WHITE PAPER

OCTOBER 2023

Leveraging PSD2 for greater revenue and customer loyalty

How Mastercard Identity helps merchants convert more transactions and deliver a frictionless customer experience

Contents

PSD2: A promise of greater security...and where we are today

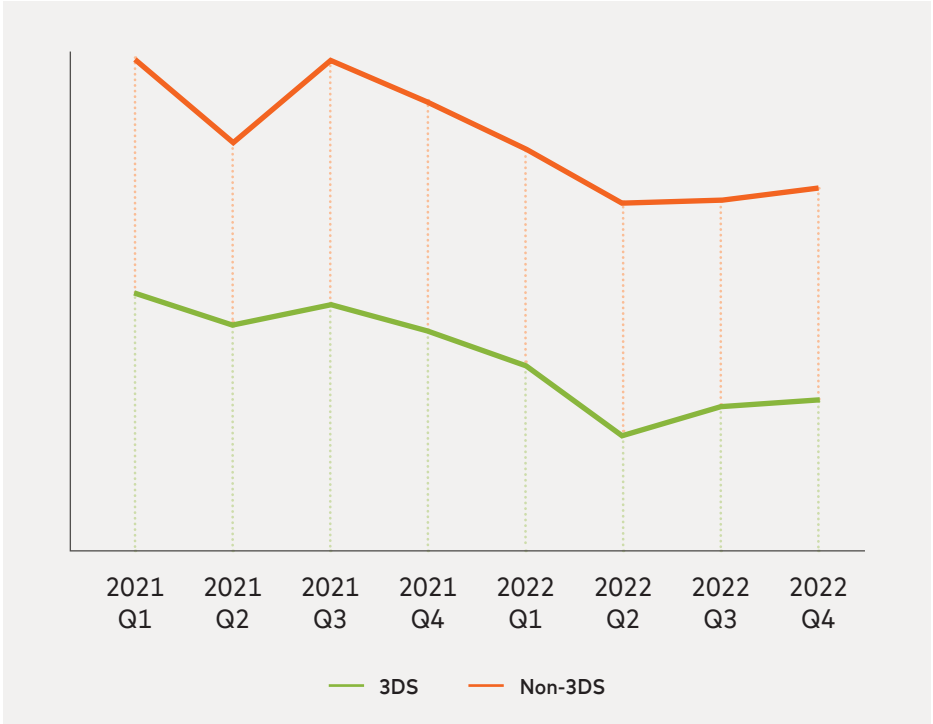
As digital transactions have grown by double digits across Europe in recent years, the need to protect consumers and merchants from rising fraud became a prime objective of the European Economic Area (EEA). With the implementation of the Payment Services Directive 2 (PSD2) in 2018, the path towards greater security and more protection for both consumers and merchants began. However, implementing these regulations has been challenging for all stakeholders in the payments industry. While PSD2 has significantly reduced fraud, many argue that it's coming at the great cost of adding complexity and friction for both consumers and merchants.

PSD2 is a major step forward in making e-commerce payments more secure for consumers and businesses, fostering innovation and establishing open, consistent standards across the European Economic Area and the United Kingdom (UK). By requiring merchants and issuers to validate consumers using Strong Customer Authentication (SCA), the fraud rate for remote card payments fell dramatically. Payments completed without SCA in the second half of 2020 experienced five times more fraud than payments made with SCA two-factor authentication.[1]

Since the adoption of PSD2, the industry has reduced e-commerce fraud by half, employing the EMV® 3-D Secure (3DS) messaging protocol. Merchants that take advantage of 3DS have started to minimize fraud and avoid liability for chargebacks of authenticated transactions, but there is still more to be done. There is still the challenge of reducing cart abandonment.

50%

Since the adoption of PSD2, e-commerce employing EMV® 3DS has seen fraud fall by 50%[2]



The challenge around optimizing for PSD2

47%

of European merchants still have not fully employed the capabilities of Strong Customer Authentication

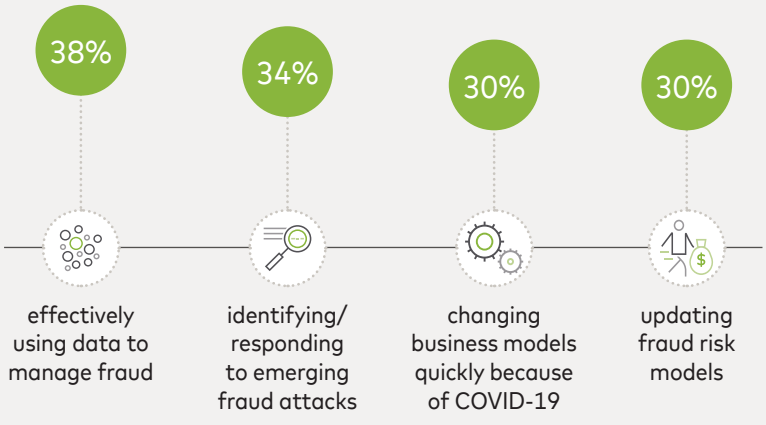
While nearly all European merchants (91%) have begun to implement SCA, 47% still have not fully employed its capabilities.[3] Admittedly, the path to optimizing the advantages of PSD2 can seem daunting. When merchants worldwide were asked what impacts SCA implementation is having or will have on their business in 2023, they cited these challenges[2]:

Impacts of SCA implementation on merchants' business

As payment methods, channels and fraud evolve, merchants struggle to keep up

PSD2 addresses rising online fraud by employing additional data to identify consumers and authenticate transactions accurately and securely. But many merchants, especially small and medium-sized enterprises, need help implementing these capabilities. In 2023, many merchants admit they face the following challenges[2]:

Merchants face the following challenges implementing PSD2



How merchants can take full advantage of shared data for greater security

The payment ecosystem is ever evolving, and every year more data insights are used responsibly to provide consumers more satisfying and safer products and services; help issuers, acquirers and merchants drive revenue growth; and empower governments to serve citizens more effectively and efficiently. When merchants, acquirers and issuers share key data elements with each other and monitor transaction risk, we can achieve payment symmetry, understand and meet each other's needs and enable effective fraud prevention across the ecosystem. Each issuer, as well as each merchant and their acquiring bank, is unique in its fraud tolerance level and risk acceptance level. But everyone benefits when we can increase the number of good transactions approved, lower operational costs, manage the critical balance of liability shifts and deliver an outstanding customer experience while keeping fraud rates low.

Mastercard continues to work diligently to bring to merchants the information and tools they need to grow their business while staying compliant.

Our approach to delivering greater security and profitability – while enhancing the user experience

Mastercard Identity Engine uses advanced machine learning derived from billions of transactions within our proprietary network to assess the potential for risk.

To get the most benefit from PSD2 and SCA, merchants should take advantage of advanced Transaction Risk Analysis (TRA) exemptions. These exemptions allow for transactions that meet a specific low fraud threshold to avoid going through additional authentication. These exemption models are essential to maintaining the right balance between simplicity and low friction for consumers expecting a seamless digital experience and active step-up authentication when needed to effectively prevent fraud. Mastercard's approach increases the efficiency of authorizations and reduces fraud rates.

Transaction Risk Analysis models from Mastercard help merchants

Approve more transactions and increase revenue

Prevent fraud as it continues to evolve by leveraging new technologies and the increasing amount of data available

Optimize business operations

Here we will demonstrate just how to do it:

Approve more transactions to increase revenue

Mastercard can leap into action even before a merchant knows whether the cardholder is legitimate. In real time, Mastercard scores the overall risk of the identity behind a transaction, drawing on our Identity Engine and its rich validation history of names, addresses, telephone numbers, email addresses and IP addresses. It uses advanced machine learning derived from the billions of transactions within our proprietary network to assess the potential for risk.

Another Mastercard tool that helps merchants assess fraud risk in real-time is our Device API. The Device API monitors and identifies authentic consumers from potential fraudsters based on their online, mobile app and smartphone interactions. The solution is fully invisible to the customer, with friction only added to the user experience if the interaction is flagged by the API as being a potential fraud risk.

90%

of transactions below 100 euros are actually low risk[4]

Step 1

Predetermine the transaction risk by drawing on real-time identity and behavioral insights

Even prior to any authentication, merchants can leverage identity insights from Mastercard to classify a transaction as low or high risk without any unnecessary friction. With these tools, only higher risk transactions need to be stepped up for cardholder authentication. Our research shows that 90% of transactions below 100 euros are low risk,[4] so merchants can most often avoid a step up in the authentication process.

Step 2

Balance the security and UX requirements of PSD2 by sending all transactions through 3DS, applying cardholder step-up authentication only where it is needed

By determining the pre-authentication risk, merchants can classify transactions as either low or non-low risk.

- For lower risk transactions, we recommend sending these transactions through 3DS, and request an exemption from the issuer, as the likelihood of this transaction being fraudulent is very low as predetermined by Mastercard.
- For transactions that are flagged as non-low risk, we recommend flagging the transaction for a challenge through 3DS to effectively help prevent fraud and to increase authorization approval rates.

Ultimately, to benefit from the most transactions being approved, merchants should focus on finding the sweet spot that balances security and a good user experience.

Balancing security and user experience needs delivers these benefits

Optimizes the ability to get transactions approved

Minimizes fraud rates

Minimizes operational cost

By effectively leveraging data insights, merchants are integrating multiple, real-time, predictive scores with one API — leading to increased revenue and improved customer retention and boosting lifetime value and sales.

↓12.1%

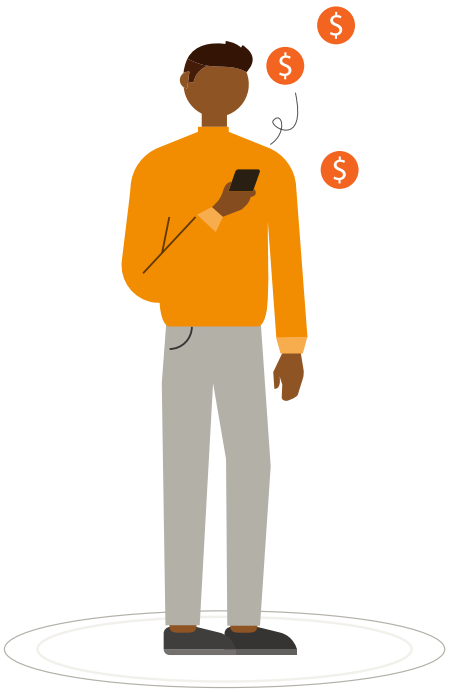
Card-not-present fraud in Europe fell 12.1% in 2021 alone[5]

Prevent fraud beyond the CNP-related type

Optimizing transaction authentication is a big step forward. Card-not-present fraud in Europe has been declining in the past few years, falling 12.1% in 2021 alone, to €1.28 billion.[5] But merchants still face an array of ever-changing and growing fraud types:.

- Phishing/pharming/whaling
- First-party misuse ("friendly fraud")
- Card testing
- Identity theft
- Scam fraud

As these and new types of fraud emerge, merchants face ongoing challenges and regulatory and operational requirements. To help improve digital payments security and increase approvals, Mastercard identity data and insights leverage over 7 billion identity elements, 5.5 billion device identities and 37 billion digital interactions. With these insights, our customers see a 60% increase in frictionless verifications, helping reduce the number of good customers that are challenged to provide additional documentation.



The Identity Engine employs more than 7 billion identity elements from real consumers and 8 billion proprietary transactions worldwide to determine probabilistically:

- If an email really belongs to transacting consumer
- If a billing address is legitimized
- When an email was first used
- Is the phone number a landline or mobile number

Our global Identity Engine then delivers an identity risk score to predict the potential for risk — helping merchants make risk-oriented decisions with greater confidence.

Mastercard provides 5.5 billion device identities that help merchants trust good users, recognize them once they become consumers and secure their accounts from harm across the customer journey, from account opening to account access and update to checkout. Mastercard helps merchants make better decisions with:

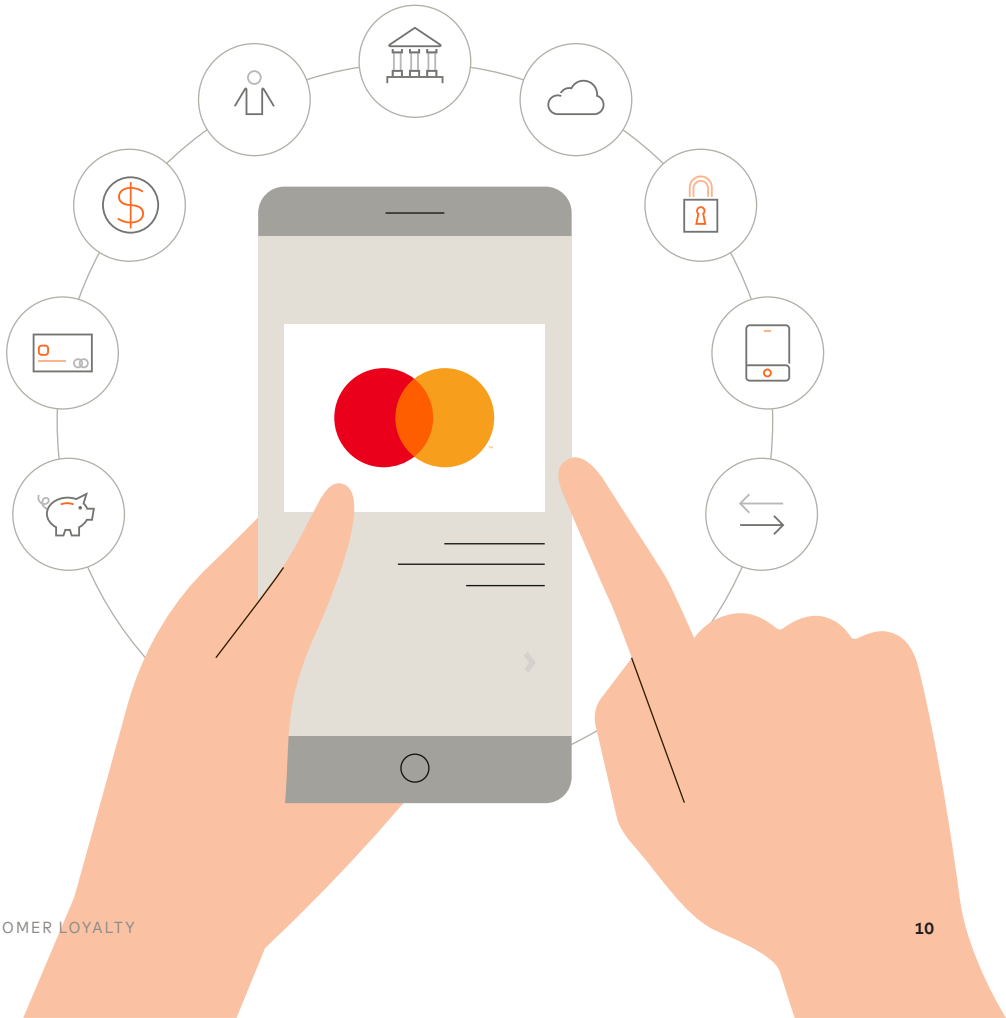
- 1-to-1 behavioral insights comparing a user's behavior against their normal behavior
- 1-to-many behavioral insights comparing the user against the normal overall population
- A global ID unique to this device
- A consortium of anonymized data and reputational insights from participating global customers to provide a real-time risk score

These powerful authentication tools provide merchants with the most sophisticated way to identify and fight fraud, no matter what form it takes or where it occurs along the customer journey. Leveraging enriched real-time data, biometrics and machine learning, merchants can ensure their fraud systems are evolving along with the fraud types — and stay one step ahead of fraudsters.

Optimize your business operations

To help merchants find the right path to implementing and optimizing PSD2 and SCA, Mastercard offers a unique set of global data-driven insights to fine-tune risk management across the customer journey. Drawing on global identity and device data, machine learning, real-time Transaction Risk Analysis models and EMV 3DS, Mastercard helps merchants:

- Decrease fraud rates by identifying bad players prior to authorization checks
- Leverage data that helps them intelligently determine who, what (device) and how (transaction approvals via Mastercard Authentication rails) are behind the transactions being made
- Approve the most transactions possible and increase revenue with a combination of data enrichment tools and exemption requests based on the results of our risk assessments
- Reduce friction and deliver the best customer experience
- Meet PSD2 requirements and optimize their overall business operations



A word on the evolution of the authentication standards and regulations

In June 2023, the European Commission announced its proposed revisions to PSD2 (to become PSD3) to update transaction requirements, strengthen consumer protections, improve open banking processes and other enhancements. It also announced a Payment Service Regulation (PSR) to address current discrepancies in implementation and enforcement approaches.

While new regulations and new standards help create new opportunities to deploy fraud protection services and measures, fraudsters will also continue to evolve their methods. In this ever-changing environment, merchants can greatly benefit from new technologies, learn about upgrades and adopt best practices designed to provide their customers with the highest levels of security. As the payment ecosystem continues to evolve, Mastercard continues to innovate and invest in new products and programs that will help you stay in line with the latest changes and protect your business.

1. European Banking Authority, Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry, Jan 17, 2022.
2. Mastercard Fraud Data reported by EEA Issuers.
3. Merchant Risk Council, 2023 Global Ecommerce Payments and Fraud Report.
4. Mastercard authorization and fraud data for the 500 largest merchants in the EEA and the UK (excluding U.S. Big Tech, such as Facebook, Amazon, Apple, Microsoft and Google), evaluated by transaction risk score, Jan-Sep 2022.
5. European Central Bank, Report on card fraud in 2020 and 2021, 2023.

Designed by Mastercard Creative Studio