hesitant to adopt due to fears of friction and cart abandonment. Now that SCA has been in place for several years, it has clearly been effective at combating fraudulent transactions. Countries such as Australia, Japan, Mexico, and Turkey already have active initiatives underway to follow the EU's lead.
Consumer expectations of the user experience are becoming more stringent	As consumers have grown accustomed to conducting their business online, their expectations for a seamless user experience have become more stringent. In response, e-commerce merchants have had to weigh these demands alongside fraud prevention efforts.
Merchants are deploying more automation in their fraud control frameworks	As ML models become more readily available and fine-tuned, merchants with in-house fraud systems are veering away from manual rule writing to ML as their first line of defense.

Source: Datos Insights

Fraud Increasing in Volume and Sophistication

E-commerce merchants face an onslaught of sophisticated fraud tactics, and combating these threats requires significant investments in fraud detection technologies. Merchants that do not implement robust fraud prevention solutions face tremendous financial exposure from direct losses as well as fines and penalties from card networks. It is an endless cat-and-mouse game as fraudsters continually evolve their methods to bypass merchant defenses. However, overly aggressive fraud technologies can lead to user friction (and thus cart abandonment) and false declines.

First-party fraud, in which the actual cardholder deliberately makes a purchase with no intention to pay, has been a particular challenge to e-commerce merchants. Nearly half of the surveyed merchants report first-party fraud is increasing.

Evolving Regulatory Requirements

PSD2 came into effect in the U.K. on January 13, 2018, as part of the country's implementation of the EU directive. This directive aimed to increase consumer protection, foster innovation, and improve security for electronic payments. For e-commerce merchants operating in the U.K., PSD2 ushered in significant changes to how customer authentication is handled during online transactions. It mandated that SCA include at least two of the following elements: something the customer knows (such as a password), something the customer has (such as a mobile phone), and something the customer is (such as a fingerprint). This increased friction in the checkout process initially led to higher cart abandonment rates for some merchants, but PSD2 has proven to be very effective at addressing high fraud rates.

Australia, Singapore, India, South Korea, South Africa, and others have mandates that are similar to the EU's SCA. However, those mandates vary from country to country and affect when customer authentication is required, merchant exemptions from user authentication, and thresholds when it is mandatory.

In North America, the U.S. and Canada have not instituted anything similar to PSD2 at a national level. However, many North American merchants and financial institutions support stepped-up authentication methods such as 3-D Secure (3DS), which is analogous to PSD2's SCA requirements, though 3DS usage is still quite low.

Customer Experience Expectations Becoming More Stringent

As online shopping has become the norm, consumers have grown accustomed to seamless and convenient experiences. They expect e-commerce sites and apps to be highly intuitive, load quickly, and require minimal steps to complete transactions.

This emphasis on as frictionless as experience as possible is putting pressure on merchants to optimize their platforms for speed and simplicity continually. Friction points such as convoluted account creation processes or lengthy checkout flows can now lead to high cart abandonment rates. Merchants must strike a balance between meeting rigorous security and regulatory requirements while ensuring a solid customer experience.

Increasing Reliance on Automation

Businesses across the globe are adopting automated tools to bolster fraud control frameworks to drive down false positives and root out sophisticated fraud attacks. On the flipside, fraudsters are harnessing AI to make their tactics increasingly clever and difficult to detect. E-commerce merchants are shifting from manual fraud rule writing to ML models in an effort to navigate this environment.[2]

The Many Faces of E-Commerce Fraud

Historically, e-commerce merchants have had to focus on fraudulent transactions in which fraudsters would use stolen payment credentials to make a purchase. As merchants have had success combating this, new forms of fraud are growing. Moreover, the perpetrators of fraud are also expanding from traditional organized and some not-so-organized crime rings using stolen credit and debit cards to unscrupulous consumers. This is plainly evident by the high percentage of merchants who report being victims of various forms of abuse (Figure 5):

- **Refund abuse:** When a consumer initiates a request to return purchased goods and receive a refund on the original purchase amount. However, rather than returning the original items purchased, the consumer fills the box with rocks, bricks, or other items. Merchants with lenient return policies issue the refund to the consumer upon the initial request of a return. Only upon inspecting the box shipped back from the consumer does the merchant realize fraud has occurred. In other cases, the consumer will claim the goods were never received when, in actuality, the consumer did receive and is in possession of them.

- **Return abuse:** When the fraudster or consumer initiates a request to return purchased goods and receive a refund. However, the item that is returned is not the original purchased item or the damaged item. In the case of a luxury goods item, the user may return a counterfeit. In the case of clothing, the item may have been worn and unable to be resold as a new item.

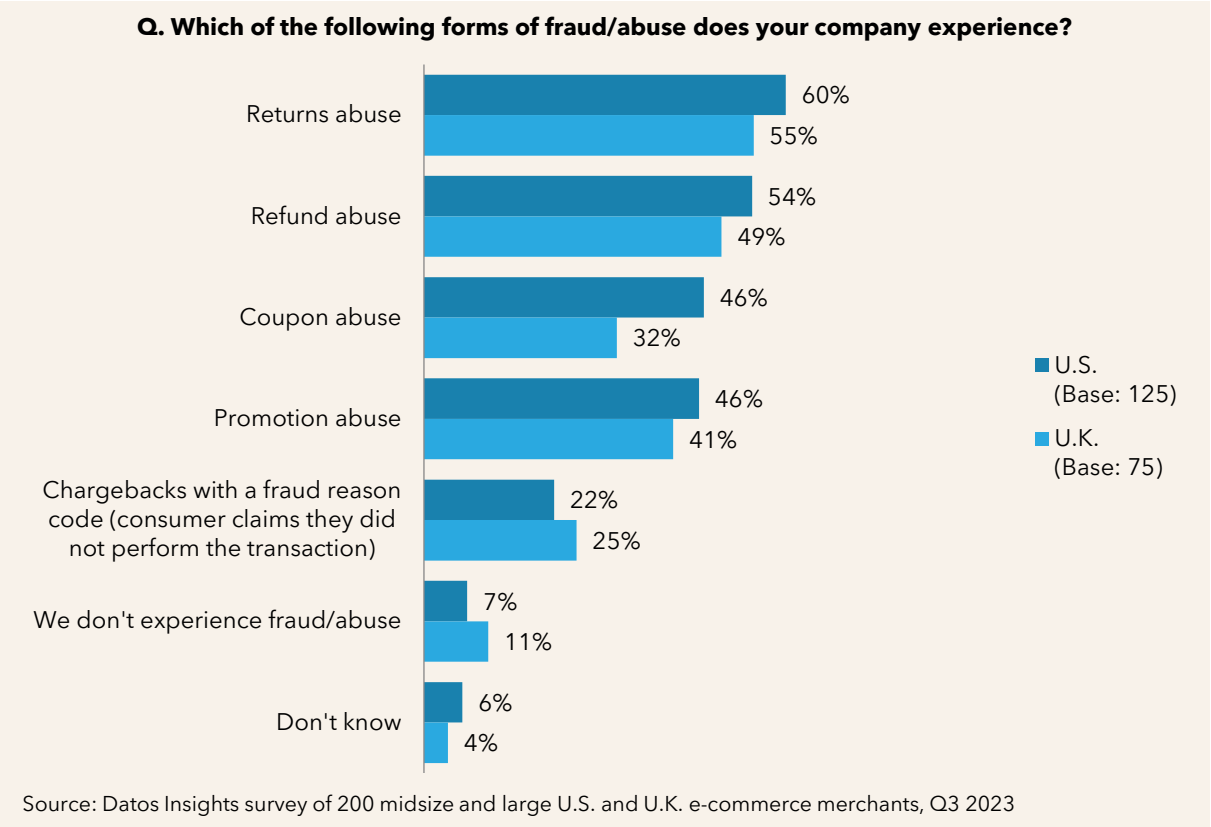
- **Coupon abuse:** When fraudsters create copies of coupons and either use them to purchase goods at a discount and resell them at a higher price or sell the coupons to others. In other cases, a consumer will complain to the merchant about being

[2] See Datos Insights' report The Double-Edged Sword of Generative AI: Fraud Perpetration and Detection, January 2024.

dissatisfied with the purchased item in the hope of receiving a coupon good for a discount on a future purchase.

- **Promotion abuse:** Often committed via automated bots trained to target a specific merchant. A merchant may offer a monetary discount on the first purchase by new customers. The bot will create multiple new accounts and make multiple purchases, entitling them to the discount. The goods are resold at a higher price and the merchant never benefits from repeat business by the supposedly new customer.

Figure 5: Types of Abuse and Fraud E-Commerce Merchants Experience



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

E-Commerce Fraud Losses

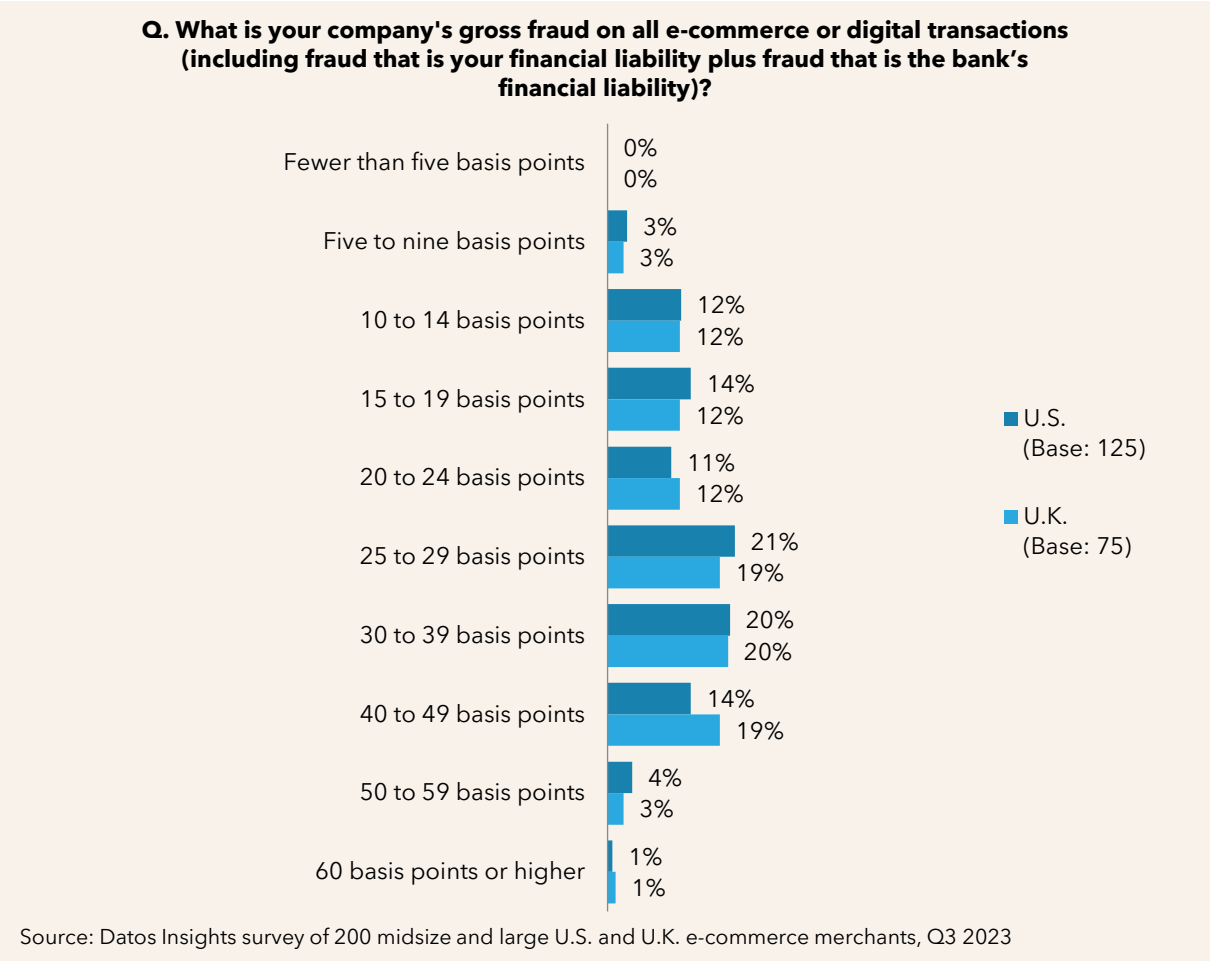
Datos Insights estimates merchants will lose nearly US$ 29 billion due to e-commerce fraud in 2024 growing to over US$ 43 billion by 2027 (Figure 4). The delta between merchant gross fraud and net fraud losses represents CNP fraud losses that are the liability of FIs.

Datos Insights estimates the weighted average gross fraud for e-commerce sales is 31.2 basis points. E-commerce gross fraud represents all fraud claims received by merchants

regardless of whether they are ultimately liable for the fraud. Merchants can defend themselves and, in some instances, avoid financial liability for fraud claims. The resulting fraud for which merchants are financially liable is referred to as their net fraud losses.

Roughly 55% of merchants report gross fraud between 25 and 49 basis points, with near equal distributions among U.K. merchants. Twenty-one percent of U.S. merchants report between 25 to 29 basis points, 20% report 30 to 39 basis points, and 14% report 40 to 49 basis points (Figure 6). These numbers remain fairly consistent across merchant annual revenue (those with less than US$1 billion versus those with greater than US$1 billion) and by e-commerce sales as a percentage of overall revenue.

Figure 6: Gross Fraud on All E-Commerce or Digital Transactions

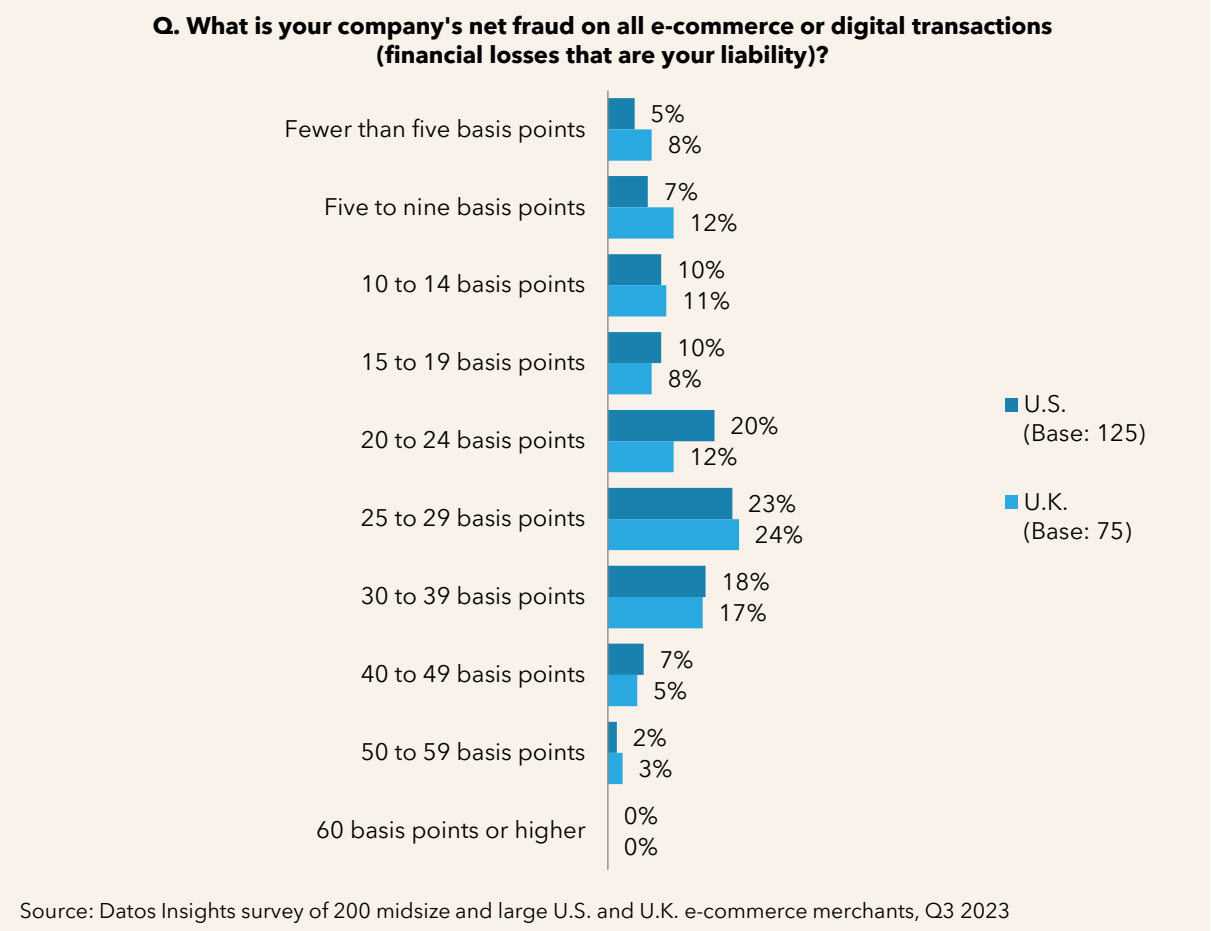


Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

Datos Insights estimates the weighted average net fraud for e-commerce sales is 24.9 basis points. Net fraud rates are relatively similar to gross fraud rates but shifted slightly lower due to merchants' ability to prove they are not liable for certain fraudulent

transactions. Roughly 60% of merchants report net fraud between 20 and 40 basis points, with similar distributions between 25 to 29 basis points and 30 to 39 basis points (Figure 7). These numbers do not vary much based on merchant sales volume, split between e-commerce vs. in-store ratios, or other characteristics.

Figure 7: Net Fraud on All E-Commerce or Digital Transactions



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

False Declines

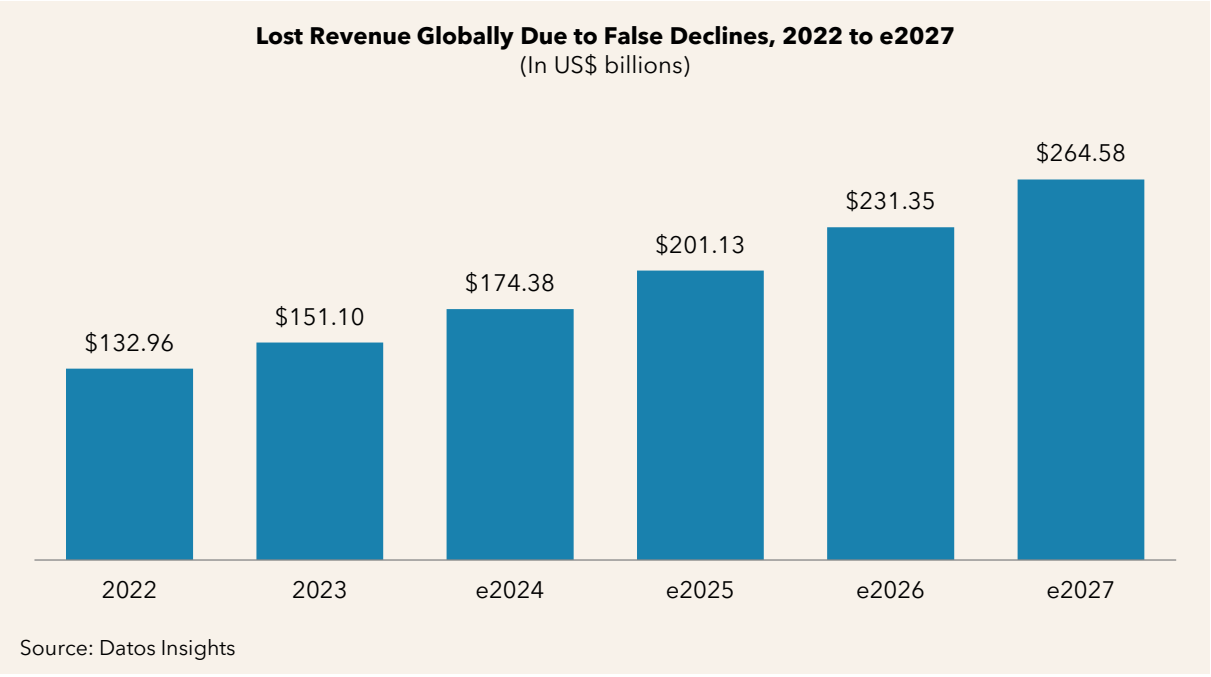
Some merchants may deploy aggressive fraud control strategies to mitigate fraud losses. Such strategies can have the unintended consequence of false declines.

False declines occur when legitimate transactions are incorrectly declined due to fraud concerns and are a significant problem for e-commerce merchants. High false decline rates can severely undermine conversion rates and brand loyalty. When a valid order is declined, the merchant loses that sale and risks losing customers' future business if they become frustrated. Merchants also dislike false declines because the fraud system just

undid all the hard work of the marketing department, which successfully attracted new customers to make a purchase—only for it to be rejected.

Datos Insights estimates the industry average false decline rate among e-commerce merchants is 1.51% of annual sales. On a global scale, this represents estimated lost e-commerce sales of nearly US$175 billion in 2024, increasing to US$265 billion by 2027 (Figure 8). False declines are the bane of an e-commerce merchant due to the lost revenue opportunity they represent and are a metric many merchants monitor.

Figure 8: Global Estimate of Lost E-Commerce Sales Due to False Declines

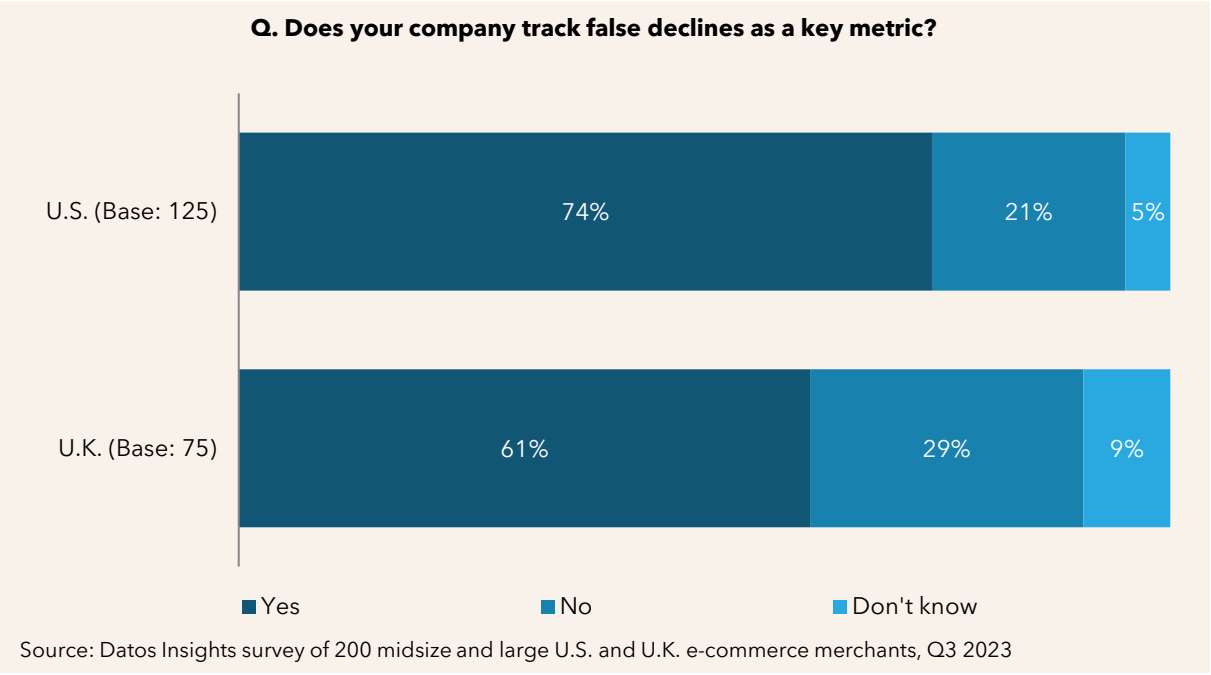


Source: Datos Insights

Tracking False Declines

Tracking false decline rates is crucial because they directly impact revenue and the customer experience. By monitoring this metric closely, merchants can identify underlying issues with their fraud prevention systems. Seventy-four percent of U.S. merchants and 61% of U.K. merchants track false declines as a key performance metric (Figure 9).

Figure 9: Percentage of Companies That Track False Declines as a Key Metric



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

Figure 10 illustrates the variety of methods used by those merchants tracking false declines to identify and track false declines. While it is possible for a merchant to deploy multiple methods concurrently, these results highlight the most popular methods:

- **A successful second attempt:** This approach captures re-attempted transactions after an initial decline. The merchant declines the first transaction due to fraud concerns, and the consumer quickly re-attempts the transaction. If the second transaction is approved by the FI and the merchant does not receive a chargeback on it, then it can be assumed the first decline by the merchant was an error. This approach is used by 35% of U.S. merchants and 33% of U.K. merchants which track false declines.

- **Inbound customer contact:** This approach captures customer calls and other communications after an initial decline. If the merchant declines customers, they may contact the merchant via a call to customer support, an email, or another communications channel supported by the merchant. While this data is coming into the call center or another part of the operations group, the fraud team must partner with their operations counterparts to collect this valuable data to improve the performance of its fraud system. This method is used by 28% of U.S. merchants and 33% of U.K. merchants that track false declines.

- **Outbound customer contact:** This approach looks to capture merchant communications confirming a suspicious transaction. FIs have long sent emails or text messages to their customers to confirm a suspicious transaction. This practice is standard within financial services but not as common among merchants as it should be. This method is used by 17% of U.S. merchants and 11% of U.K. merchants.
- **Control group:** This approach looks to capture allowed suspicious transactions without a corresponding chargeback. A merchant will purposefully approve a transaction it thinks is fraudulent to see if it results in a chargeback. If the transaction is truly fraudulent, the incoming chargeback proves to the merchant that its initial assessment was correct. However, if no chargeback is received, the merchant assumes that their assumption of fraud was incorrect. This approach is used by 16% of U.S. merchants and 24% of U.K. merchants that track false declines.

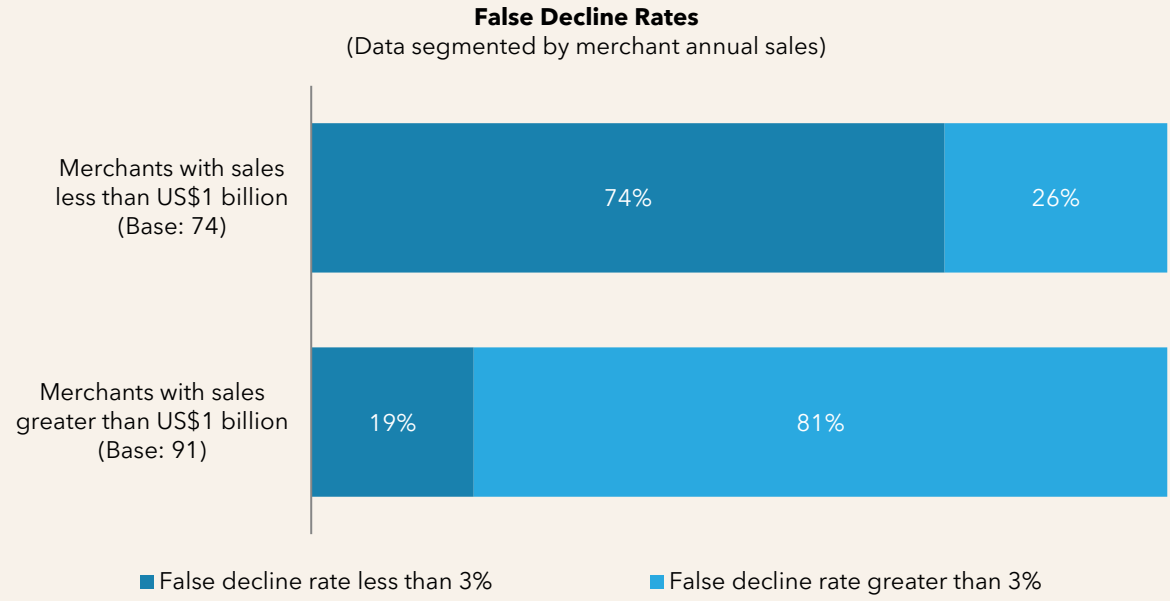
Figure 10: Methods Used to Measure False Declines

Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

Large vs. Smaller Merchant False Decline Management

Interestingly, larger merchants manage false declines better than smaller merchants. Seventy-four percent of merchants with less than US$1 billion in annual revenue have false decline rates above 3%, whereas 81% of merchants with more than US$1 billion in annual revenue have false decline rates of less than 3% (Figure 11).

Figure 11: False Decline Rates by E-Commerce Sales Volume



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

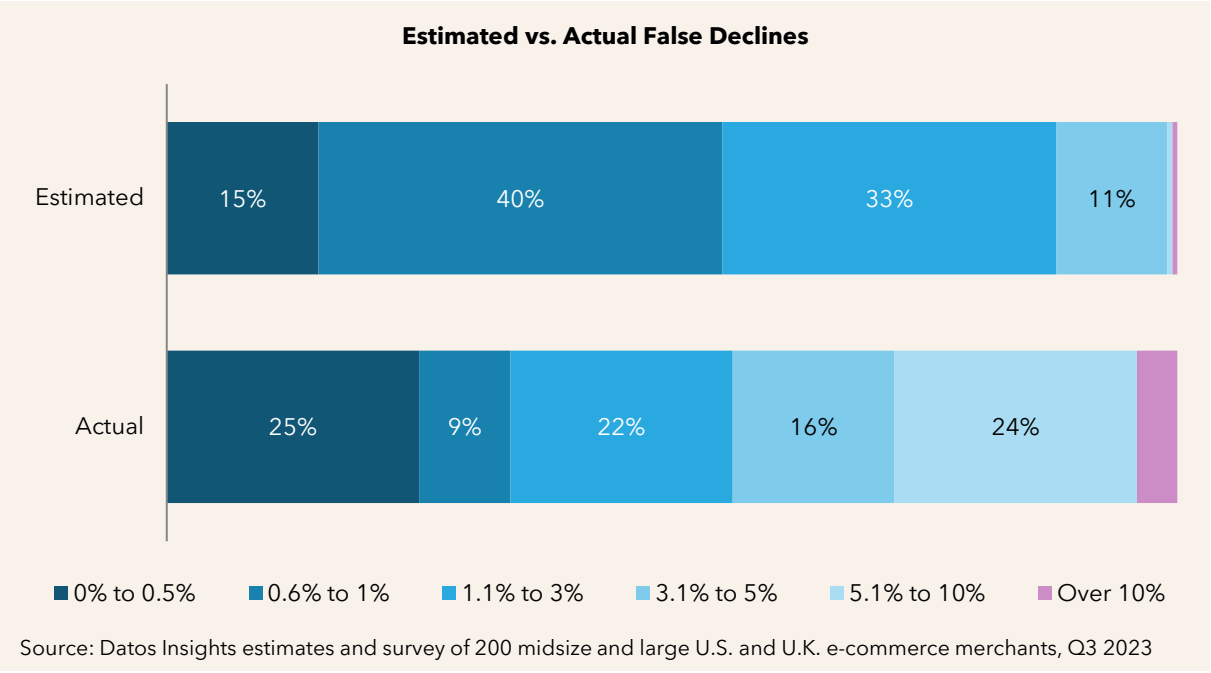
Larger merchants tend to have more resources and tools to manage fraud and the staff to perform analyses to manage false declines. False declines also represent a significant source of revenue opportunity for them. They are likely to have experienced more consumer complaints regarding false declines and have made the needed changes to address this issue and the resulting revenue impact it has.

False Declines: Perception vs. Reality

With false declines, there may be a disconnect between merchant perceptions and realities; merchants tend to underestimate their false decline rates, thinking it is better than their actual rates. Datos Insights asked merchants to estimate their false decline rates and also calculated the actual false decline rates based on data provided by the merchants.

Fifty-three percent of merchants estimate their false decline rate to be less than 1%. However, based on Datos Insights' calculations, only 34% of merchants have a false decline rate of less than 1%. On the other end of the spectrum, the percentage of merchants with an actual false rate of more than 3% is 44%. Yet only 12% of merchants estimate their false decline rate to be 3% or higher. Clearly, merchants may have a rosier belief of their false decline rates versus what they really are (Figure 12).

Figure 12: Merchants' Perception vs. Reality of Their False Decline Rates



Source: Datos Insights estimates and survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

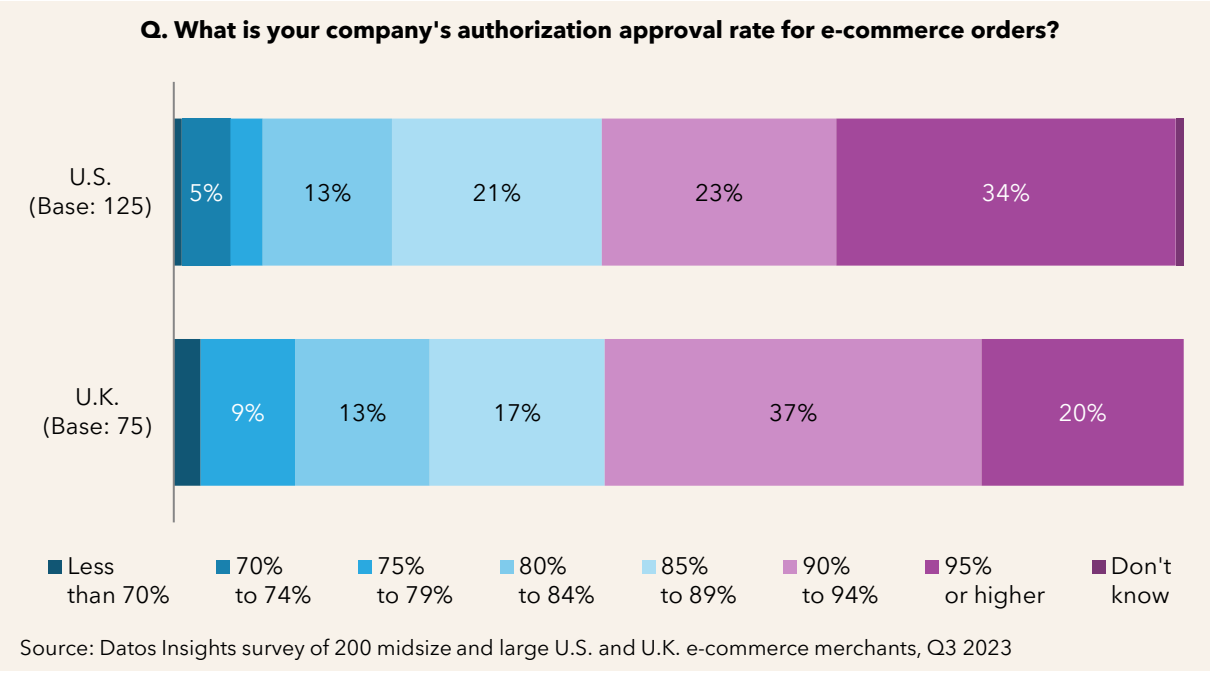
The gap between perception and reality highlights the ongoing need for merchants to manage false declines more diligently. This metric is important to increase revenue and customer satisfaction. Merchants should know their actual performance number and work constantly to lower it.

Authorization Approval Rates

Authorization approval rates have been a hotly debated and analyzed metric in the e-commerce industry for many years. Traditionally, the rates have been in the low-to-mid 80% range, whereas CP authorization approval rates have been in the high 90% range.

Some of that difference is warranted as fraudsters migrated from CP fraud to CNP fraud when EMV cards were introduced. However, that does not explain the gap entirely. Overly zealous merchant and FI fraud systems are declining too many good transactions. The industry has been working for years to close the gap between CNP and CP approval rates. Progress is finally being made, with 57% of U.S. and U.K. merchants reporting authorization approval rates in the 90% range (Figure 13).

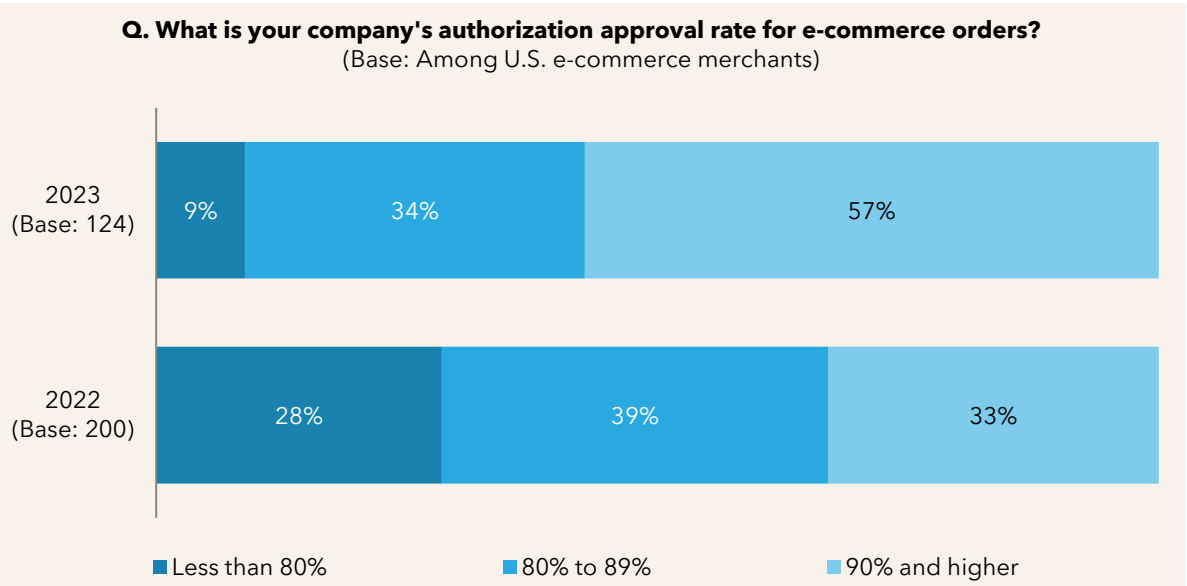
Figure 13: Authorization Approval Rates for E-Commerce Orders



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

Among U.S. merchants, authorization approval rates have dramatically improved from 2022 to 2023. The percentage of merchants reporting approval rates below 80% shrunk from 28% in 2022 to 9% in 2023. Moreover, the percentage of merchants reporting approval rates of 90% or higher jumped from 33% in 2022 to 57% in 2023 (Figure 14).

Figure 14: Authorization Approval Rate Improvements, 2022 vs. 2023



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023, and Datos Insights survey of midsize and large U.S. e-commerce merchants, 2022

Of particular interest is the change in the percentage of merchants reporting approval rates of 95% and higher, which is on par with CP rates. In 2022, only 7% of U.S. merchants were in this tier compared to 34% of merchants in 2023.

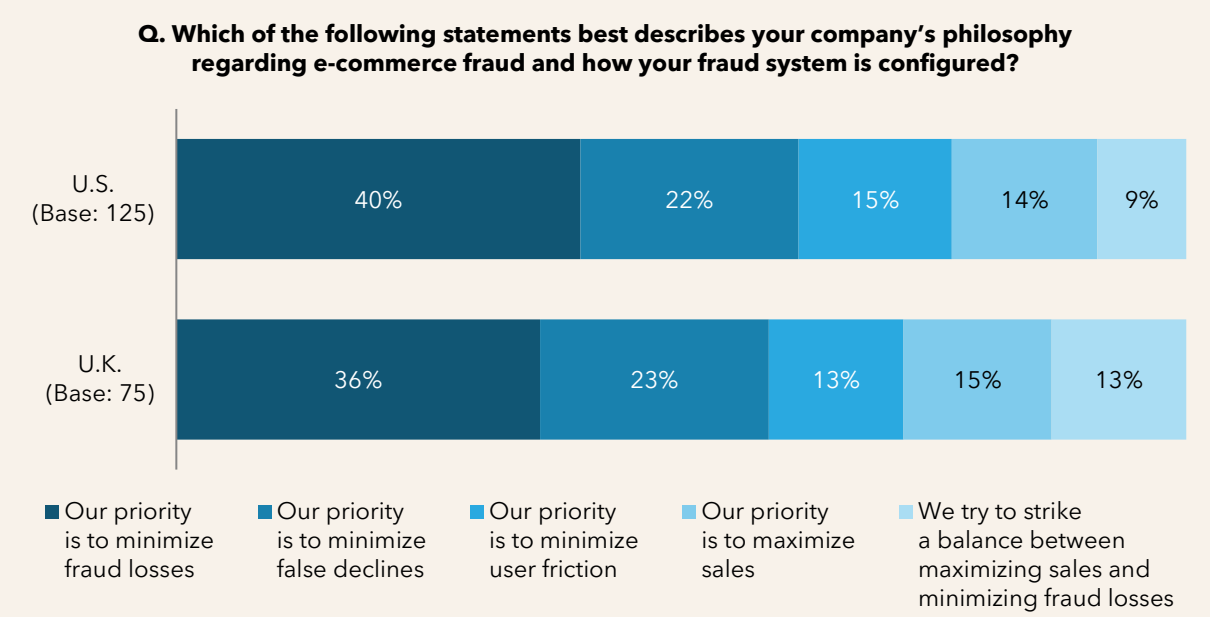
Several factors may be attributed to this improvement, such as the higher adoption of ML models, increases in first-party fraud, which ML models detect less frequently due to lack of confirmed fraud tagging, and changes in fraud attack patterns from payment fraud via stolen cards to post-transaction fraud such as returns, refunds, promotion abuses.

The State of E-Commerce Fraud Control Frameworks

While the rise in e-commerce has brought opportunities to both consumers and merchants, it has also facilitated an uptick in fraud. In response, merchants are outsourcing fraud management to third parties, integrating new tools into their fraud detection suites, shifting away from manual reviews, and adopting more ML models. Alongside the desire for increased fraud mitigation, merchants want to prevent revenue loss stemming from false declines and cart abandonment.

Lowering costs and growing sales are neck and neck when it comes to prioritizing how best to configure a merchant's fraud control framework. Minimizing fraud losses (i.e., lowering costs) is still a top priority for 40% of U.S. and 36% of U.K. respondents. Growing sales is a close second based on prioritization of minimizing false declines and maximizing sales, with 36% of U.S. and 38% of U.K. merchants rating this high (Figure 15).

Figure 15: Approaches to E-Commerce Fraud and Configuration of Fraud System



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

This is not surprising given merchants' increased willingness to invest in fraud prevention, whether that is adopting new technologies as part of an in-house fraud suite or outsourcing fraud management to a third party. In the Datos Insights' 2022 survey, 25%

of U.S. merchants reported they try to strike a balance between maximizing sales and minimizing fraud losses compared to just 9% in 2023. This decreased prioritization in striking a balance is roughly offset by the increase in minimizing fraud losses from 2022 (27%) to 2023 (40%).

Fraud Control Management

As the fraud and regulatory landscapes shift, e-commerce merchants are refining their approaches to fraud loss prevention. There has been a major shift in merchants' approach to fraud loss management, as a realization that fraud is too complex and evolves too quickly for them to tackle it proficiently.

Managing advanced fraud detection operations in-house requires significant investments in data science expertise, ML capabilities, and robust technology infrastructure. Outsourcing allows merchants to achieve greater operational efficiency and focus on their core business. In 2023, 77% of U.K. merchants and 73% of U.S. merchants outsource fraud management to a third party (Figure 16). In comparison, a significantly lower 56% of U.S. merchants outsourced fraud management to a third party in 2022.[3]

Figure 16: Management of Fraud Loss Prevention

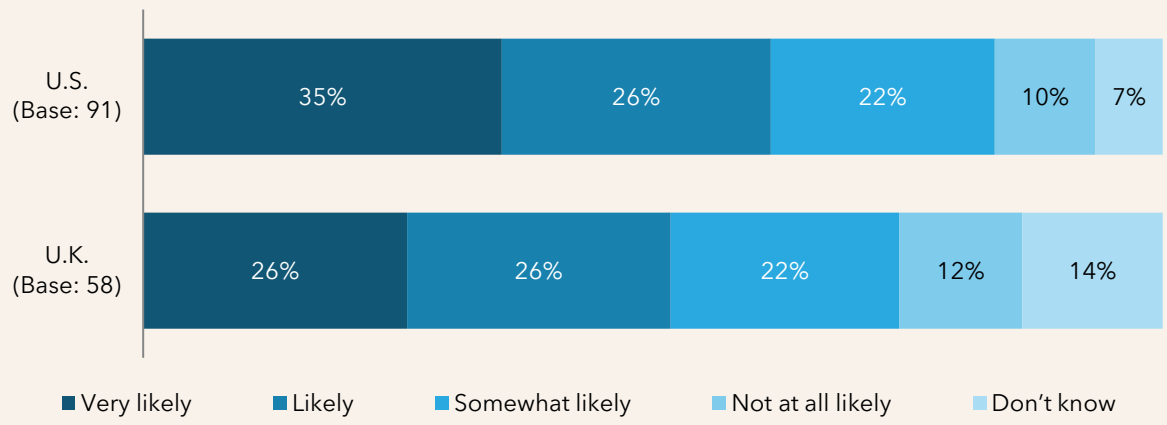
Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

[3] See Datos Insights' report The E-Commerce Fraud Enigma: The Quest to Maximize Revenue While Minimizing Fraud, July 2022.

When outsourcing fraud management, a merchant has the option to retain the financial liability for fraud or have a third-party firm assume it. Interestingly, all of the merchants in the 2023 survey retained fraud liability; none of them transferred the liability to a third party. These merchants value the expertise the third-party firms offer, and retaining ownership of the fraud liability provides an easier first step toward outsourcing.

Yet, as merchants seem to be pleased with the performance of the third-party firms, many intend to take the next step and move to a model whereby both fraud management and liability are outsourced to these firms. Sixty-one percent of U.S. merchants and 52% of U.K. merchants note that they are likely or very likely to adopt such an arrangement (Figure 17).

Figure 17: Likelihood of Company Switching to Third Party That Assumes Financial Liability for Fraud



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

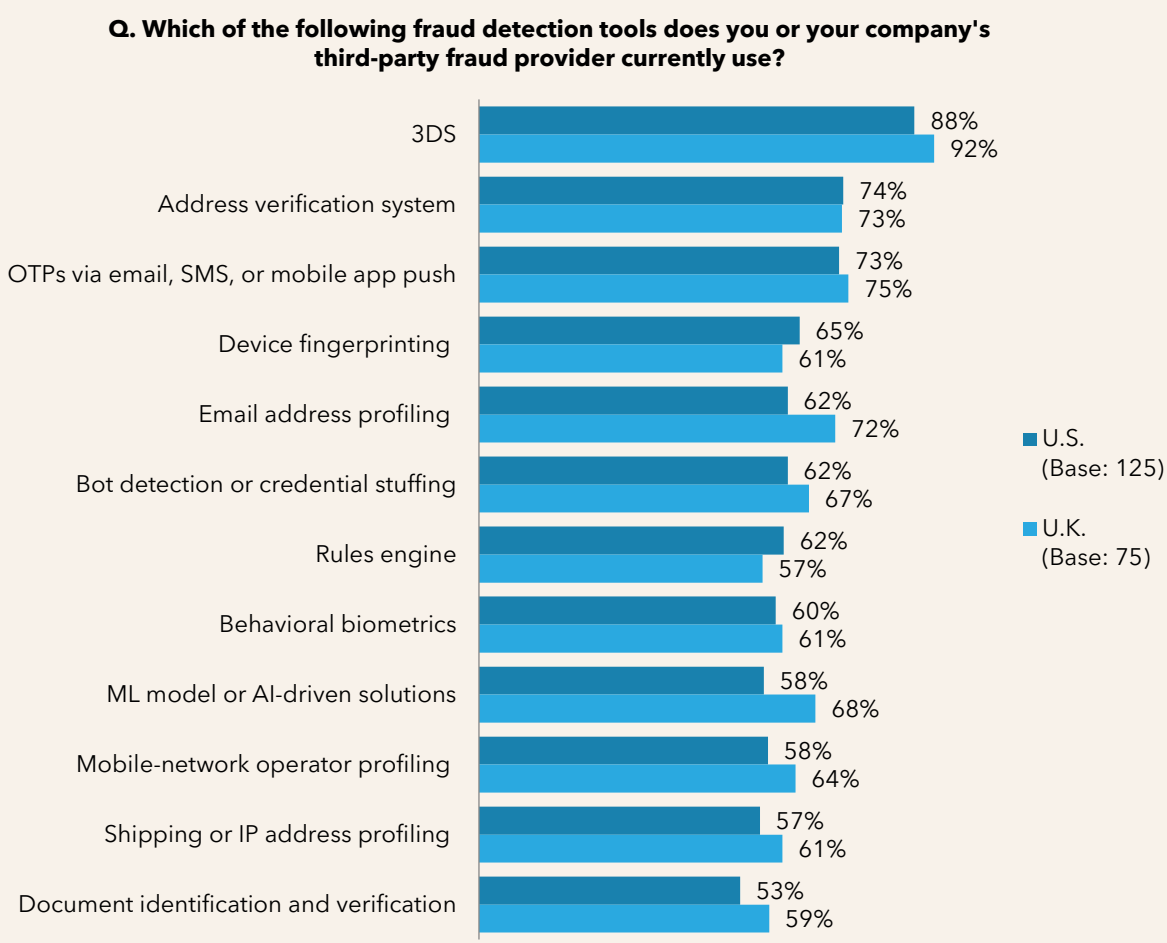
Fraud Control Technology

In combating fraud, it is clear that no single solution is sufficient. Rather, it is a suite of solutions. Relying on just a single fraud prevention tool leaves e-commerce merchants vulnerable to emerging fraud tactics that can bypass the solution.

A multilayered approach employing a comprehensive suite of complementary fraud solutions provides a much stronger defense. When asked which fraud detection tools they or their third-party fraud providers leverage, merchants cited 3DS, at 92% for the U.K. and

88% for the U.S. Following 3DS, address verification systems and one-time passcodes (OTP) were most commonly used (Figure 18). Continued usage of OTP is interesting, given that it is a common target for fraudsters, who are increasingly using social engineering to gather OTP information.

Figure 18: Common Fraud Detection Tools Deployed by Merchants

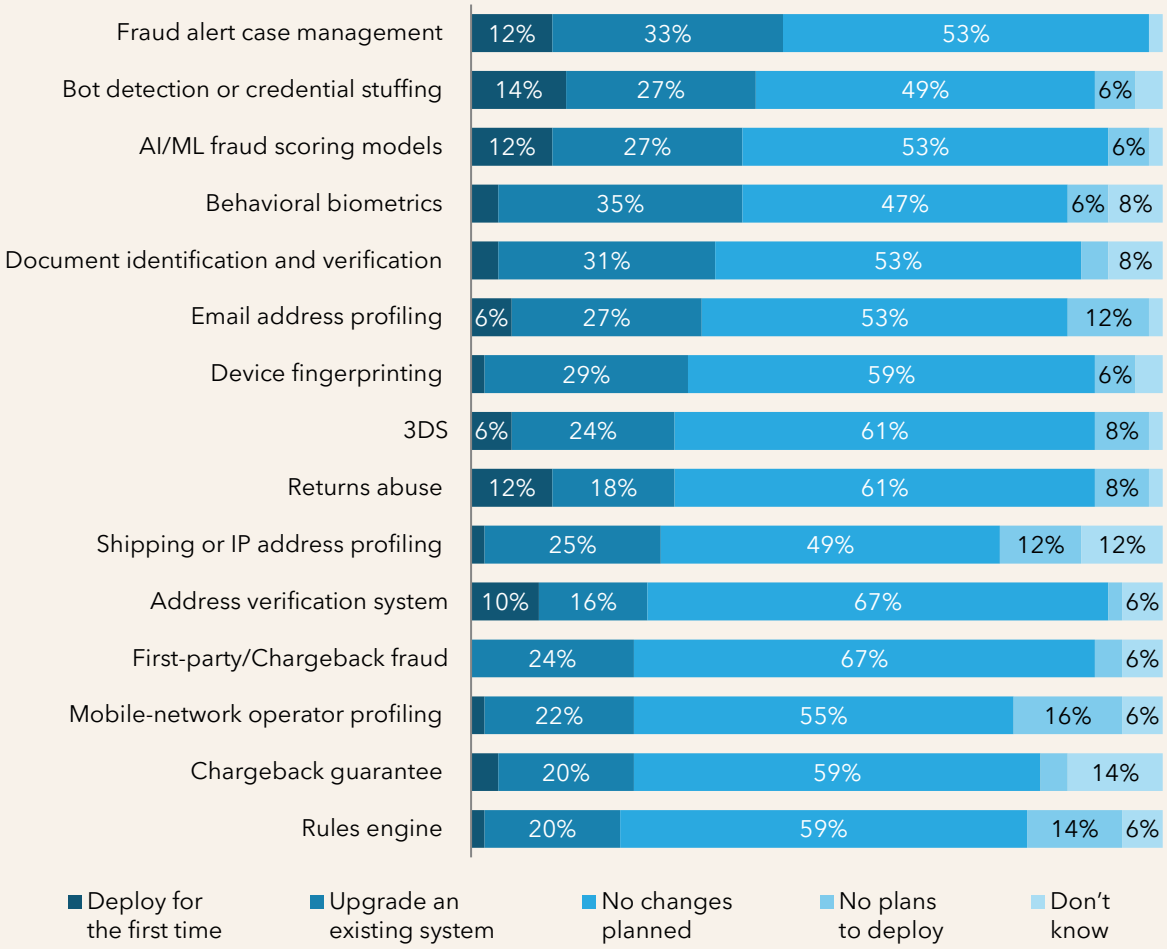


Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

With the growing number of fraud attempts, merchants need a way to manage them from creation to resolution. A case management system that can support multiple payment types pays dividends by consolidating fraud alerts and their related information in one spot. This facilitates the dissemination of data within an organization and can be used to track attacks upon a customer across multiple payment types. Merchants are signaling a clear interest in enhancing their in-house fraud systems within the next one to two years. Fraud alert case management systems top the list as the most likely to be deployed for the first time or an existing system that will be upgraded (Figure 19).

Figure 19: Planned Changes to In-House Fraud System in the Next One to Two Years

Q. Which of the following fraud detection tools does your or your company's third-party fraud provider currently use?
(Base: 51 e-commerce merchants in the U.S. and U.K. that have the tools and staff to manage fraud in-house)



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

Bot detection is the second most likely system to be deployed or upgraded, and with good reason. With the rise in various forms of abuse, such as promotion and coupon abuse, along with the ongoing popularity of guest checkout in which a user does not need to create an online account, bots can wreak havoc on a merchant. The proliferation of inexpensive bot tools on the dark web simplifies this form of attack by fraudsters.

First-time deployments and upgrades of AI/ML fraud scoring as the third most likely enhancement is positive news. Traditional fraud detection systems relying on static rules are proving inadequate against the rising volume and sophistication of online fraud attacks. A fraud analyst writing static rules based on commonalities across a set of

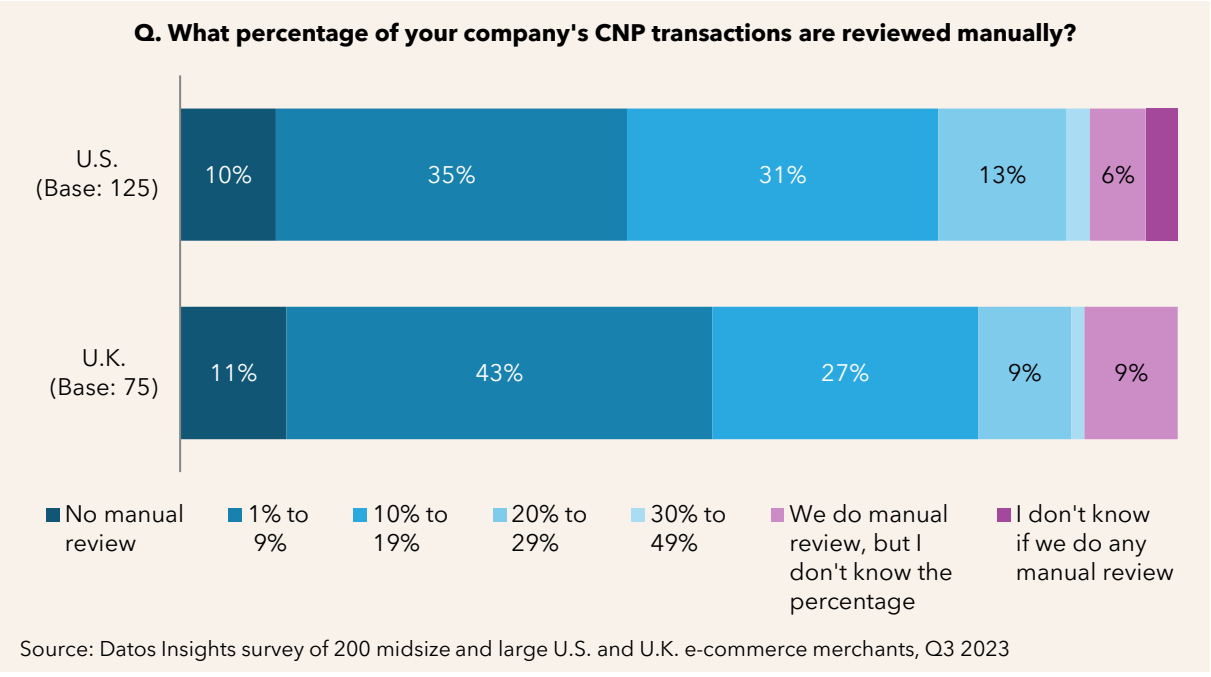
confirmed fraud transactions cannot keep pace with rapidly evolving fraud patterns and tends to generate high false positive rates.

In contrast, AI/ML models can be trained on large amounts of data to identify subtle transaction anomalies that humans can rarely discern manually. They are much better at differentiating legitimate from fraudulent transactions. By continually retraining on new data, models can stay ahead of fraudsters' latest methods. This precision allows merchants to minimize costly fraud losses and customer insults from false declines.

Manual Operations

In years past, merchants were overly reliant on manual reviews, which led to operational inefficiencies in terms of wasted time and resources. Too many transactions were sent for manual review, only for most of them to be approved anyway. Today, merchants send fewer transactions for manual review, with 35% of U.S. merchants and 43% of U.K. merchants reporting they manually review 1% to 9% of transactions. Still, a significant number of merchants (31% of U.S. merchants and 27% of U.K. merchants) note that they manually review 10% to 19% of transactions (Figure 20).

Figure 20: Percentage of CNP Transactions Reviewed Manually

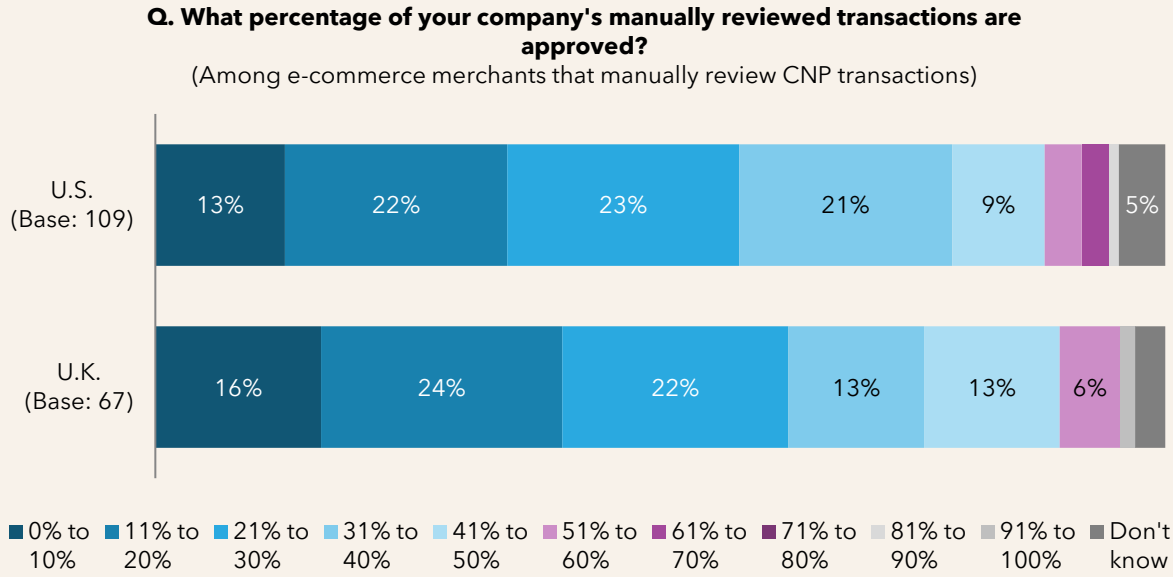


Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

Since merchants' fraud controls are now more selective regarding which transactions are sent for manual review, approval rates are much lower now, too. This is positive news,

signaling that systems have finally been tuned to send only medium- to high-risk transactions for review, and manual review agents are finding a smaller subset of good transactions that should be approved (Figure 21).

Figure 21: Manually Reviewed Transaction Approval Rate



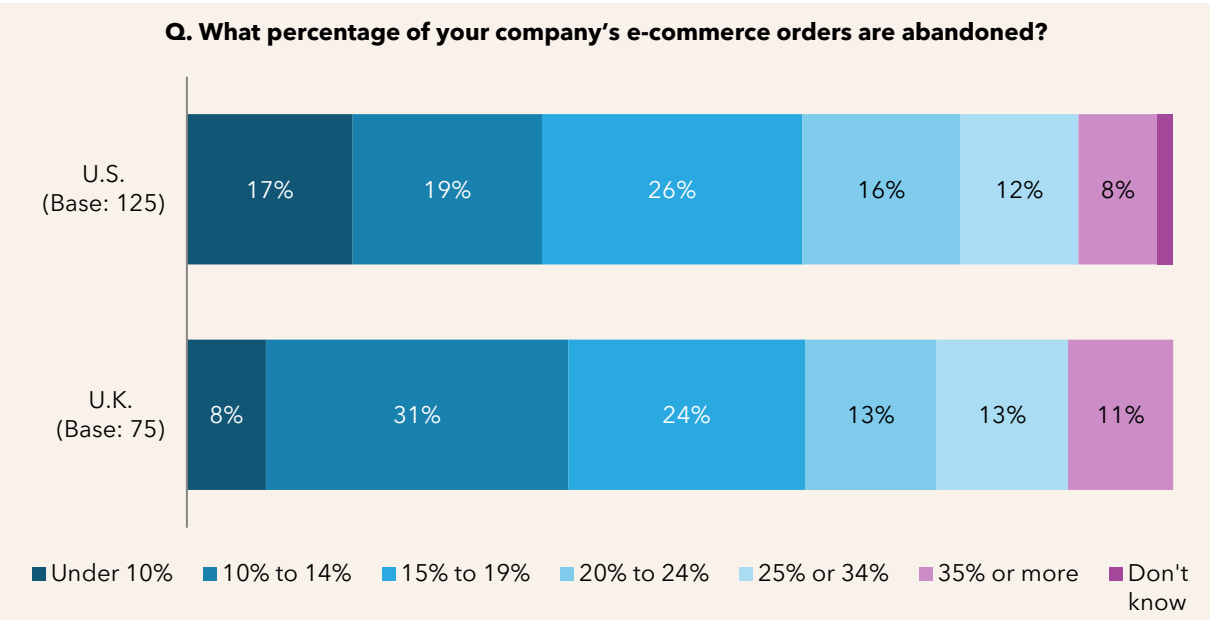
Source: Datos Insights survey of 200 mid-size and large U.S. and U.K. e-commerce merchants, Q3 2023

Cart Abandonment

E-commerce merchants contend with high rates of cart abandonment. This occurs when a customer adds items to their online shopping cart and then leaves the website before completing the transaction. There are myriad reasons for cart abandonment. One major reason for cart abandonment is a reaction to unexpected costs like high shipping fees or taxes being added at the final stage. Complex or lengthy checkout processes that require account creation can lead customers to abandon their carts out of frustration.

Thirty-one percent of U.K. merchants report a cart abandonment rate of 10% to 14%, and 24% of U.K. merchants report a rate of 15% to 19%. The situation in the U.S. is similar; 19% of merchants report rates of 10% to 14%, and 26% of merchants report rates of 15% to 19% (Figure 22).

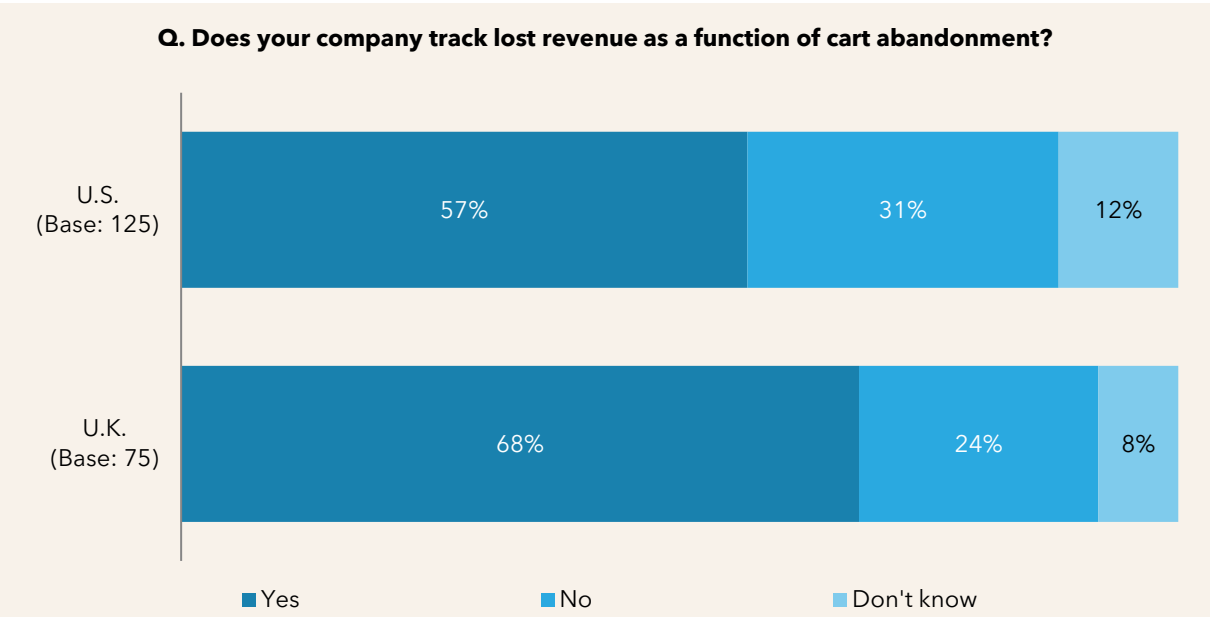
Figure 22: Percentage of E-Commerce Orders That Are Abandoned



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

Sixty-eight percent of U.K. merchants and 57% of U.S. merchants track lost revenue as a function of cart abandonment (Figure 23).

Figure 23: Percentage of Companies That Track Lost Revenue as a Function of Cart Abandonment



Source: Datos Insights survey of 200 midsize and large U.S. and U.K. e-commerce merchants, Q3 2023

Interestingly, more merchants track lost revenue associated with false declines than they do lost revenue associated with cart abandonment. Tracking lost revenue from cart abandonment is vital for e-commerce merchants because it highlights lost sales that directly impact topline performance. By measuring and analyzing cart abandonment rates and revenue amounts, merchants can identify potential areas of friction.

Conclusion

E-commerce merchants navigate a challenging fraud landscape and have made great strides in fine-tuning their fraud control frameworks. Unfortunately, when it comes to fraud, no one can rest on their laurels; merchants must continue to tweak and enhance their suite of tools.

Key recommendations for merchants and vendors include the following:

- **Consider outsourcing your fraud operations:** Managing fraud prevention in-house can be resource-intensive and challenging, especially for smaller businesses. By partnering with a reputable fraud prevention service provider, e-commerce merchants can leverage their expertise and cutting-edge technologies to combat fraud more effectively. Outsourcing fraud management is also valuable to merchants in that it frees up internal resources to focus on core business operations.
- **Determine whether a shift in liability makes sense:** For e-commerce merchants, retaining ownership of one's fraud liability can provide an easier first step toward outsourcing fraud management to a third party. Should merchants be pleased with the performance of these third parties, they can consider whether it makes sense to transfer fraud liability.
- **Leverage a suite of tools in tackling fraud:** There is no silver bullet when it comes to tackling e-commerce fraud, and a single fraud prevention method may not be sufficient to detect and prevent all types of fraudulent activities. By taking a multi-pronged approach to fraud prevention, e-commerce merchants and vendors are better able to shore up their defenses.
- **Look to adopt AI/ML models:** Static rules are no longer suited to today's fraud landscape. E-commerce merchants and vendors must leverage AI/ML models, which can ingest large troves of data to produce more accurate results and tamp down on erroneous fraud declines of good transactions.
- **Measure false declines:** False declines can lead to lost revenue and customer dissatisfaction; e-commerce merchants and vendors should analyze the reasons behind false declines and adjust their fraud prevention rules accordingly. Strike a balance between stringent security measures and a smooth customer experience to maximize conversions while minimizing fraud risks.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

David Mattei

dmattei@datos-insights.com

Contributing author:

Gabrielle Inhofe

ginhofe@datos-insights.com