FORTER®

Data Security vs. Customer Experience:

CONSUMER ATTITUDES TOWARDS ONLINE PAYMENTS AUTHENTICATION

Executive Summary

With online shopping now a common practice and the number of online buyers predicted to reach 2.14 billion by 2021, e-commerce merchants need to ensure the sensitive consumer data used in transactions is appropriately safeguarded. To balance this priority with the need for an optimal customer experience, businesses should aim to be transparent about the requirement of authentication processes and reduce friction wherever possible.

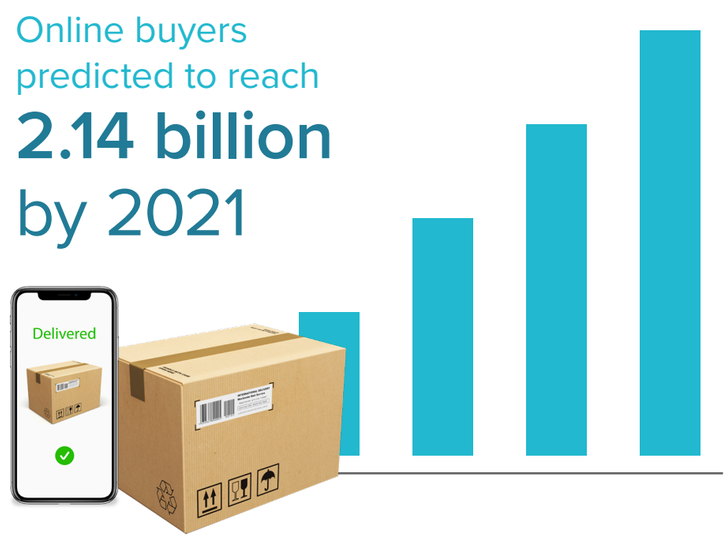
Retail is undergoing an omnichannel evolution. As consumer engagement has expanded beyond brick and mortar stores, merchants have had increasing opportunities to extend their reach across digital channels and devices. With the industry stretching further than ever, a subsequent spike in global revenue — set to tip $4.77 trillion in the next two years — is to be expected. It's unsurprising that fraud is rising in parallel.

Fraudsters are launching increasingly sophisticated and targeted attacks on digital retail in a bid to tap growing online spending. According to the seventh edition of Forter's Fraud Attack Index, verticals such as online apparel and accessories have seen a 44% increase in attempted fraud in Q2 2019 vs. Q2 2018. As a result, there is an urgent need for more robust online protection for merchants and their customers, which PSD2 aims to fulfil by enhancing digital verification and diminishing the vulnerabilities fraudsters can exploit.

For e-commerce merchants, however, the regulation presents many points of confusion. Implementation across Europe is disparate, with some markets already embedding new rules, while others — including the UK, Germany, and Greece — opt to embrace the European Banking Authority's offer of delayed SCA adoption. There is also the question of how consumer expectations of streamlined online shopping can be reconciled with the friction that extra authentication will likely add to the purchasing experience.

To find a way through the complexity, this report takes an in-depth look at the way online buyers conduct transactions and their reactions to varied authentication processes.

The data demonstrates that businesses need to carefully evaluate how they route consumers through multistep authentication when purchase amounts or risk levels demand further verification. E-commerce merchants can select the verification measures most likely to win favour with consumers while also achieving the all-important goal of fraud limitation and prevention and ensuring security measures are PSD2-ready. Optimising consumer experience, reducing friction in the path to purchase, and minimising abandonment will depend on informed choices.



Key Findings Include:

- A majority of participants across the UK, France, Germany, Italy, and the Netherlands find multistage authentication an unappealing security measure, and around half (UK 48%, FR 49%, DE 52%, IT 46%, NL 50%) may be more likely to abandon a purchase as a result.
- There are particular frustrations with this process when making repeat purchases from the same vendor, with a high proportion of participants not understanding the need for this.
- A significant number of participants report that the use of authentication methods such as fingerprint ID, facial recognition, and 3D Secure as part of a multistep process at the payment stage is particularly likely to cause them to abandon their purchases.

Percent more likely to abandon	3D Secure	Face ID	Fingerprint ID
UK	45%	60%	54%
FR	44%	59%	55%
IT	46%	58%	49%
NL	52%	59%	56%
DE	56%	61%	55%

Methodology

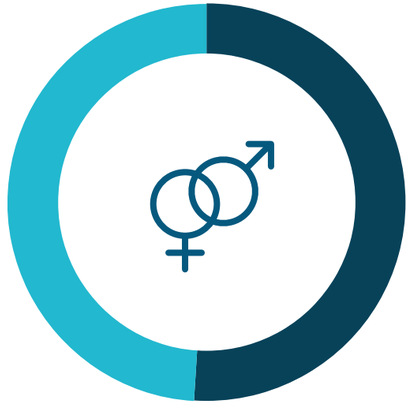
The Data Security vs. Customer Experience: Consumer Attitudes Towards Online Payments Authentication report study was conducted in June 2019 and covered five core European markets. A total sample of 5,069 consumers over 16 years of age took part through an online survey, broken down by country: France (20%), Germany (20%), Italy (20%), the Netherlands (20%), and the UK (20%). The survey evaluated consumers' methods of digital purchase and their perspectives on a range of online payment authentication tools, in addition to their knowledge of upcoming changes. Specifically, the survey set out to examine how consumers felt towards multistep authentication as enforced by PSD2.

DEMOGRAPHICS OF CONSUMERS SURVEYED

By Region

20% United Kingdom
20% France
20% Italy
20% Netherlands
20% Germany

By Sex



51% Men
49% Women

By Age

56.8% Aged 35+
43.2% Aged 16-34

Key Findings: Purchasing Methods

OMNICHANNEL SHOPPING IS THE NORM

Data collected from all regions shows that connected mobile devices have now reached parity with desktop computers as popular purchasing tools. Exactly the same number of consumers — 53.4% — use smartphones and desktop computers for their digital purchases, with a lower yet significant 22.4% also shopping via tablet.

Devices consumers use to make online purchases

Smartphones

53.4%

Desktop

53.4%

Tablets

22.4%

RECOMMENDATION:

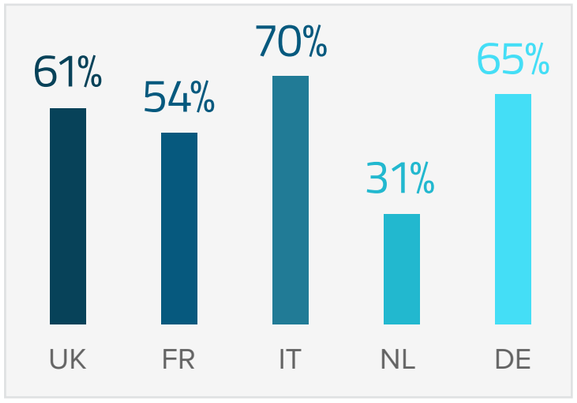
The high usage of smartphones and tablets suggests that many online purchases are made on the move, conveying a need for greater security as transactions take place over open Wi-Fi networks.

BETTER THE PAYMENT YOU KNOW

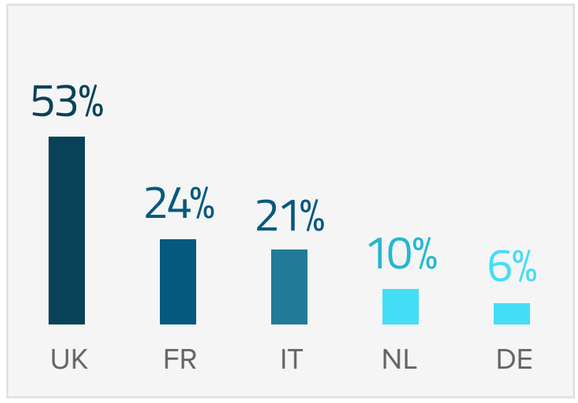
Comparison of payment methods across markets quickly reveals a common trend towards several established options. PayPal, for instance, is heavily used in almost all EMEA areas: adoption rests at 70% in Italy, 65% in Germany, 61% in the UK and 54% in France, before dropping to 31% in the Netherlands. The global digital platform is closely followed by credit cards, each used by more than 20% of consumers in the EMEA markets. On the whole, newer methods such as Amazon Pay, Google Pay and Apple Pay are still emerging.

Adoption of payment methods by country

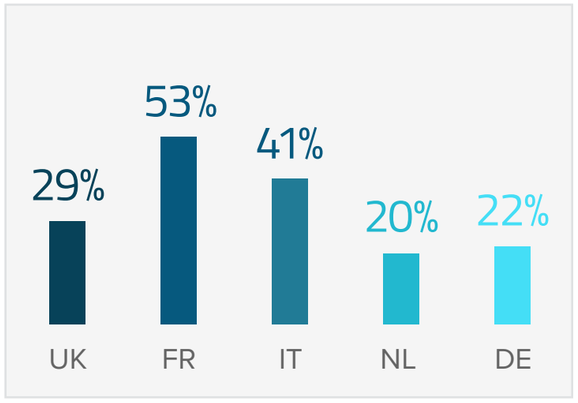
Paypal



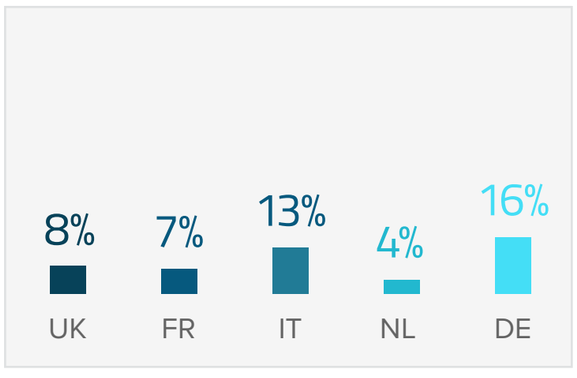
Debit Cards



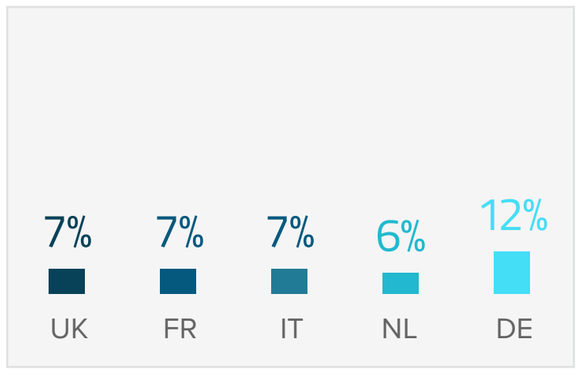
Credit Cards



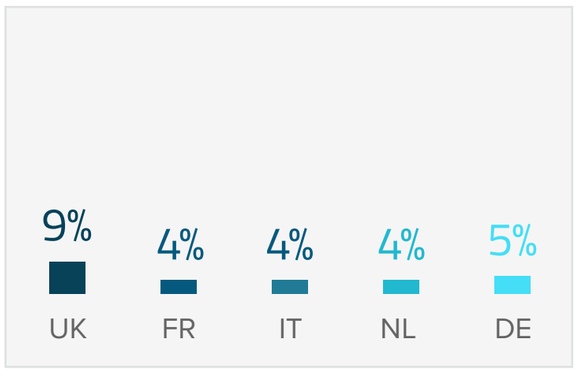
Amazon Pay



Google Pay



Apple Pay



RECOMMENDATION:

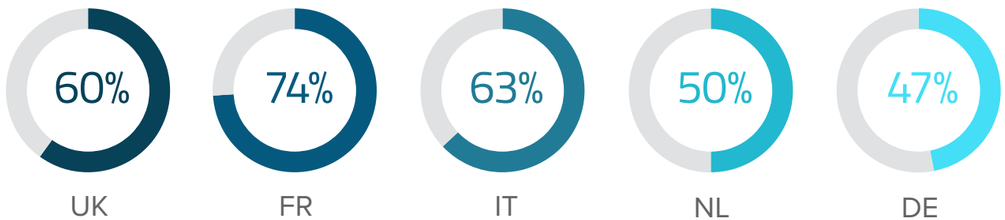
Although consumers tend to stick with trusted payment options, retailers should remain aware of emerging innovations in payments technology and ensure their authentication systems are compliant with and adaptable to newer methods.

Key Findings: Authentication

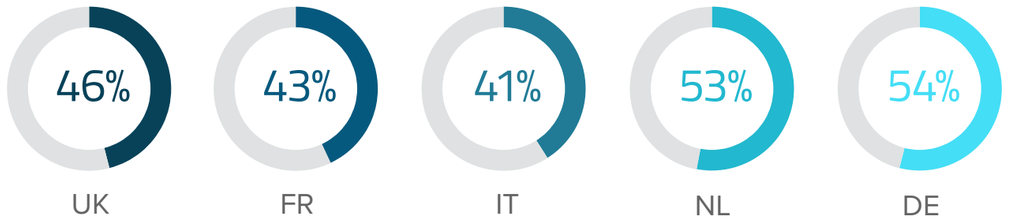
MIXED FEELINGS TOWARDS SECURITY

Encouragingly, findings signal that consumers aren't necessarily averse to the concept of authentication. In fact, more than four in ten respondents overall understand the need to authenticate a purchase and are happy to participate, with recognition especially high among consumers in France (74%) and the UK (60%). It seems negative attitudes stem more from inefficiencies or low transparency in implementation than general use. Over 30% of consumers cite frustration with multifactor authentication for repeat purchases from the same vendor, since they don't comprehend the need in this instance. Additionally, almost half of respondents across regions feel nervous about their personal data during online payment authenticationand on average, about a third do not believe authentication is a secure process. All together, the data suggests that better education around the reasoning behind multifactor authentication will minimise consumer resistance and allow companies to capitalise on the broadly positive view of verification. Retailers need to ensure that consumers understand that these processes benefit them by better protecting them against fraud. Furthermore, retailers should look to security measures that effectively protect data at all stages in the path to purchase to demonstrate their commitment to keeping consumers safe and build trust.

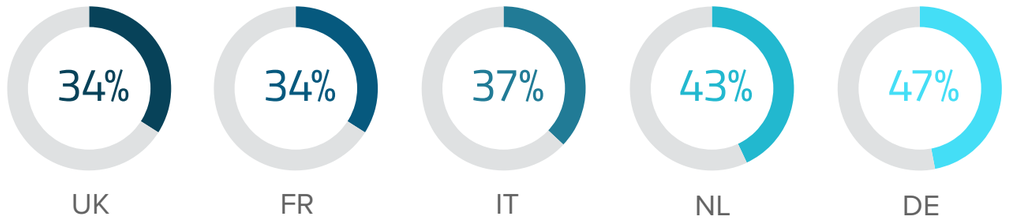
Consumers who understand the reason for authentication and are happy to participate.



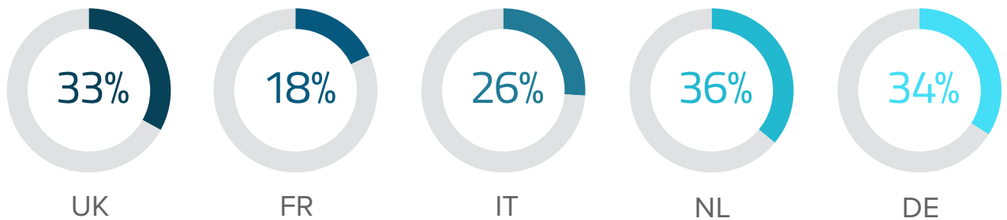
Consumers who feel nervous about their personal data when authenticating online purchases.



Consumers who do not understand the need for multifactor authentication for repeat purchases.



Consumers who do not agree that authentication is a secure process.



COMPLEXITY FUELS PURCHASE ABANDONMENT

Multifactor authentication is another known quantity for consumers. With its use now standard at certain stages of the purchase path, such as logging in to e-commerce platforms, many will have encountered security that goes beyond an entry password.

The issue, however, is that they aren't accustomed to jumping through more hoops at other stages, such as payment. Findings reveal that around three in ten consumers across regions would seek an alternative retailer if asked to complete multistep authentication when making a purchase. Moreover, a similar percentage claim they would even abandon the purchase altogether.

To preserve their bottom lines, retailers must provide a clearer explanation of the dual motivation for multifactor verification: consumer safety and revenue defence. It is also important to identify which authentication approaches cause the least concern.

Consumer reactions to multistep authentication	Would shop elsewhere	Would abandon
UK	30%	27%
FR	28%	26%
IT	27%	28%
NL	34%	34%
DE	28%	35%

LEVELS OF COMFORT WITH DIFFERENT AUTHENTICATION METHODS

Findings reveal strong links between familiarity and comfort when it comes to authentication type. The verification methods consumers come up against often are also the approaches they feel most comfortable with: passwords, emails, and SMS. Exact levels vary across markets; for example; the French are most enthused about SMS (92%), while the Italians prefer passwords (89%). But, generally, trends show that confidence steadily decreases in line with how common methods are for consumers, with newer methods such as fingerprint ID and facial recognition ranking significantly lower: 59% of UK consumers are comfortable with facial recognition, and this number drops to 44% for the Netherlands.

The data highlights that the path to payment authentication acceptance will, at least initially, involve starting with methods consumers know best. By adopting this approach, businesses can increase their chances of retaining consumer satisfaction as they enhance security and prepare for PSD2 legislation.

However, it is worth noting that older verification tools are also familiar to fraudsters and in turn are vulnerable to attack. To ensure customers are adequately defended, businesses must ensure their security efforts encompass the entire customer journey — not just the point of transaction. Complying with PDS2 should only be the beginning; retailers must aim to consistently monitor every leg of each buying journey so alternative attack methods, such as account takeovers (ATOs), can be prevented.

Consumers who are comfortable with each method of authentication as part of a multi-step process.

	Password	Email	SMS	3D Secure	Fingerprint ID	Face ID
UK	86%	71%	77%	78%	74%	59%
FR	88%	86%	92%	77%	64%	49%
IT	89%	88%	88%	74%	68%	54%
NL	79%	69%	69%	62%	74%	64%
DE	74%	74%	75%	54%	59%	44%

Four Key Takeaways

Online Purchase Authentication in General

1

Consumers are generally happy with the idea of online purchase authentication, but only when processes are familiar and efficient.

New Authentication Methods

2

Many consumers are uncomfortable with newer authentication methods such as facial recognition and fingerprint ID, preferring passwords or emails.

Speed of Authentication

3

Consumers are frustrated when payment authentication slows down and disrupts their purchase journey by adding seemingly unnecessarily steps.

Multi-factor Authentication

4

Multifactor authentication at the payment stage is currently unpopular, with nearly half of consumers likely to abandon purchases as a result.

Conclusion

PSD2 may have brought online payment security into the spotlight, but it isn't the only reason retailers should be enhancing their digital defences. As increased online spending attracts criminal interest, both business revenues and consumer wallets are at greater risk of fraud. Consequently, there is an urgent need for robust security throughout the purchase journey. But e-commerce merchants must tread carefully.

Consumers have a complicated relationship with online payment authentication. This study illustrates that most are open to verification and understand its key advantages, in theory. At a practical level, however, this enthusiasm can often be overshadowed by irritation and uncertainty. Use of processes that are perceived as overzealous or cross into unfamiliar territory makes consumers feel uncomfortable and annoyed, even driving them to seek more familiar, and less convoluted, paths to purchase with other retailers.

Overcoming these challenges will require a multifaceted solution. As well as educating consumers about the importance of multifactor verification, merchants must offer the right mix of security and convenience. By using best-in-class fraud prevention tools that continuously monitor for any suspicious activity, and only implementing preferred additional authentication methods when necessary, retailers can minimise friction and maximise consumer satisfaction and safety.

FORTER®

ABOUT FORTER

Forter is the leader in e-commerce fraud prevention, protecting over $140 billion in online commerce transactions for over 500 million consumers globally from credit card fraud, account takeover, identity theft, and more. The company's identity-based fraud prevention solution detects fraudulent activity in real-time, throughout all online consumer experiences.

Forter's integrated fraud prevention platform is fed by its rapidly growing Global Merchant Network, underpinned by predictive fraud research and modeling, and the ability for customers to tailor the platform for their specific needs. As a result, Forter is trusted by Fortune 500 companies to deliver exceptional accuracy, a smoother user experience, and elevated sales at a much lower cost.

Forter is backed by $100M of capital from top-tier VCs including Sequoia, NEA, and Salesforce.

www.forter.com