August 2024

The Future of E-Commerce: Innovations to Protect and Enrich the Online Channel

David Mattei

Prepared for:

VISA

Table of Contents

List of Figures

Executive Summary

The e-commerce industry has been grappling with the contrast between the secure and user-friendly in-store purchasing experience and the fraud-prone, less streamlined online environment. Efforts to bring safety and convenience to e-commerce transactions and close the gap with in-store purchases are beginning to bear fruit. This white paper delves into the factors contributing to this disparity and explores the innovative solutions that are bridging the gap.

- **Chip cards and data breaches significantly contributed to e-commerce fraud rates:** The confluence of industry events in the 2010s, such as the adoption of EMV chip cards and the exposure of compromised online credentials, has led to a surge in card-not-present (CNP) fraud losses for e-commerce merchants.
- **Early efforts to contain CNP fraud losses exacerbated the issue:** Merchants' aggressive fraud controls resulted in lower conversion rates, higher false positive rates, and poor online user experiences. Issuers' concerns with CNP fraud rates and higher dispute volume also led to aggressive fraud controls that resulted in lower CNP authorization approval rates.
- **A variety of fraud prevention innovations coupled with collaboration are leading to a much-improved online buying ecosystem:** The industry is poised to narrow the performance gap between card-present (CP) and CNP transactions by leveraging better data-sharing initiatives, improved user authentication solutions, and advanced risk mitigation solutions.
- **Merchants and financial institutions (FIs) are beginning to reap the benefits from implementing these capabilities:** By adopting these innovations, merchants and FIs are starting to realize higher revenue, lower fraud costs, and provide a better user experience to consumers.

E-commerce can effectively combat fraud while simultaneously cultivating trust and confidence among consumers by embracing cutting-edge technological solutions and fostering close collaboration among industry players. The successful implementation and continuous refinement of these strategies will be instrumental in driving the sustained growth and prosperity of the e-commerce sector in the coming years, ultimately benefiting merchants, FIs, and consumers alike.

Introduction

Consumers have been transacting in stores for decades. Merchants and consumers have enjoyed a rather safe and streamlined experience since the introduction of chip cards. Fraud rates are relatively low, authorization approval rates average over 95%, and especially with contactless chip payments, the payment process is simple and fast. However, e-commerce merchants and consumers look upon in-store purchasing with envy. Fraud rates on e-commerce transactions are much higher, authorization approval rates have historically been in the mid-80% range, and completing the online purchase can be interrupted by requests for users to authenticate themselves.

Why is there such a contrast between online and in-store purchases? Moreover, given the pace at which technology is advancing, how can the industry leverage it to address this disparity? This paper explores why these differences exist and solutions that have recently come to market that promise to close this gap allowing merchants and FIs to increase revenue and lower fraud costs while also delivering an improved user experience to delight consumers.

Methodology

This white paper is based on multiple global studies Datos Insights has conducted with merchants, FIs, and consumers, as well as extensive briefings provided by many solution providers.

The E-Commerce Dilemma

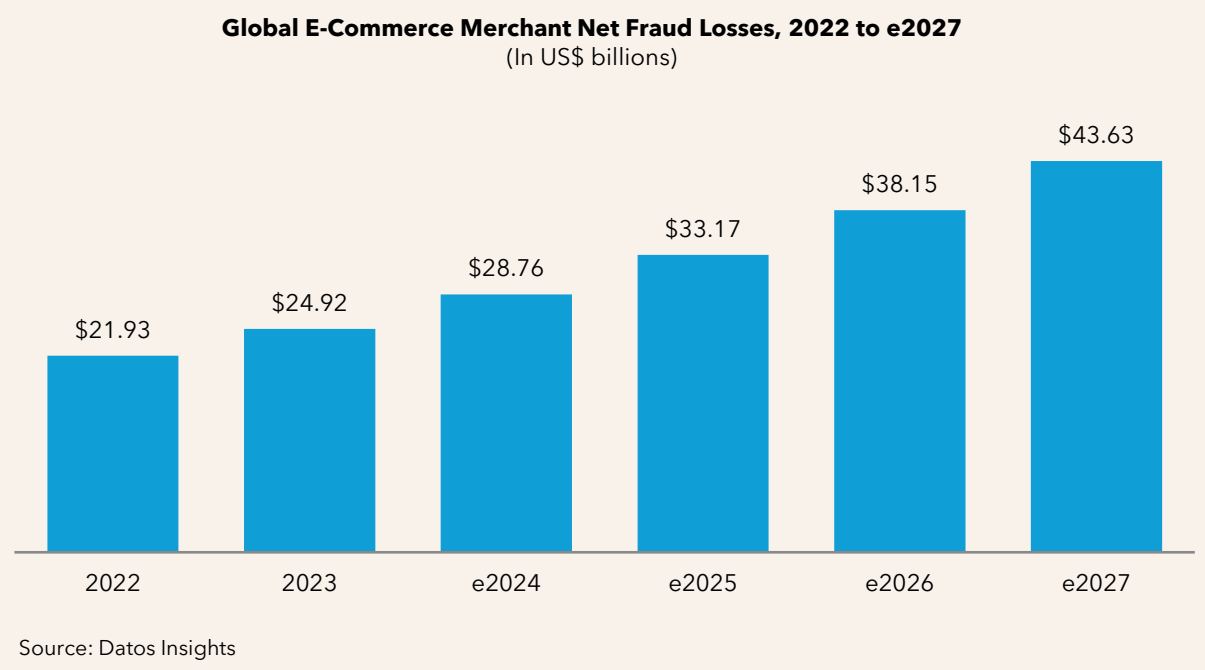
In the 2010s, an interesting confluence of industry events occurred in rapid succession, resulting in the current state of card fraud. Not too long ago, CP fraud losses for in-store transactions exceeded CNP fraud losses for e-commerce transactions. Countries around the world migrated to EMV chips on credit and debit cards, and fraudsters found it increasingly difficult to commit CP fraud. As chip cards became mainstream, e-commerce sales were accelerating—a significant shift in consumer purchase volume.

Chip cards are highly effective at reducing fraud on CP transactions, yet they offer no protection for CNP transactions. Thwarted by the protections provided by chip cards, fraudsters followed the money, migrating to the next weakest link: e-commerce sales. This ushered in an era in which data breaches exposed billions of compromised online credentials, payment details, and personally identifiable information (PII). This data, coupled with increasing e-commerce sales and new technologies, allowed fraudsters to commit CNP fraud at scale.

Merchants were ill-prepared for the speed with which these changes occurred. FIs are typically liable for CP fraud losses, while merchants are liable for CNP fraud losses. In the prior era, the majority of card fraud occurred on CP transactions; merchants had little need to invest in robust fraud solutions. This dynamic changed rapidly and dramatically as CNP fraud losses soared, forcing merchants to adopt fraud controls quickly to stem the financial bleeding.

Even as merchants invest in new fraud controls, fraudsters continue to attack e-commerce with relentless pursuit, resulting in mounting losses. Datos Insights estimates 2024 global e-commerce fraud losses to be US$28.8 billion, growing to US$43.6 billion by 2027 (Figure 1).

Figure 1: Global E-Commerce Merchant Net Fraud Losses, 2022 to e2027



Source: Datos Insights

Early merchant and FI fraud control frameworks introduced a three-prong problem:

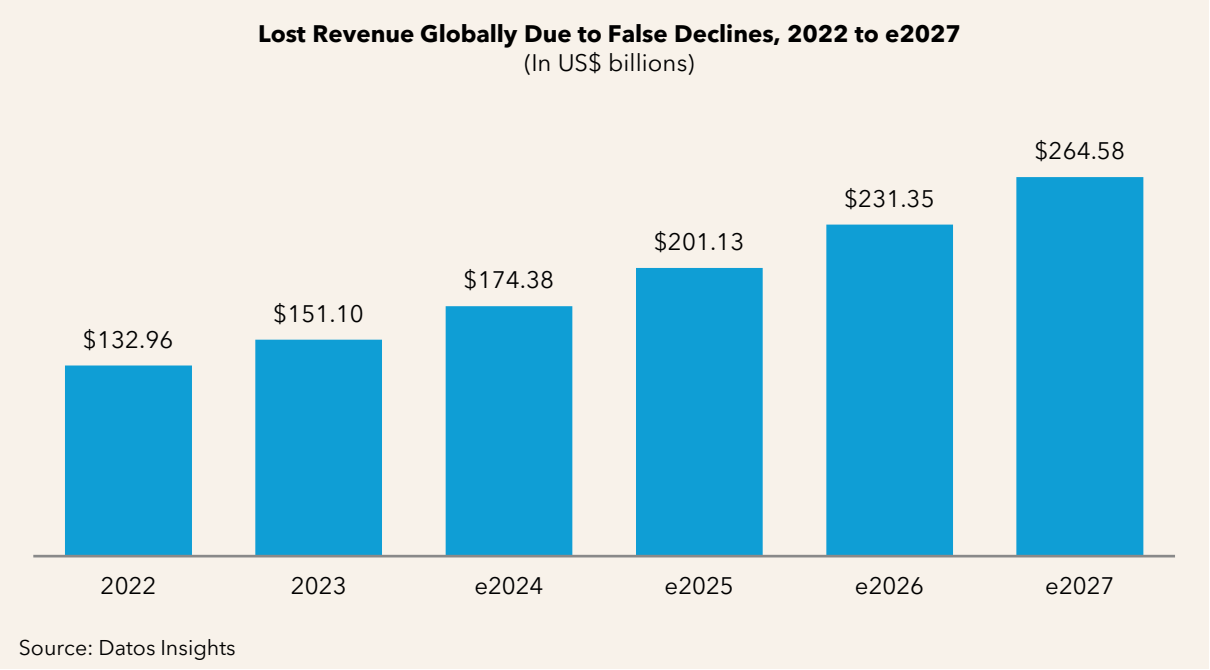
- **Low CNP conversion and authorization approval rates:** In an effort to lower CNP fraud losses, some merchants deployed overly aggressive fraud strategies, resulting in low conversion rates. FIs were also concerned with increases in the number of fraudulent CNP transactions and the resulting rise in dispute volume. FIs likewise implemented aggressive fraud strategies, resulting in CNP authorization approval rates in the low-to-mid-80% range. In comparison, CP authorization rates increased to the high 90% range due to the fraud controls offered by chip cards. Even in Q4 2023, Visa observed CNP approval rates 6% lower than CP approval rates.[1]

- **High false positive rates:** Aggressive merchant fraud controls had an unintended consequence of denying good customer transactions. Merchant marketing dollars spent to attract new customers were wasted as fraud departments blocked their transactions. Fraud departments became known euphemistically as the "sales prevention" department due to poorly tuned strategies. Denying a good transaction also results in lost revenue opportunities. Datos Insights estimates that 1.51% of global

[1] Source: Visa Risk Cheat Sheet. Fraud data from Q3 2023. Approval rate from Q4 2023.

e-commerce sales are lost to false declines, costing merchants US$174 billion in 2024, growing to US$264 billion by 2027 (Figure 2).

Figure 2: Global Lost Merchant Revenue Due to False Declines, 2022 to e2027



Source: Datos Insights

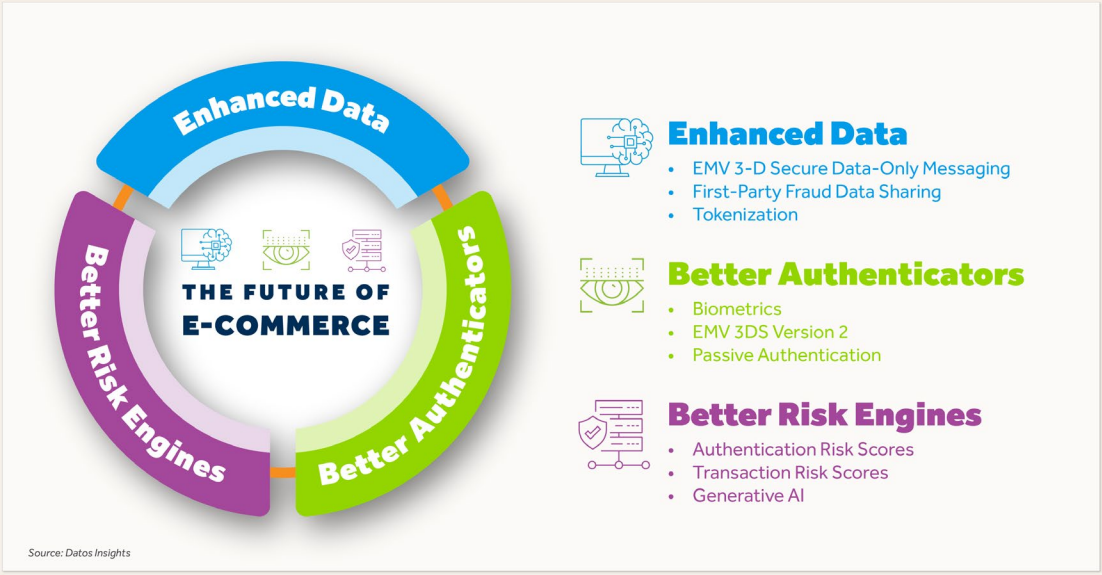
- **Poor online user experiences:** Fraudsters love the online world because it is easy to remain anonymous and to impersonate someone else. To understand who you are doing business with, merchants deployed solutions to authenticate a user and stop fraudsters. Some of this was driven by government and industry efforts to lower CNP fraud losses in certain parts of the world, such as the EU's second Payment Services Directive for strong customer authentication, Japan's Online Gaming Association, Singapore's Monetary Authority, and other efforts in countries such as Australia, New Zealand, and South Africa. Consumers found certain authentication processes cumbersome to complete or annoying at best (e.g., 3-D Secure V1, which required user enrollment, a password, and the early use of one-time passcodes), leading to abandoning transactions or shopping elsewhere.

Fortunately, the industry has come a long way over the past decade. Merchants have improved the tuning of their fraud controls, and new solutions have emerged from the vendor community. A new day is dawning in the e-commerce fraud fight.

A View Into E-Commerce's Future

Mirroring the speed of industry changes in the 2010s, fraud and authentication solutions have rapidly evolved in the 2020s with innovative solutions and technologies coming to market. The e-commerce industry is on the threshold of narrowing the gap between performance statistics of CP and CNP transactions, much to the delight of merchants, FIs, and consumers. Getting there involves improving three key elements: data, authentication, and risk engines (Figure 3).

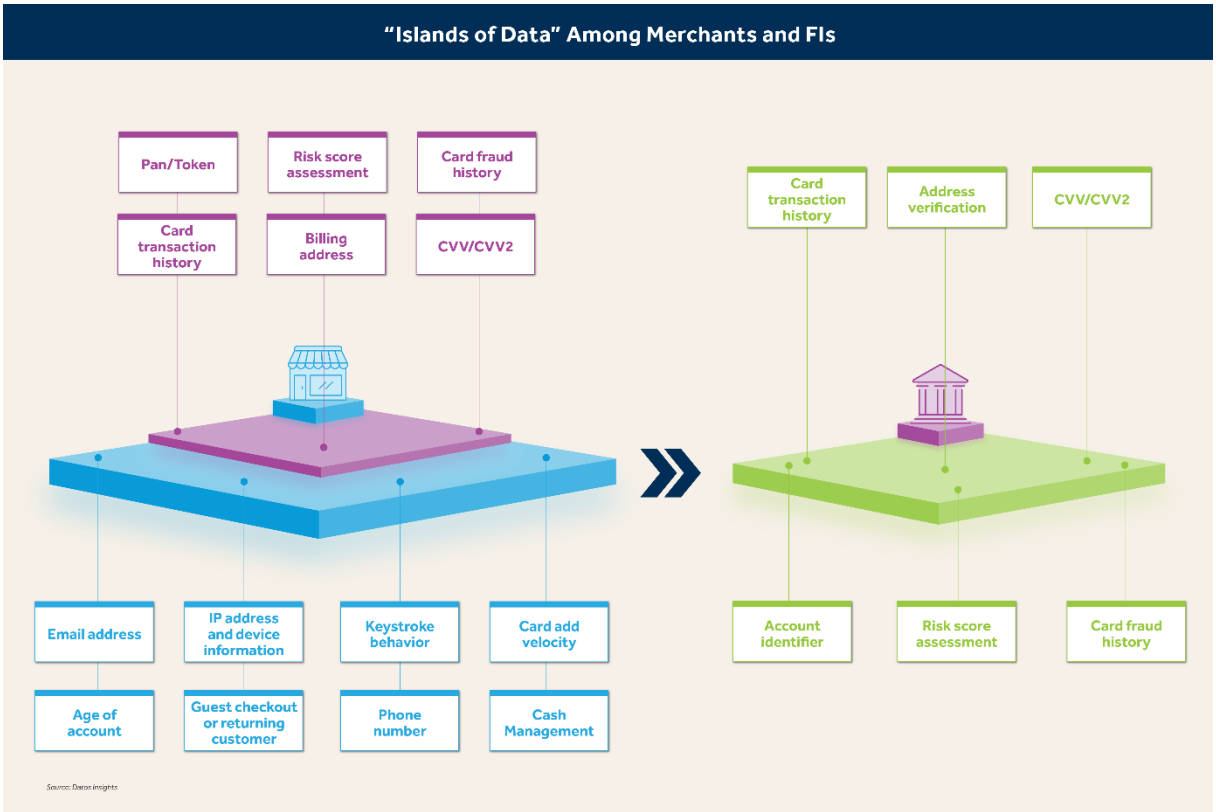
Figure 3: Three Key Elements to Secure the Future of E-commerce



Enhanced Data

The adage "data is king" has never been truer than today. In fact, the e-commerce industry has the data to stop most, if not all, fraud. Unfortunately, data is scattered across industry participants along the payment flow, including merchants, processors, card networks, and FIs. Fraudsters count on and thrive on these "islands of data" across the ecosystem, which limit fraud systems from seeing the bigger picture (Figure 4).

Figure 4: Siloed Customer and Transaction Data Across the Ecosystem



The lack of data sharing between merchants and FIs is a significant cause of the false decline problem. Even if merchants prevent global CNP fraud, which Datos Insights estimates to be US$36 billion in 2024, the industry still must contend with the Datos Insights estimated US$174.4 billion in global lost sales due to false declines—a 4.8 times larger issue.

Different ways to close the data gap to mitigate fraud are described below.

EMV 3-D Secure Data-Only Messaging

3-D Secure (3DS) has been around for over 20 years and is used to authenticate a consumer during an e-commerce transaction. What is less known is that EMVCo, the entity that controls the EMV 3DS technical specification, introduced a data-only capability in EMV 3DS that allows data sharing between merchants and FIs. Since it does not involve a user authentication component, merchants can share data such as merchant information, user information, payment credentials, and the user's browser and device details, which FIs can leverage within their fraud systems to make more informed decisions.

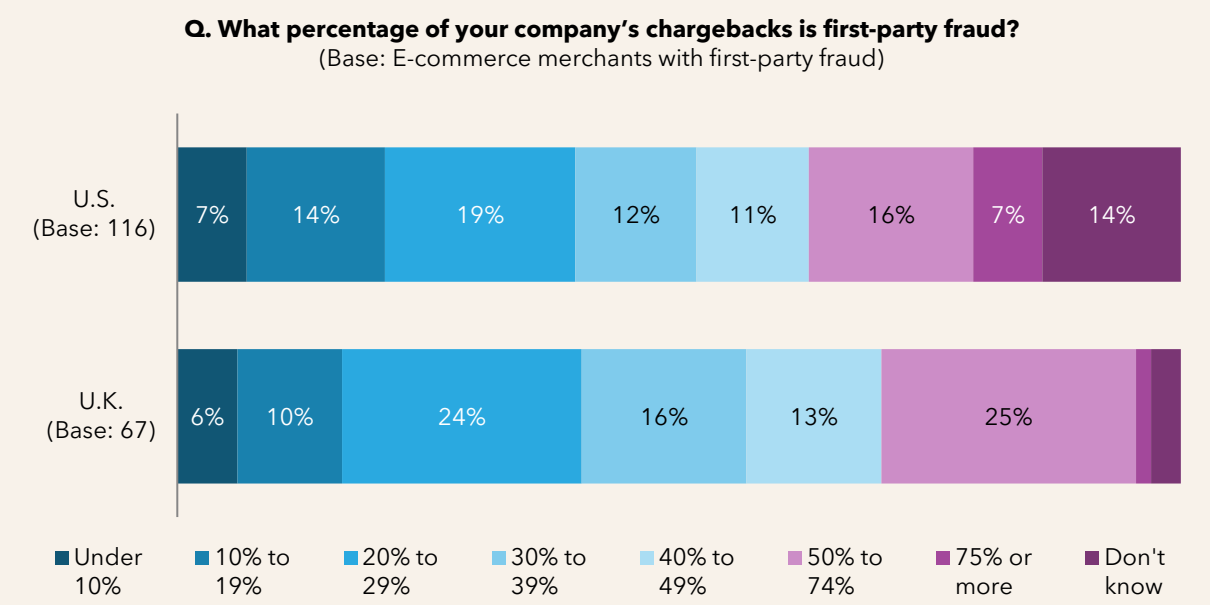
Visa and Adyen conducted a test of 3DS data-only sharing in Brazil and observed a 7% increase in CNP authorization approval rate.[2] This improvement occurred without invoking any form of consumer authentication

First-Party Fraud Data Sharing

Much has been written and done to combat criminals who steal payment and online account credentials for financial gain (i.e., third-party fraudsters). However, another troubling form of fraud is when the rightful owners of the payment and online account credentials make a purchase but then dispute it, claiming they didn't make it. This form of fraud has many names, such as first-party fraud, friendly fraud, and first-party misuse. It is a significant issue for merchants and FIs alike.

In a study of 200 e-commerce merchants in the U.K. and U.S., 57% of U.K. merchants and 47% of U.S. merchants report that over 30% of their chargebacks are related to first-party fraud (Figure 5).

Figure 5: Percentage of Chargebacks Related to First-Party Fraud



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

The card networks are well aware of this issue and have launched data-sharing initiatives to combat this. When merchants suspect that a dispute or chargeback is first-party fraud, they can provide additional details to FIs, such as the user's IP address, device ID, and email

[2] Adyen Visa Data Only results in Brazil from July to November 2023 for Visa transactions.

address. With this additional data, FIs can use this to refute the dispute with their cardholders. If the cardholder happens to be a user of the FI's mobile banking app, the FI can further strengthen its claim of first-party abuse by comparing IP addresses and device IDs from the merchant with internal records of mobile banking usage.

Tokenization

Leveraging data among industry players can lead to better fraud performance, but protecting data is equally important. Protecting sensitive data in the payment ecosystem is needed to ensure the data cannot be intercepted and used for nefarious purposes. The introduction of tokenization and its many variations has done just this. It replaces the credit or debit card number, expiration dates, and security codes with a hashed equivalent that only the recipient of the data can detokenize. Tokenized data are useless to fraudsters; they cannot use it to make a payment. Since this was introduced over 10 years ago, nearly 30% of all VisaNet transactions processed by Visa are now tokenized.[3]

Use cases for tokenization have expanded from its original purpose of protecting payment credentials. In an era of heightened data privacy concerns and data breaches, tokenization can also be used for PII data such as numerical data (government identities, passports, mobile phone numbers) and alphanumeric data (email addresses, dates of birth).

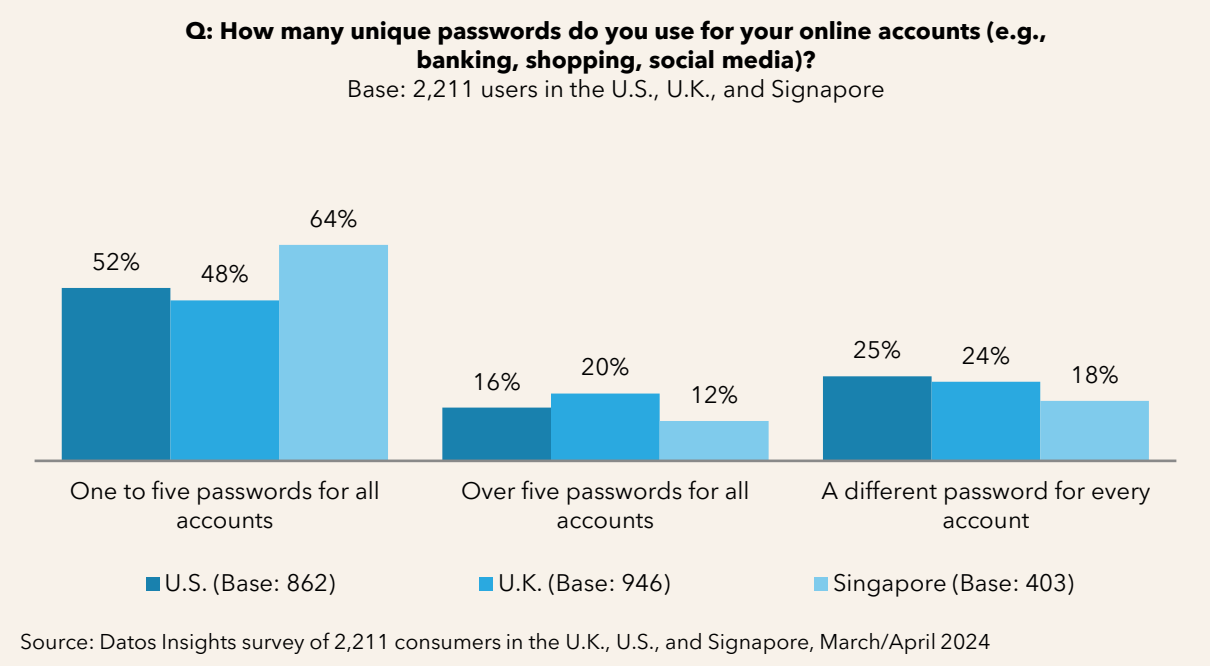
Better Authenticators

Verifying the identity of a person who is attempting to perform a transaction in a non-face-to-face channel (e-commerce, call centers, mobile/online banking) is becoming more critical for companies to protect themselves. Fraudsters can too easily impersonate a legitimate user, and they prefer remote channels since it is easier to remain anonymous.

Unfortunately, the weakest link in any authentication process is the consumer. All too often, they reuse the same password across multiple online sites, which can lead to account takeovers. In a recent study of consumers in Singapore, the U.S., and the U.K., Datos Insights found password reuse is a global issue, with 64% of consumers in Singapore using five or fewer passwords across all online accounts with 52% in the U.S. and 48% in the U.K. (Figure 6).

[3] VisaNet, April 2024. Global CNP and CP transactions for tokenized vs non-tokenized credentials. https://investor.visa.com/news/news-details/2024/Visa-Reinvents-the-Card-Unveils-New-Products-for-Digital-Age/default.aspx.

Figure 6: Prevalence of Password Reuse Across Online Accounts



Source: Datos Insights survey of 2,211 consumers in the U.K., U.S., and Signapore, March/April 2024

Even when multi-factor authentication is used, commonly via one-time passcodes (OTP) sent via email or SMS/text message, these OTPs are more susceptible to being intercepted or inadvertently divulged via social engineering. Several authentication solutions are growing in popularity, offering the possibility of eliminating passwords and OTPs.

Biometrics

Physical biometrics are quickly gaining traction among consumers as a way to authenticate themselves. Mobile devices ushered in a new era of biometrics in which consumers can unlock their devices with a face scan or fingerprint, replacing passwords and 4-digit or 6-digit PINs. As consumer adoption accelerated, mobile banking apps followed suit. In a Datos Insights 2024 survey of 2,211 consumers in Singapore, the U.K., and the U.S., biometric options were two of the top three preferred authentication methods, with fingerprint being second and facial being third, very close behind username/password being the most preferred.

The FIDO Alliance is an industry association focused on standards for online sign-ins using passkeys that are resistant to phishing attacks and are more secure than passwords and OTPs. It leverages public/private key cryptography in which the private key is in the user's possession and the public key with the online service (an e-commerce merchant, a financial services firm, payment network, other). When logging into an online site or completing a purchase, users verify themselves in a number of ways; physical biometrics

is one of those options. As unlocking a mobile device via a face or thumbprint scan becomes mainstream, using FIDO technology coupled with physical biometrics offers a familiar and easy-to-use method to replace passwords and OTPs.[4] In a production implementation, Visa observed a 51% reduction in fraud when out-of-band biometrics were used compared to SMS OTP for authentication.[5] With FIDO's phishing-resistant feature, account takeovers could be a thing of the past.

EMV 3DS Version 2

EMV 3DS is designed to mitigate fraud and increase approval rates on e-commerce transactions by risk assessing the transaction and if suspicious, authenticate the user. Many merchants have an opinion of 3DS from the 2000s and early 2010s when version 1 was most prevalent. However, EMVCo introduced a new version (EMV 3DS), which greatly improved the user experience, enhanced the data exchange, and broadened the number of authentication methods. Users can now be authenticated via OTP, physical biometrics, and other methods. For example, Best Buy Canada implemented EMV 3DS and, over two fiscal quarters, saw CNP fraud losses drop from 36 basis points to 14 basis points—a 61% reduction. EMV 3DS-protected CNP transactions had an 86% authorization approval rate compared to only 62% for non-EMV 3DS-protected CNP transactions.[6]

EMV 3DS also introduced enhanced data exchange and a new capability called risk-based authentication, in which the CNP transaction is risk-assessed, and a determination is made whether additional user authentication is needed. If the risk level is low enough, no additional authentication is performed, providing users with a frictionless experience.

Passive Authentication

Authentication does not always require a user to perform an action. A newer breed of solutions can silently authenticate a user in the background. These solutions, known as passive authenticators, include technologies such as device fingerprinting, behavioral biometrics, location behavior, email address profiling, mobile network operator profiling, and IP address profiling. These solutions build a digital fingerprint of an individual. Any digital transaction can capture these data elements and compare the current online session with prior sessions, looking for anomalies. If all the data elements are consistent

---

4 "Visa Reinvents the Card, Unveils New Products for Digital Age," Visa Inc., May 15, 2024, accessed August 15, 2024, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20686.html.

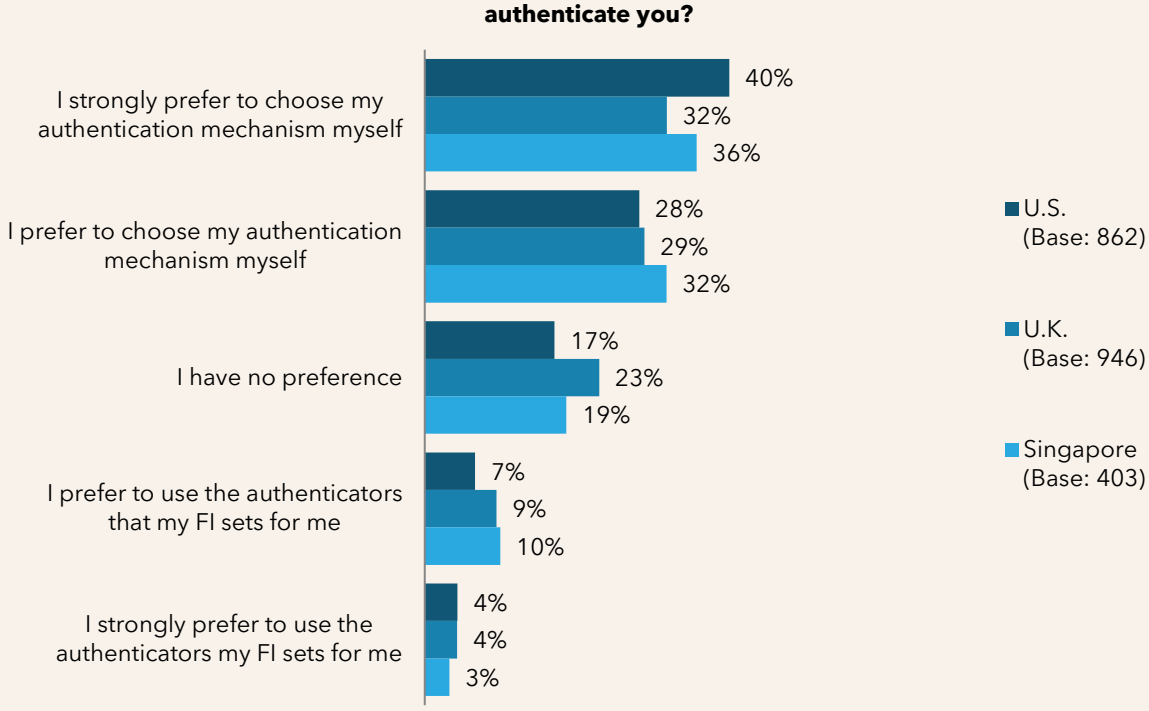
5 VisaNet data globally from July to December 2023

6 "Visa Secure with EMV 3-D Secure," Visa Inc., accessed August 15, 2024, https://globalclient.visa.com/bestbuycanada_ca_en.

across online sessions, there is no need to invoke an active authentication such as OTPs or physical biometrics, resulting in an improved user experience.

There is no single authenticator that is best for all users all the time. Companies should support multiple authenticators, as different user demographics have different capabilities and preferences. In a recent Datos Insights study of consumers in Singapore, the U.K., and the U.S., nearly two thirds of users prefer to choose the method by which they are authenticated vs. not having a choice (Figure 7).

Figure 7: Users Preference to Choose Their Authentication Method



Source: Datos Insights survey of 2,211 consumers in the U.K., U.S., and Signapore, March/April 2024

Better Risk Engines

Early risk systems were based on static "if/then" conditional rules. However, that approach to fighting fraud has problems. The pace, scale, and complexity with which fraudsters operate make it difficult for fraud analysts to keep up. Moreover, static rules tend to be very broad in scope, leading to high false positive rates. Artificial intelligence (AI) and machine learning (ML) are the core of most modern fraud systems since they can learn and adapt as fraud patterns evolve. Merchants and FIs can leverage AI/ML in several ways.

Authentication Risk Scores

There is a wealth of information that can be collected and used to assess risk beginning at the point when a user lands on a website, browses online, logs in, and after logging in. Information such as email address, IP address, device details, website interactions, behavioral data, and others can be used to assess the risk of digital interactions. This data, combined with known good and known fraudulent behavior, can be used to train an ML model to assess a user's authentication risk. As new data is captured and new attack vectors emerge, specialized ML models can be created to detect more nuanced risks. Low authentication risk scores can allow users to proceed with their business, while high authentication risk scores can lead to further authentication processes.

Transaction Risk Scores

An early use of ML was to detect the likelihood of a transaction being fraudulent. Known fraudulent transactions were used to train these models, which could determine in real time whether to approve or decline an authorization request. While still very useful in generating a risk score for the transaction, transaction risk scores can be combined with authentication risk scores to improve fraud detection while also lowering false positives.

Generative AI (GenAI)

GenAI technology is still emerging, but it already offers a significant opportunity to empower fraud fighters to elevate their fraud detection capabilities. Rather than relying on a data scientist to guide the ML process, GenAI is well-equipped to discover the unique characteristics of fraudulent transactions automatically and can do so using a larger quantity of training data than ML. This improves fraud detection and does so more accurately, thereby reducing false positives.

GenAI can adapt and find new fraud patterns dynamically rather than requiring re-training of the ML model; this leads to continuous fraud detection, which is critical considering the scale and speed of fraudsters' attacks. The ease of using GenAI also allows a broader group of fraud fighters to use this technology rather than needing the specialized skills of data scientists. As GenAI evolves, fraud fighters need to be cognizant of the importance consumers will place on trust and transparency in its use.

E-commerce is a complex business in which merchants and FIs continue to strive for the ideal user experience of approving all good transactions with little to no user friction while also declining all fraudulent transactions. No single solution can achieve that goal. A holistic, layered approach is needed to address risks that are identified along the customer

journey to close the industry gap in authorization approval rates between CP and CNP transactions. Enhanced data coupled with better authenticators and risk engines provide a solid foundation to improve e-commerce among consumers, merchants, and FIs.

Conclusion

The e-commerce industry has had stiff headwinds in its fight against CNP fraud, leading to subpar authorization rates, high false positive rates, and unsatisfactory user experiences. However, the rapid development of fraud prevention and authentication solutions in the 2020s and closer collaboration efforts among industry participants have brought the industry to the cusp of closing the performance gap between CP and CNP transactions. The keys to success lie in the following:

- **Embrace data-sharing initiatives** to enhance fraud detection and prevention**.** Breaking down "islands of data" that exist among merchants, FIs, card brands, and others brings heightened visibility into authentication and fraud decisioning.
- **Implement improved authentication solutions** to verify user identities while maintaining a seamless experience. Leverage passive authenticators as a first line of defense and step up to active authenticators as risk levels rise.
- **Continuously monitor and adapt** to emerging fraud trends and techniques to stay ahead of fraudsters. As the industry further tightens the screws on fraudsters limiting their ability to commit their crimes, fraudsters will constantly be looking for the next hole in its defenses.
- **Educate consumers** about best practices for online security and the importance of secure authentication methods. As the user is commonly the weakest link in payment fraud, the more informed they are about how fraud occurs they become frontline fraud fighters.

About Visa

Visa is a world leader in digital payments, facilitating transactions between consumers, merchants, financial institutions and government entities across more than 200 countries and territories. Our mission is to connect the world through the most innovative, convenient, reliable and secure payments network, enabling individuals, businesses and economies to thrive. We believe that economies that include everyone everywhere, uplift everyone everywhere and see access as foundational to the future of money movement.

As the payments ecosystem continues to evolve, Visa helps its clients stay ahead of challenges to drive growth and deliver secure, seamless payments to customers. Within Visa's value-added service offerings, Visa Protect is a suite of enterprise risk solutions and AI-powered real time decisioning that work across the entire transaction flow and across all payment networks. Visa Protect risk solutions help businesses prevent fraud and financial crimes, streamline operations, and build trust with their customers. Learn more at Visa.com/protect.

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