THE PAYPERS

Insights into Payments and Beyond

Fraud Prevention in Ecommerce Report 2022-2023

What It Takes to Build Trust and Safety in Digital Commerce

Supporting partners:

MRC

Marketplace Risk.

Key media partner:

mpe MERCHANT PAYMENTS ECOSYSTEM

Worldline

How to Optimise User Experience While Ensuring a High Level of Security

Claire is responsible for the product management of Strong Customer Authentication & Security solutions such as Access Control Server, Trusted Authentication, and Digital Intrusion Protection. With 10 years of experience in international business developments and bids, she has developed strong skills to understand customers and market requirements, with a special focus on security, payments, and identity.

Claire Deprez-Pipon ▪ *Lead Product Manager of Identity & Authentication* ▪ Worldline

Strong authentication has been deployed since June 2021. It was intended to promote innovation and fight against fraud in online card payments. Indeed, in 2019, **80% of the value of card fraud resulted** from Card-not-present (CNP) transactions.

The primary objective of reducing fraud was achieved, as a significant decrease in CNP fraud can be seen; for remote card payments reported by acquirers, the share of fraud in total volume is five times higher for the payments authenticated without SCA compared with **the payments authenticated with SCA**.

Moreover, even if the kick-off has been complicated for many e-retailers, success rates on strong authentication have also increased. A new authentication method implemented will have an increase in the success rate of 30% in the first six months of the implementation, mainly due to:

- Enrolment time of the authentication method;
- Time for cardholders to learn how to use the authentication method;
- Time to deal with any problems integrating the payment method into the end-to-end purchase process;
- Communication to support the cardholder in enrolment and authentication.

What can be done to make the user journey smoother?

The reinforced One-Time Password SMS (OTP) has often been deployed as a complement to a mobile strong authentication method, because it is simpler to implement, and allows it to meet time constraints. However, it is a less secure method (the SMS is not encrypted, the message can be intercepted; the OTP and the password are privileged factors for phishing because they are easily transmitted, etc), and whose ergonomics are not the most suitable (password can be forgotten, two-step strong authentication, etc). To remove friction from the user journey, banks must:

1. Use an authentication method that does not impact the user experience

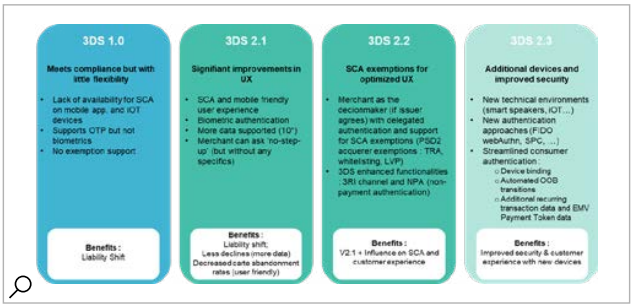
- Implement a transparent authentication factor, based on the trusted device (a smartphone or browser). This authentication method is a good alternative to SMS OTP, as it eliminates an authentication step thanks to the possession factor which is transparent while providing a higher level of security.
- Implement a biometric solution, whether linked to the OS (smartphone biometrics, computer biometrics), or via external solutions. This technology is preferred by many users as it improves the overall experience with password-less authentication **(74% of respondents chose biometric authentication as their preferred method)**. The use of biometrics can increase the success rate by at least 10%.

2. Work on the authentication workflow and user journey

The integration of an authentication method into the user journey can impact the success rate. The diversity of the type of integration is multiplied at each node of the authentication and payment chain.

The same authentication method can be integrated in different ways in the banking environment (Software Development Kit, separate mobile application, authentication flow, PIN, or biometrics). Moreover, authentication pages are integrated by merchants differently, depending on the channel (mobile, browser) or the type of integration (i-frame, redirection, 3DS SDK). →

Therefore, it is important to implement the ergonomic evolutions proposed by the EMVCo 3D-Secure 2.1 protocol (support biometric authentication), 2.2 (app-to-app flow), and 2.3 (SPC/ FIDO, device binding), which continuously improve the customer experience by adding more devices and more integration to the authentication flow.



3. Increase the exemption rate, but not at the expense of fraud

The rate of friction can directly impact the success rate. **A report by Ravelin** illustrates that the higher the percentage of frictionless payments is, the higher the authentication success rate. For example, the success rate in North America is 99% for 89% frictionless, compared to 55% in Europe, with 46% frictionless.

However, a high frictionless rate can still impact fraud rates. It is important to put in place rules that allow for the application of exemption requests while relying on scoring to assess the risk, and taking into account artificial intelligence. Data collection will become increasingly essential in the authentication process, as it feeds artificial intelligence, not only to feed Risk-Based Authentication (RBA) scoring, but also to enable the detection and prevention of phishing, adaptive authentication with risk scoring, and behavioural analysis.

How Worldline assures a high level of security while improving the customer journey?

Worldline supports its customers throughout the 3D-Secure authentication chain:

- **Worldline Access Control Server** allows fraud prevention for e/m-commerce implementing 3D-Secure and strong authentication. It provides a rich back-office and artificial intelligence tool based on an analysis of past transactions to improve fraud management.
- **Worldline Trusted Authentication** protects your online services from unauthorised access with Strong Customer Authentication solutions for all devices, enabling password-less authentication thanks to transparent factors, biometrics, and FIDO authentication.
- **Worldline Digital Security Suite** protects your fleet with local and remote protection of your devices. It enables adaptive authentication methods and enrolment with our device eligibility scoring, thanks to our artificial intelligence model on device scoring and behavioural biometrics.

With all these measures, where is the risk of fraud now?

The new authentication methods are reliable and have very low fraud rates. The main concern remains on the enrolment process which proves to be the weakest point of the chain. To enrol an authentication method, PSD2 requires to have two authentication factors. But, at this stage, the information known by the bank is the mobile phone number and the password. These two elements are most often the target of phishing attacks. The risk is now positioned on the cardholder.

It is important to avoid methods (both enrolment and authentication) that can be 'phished' (notably SMS OTP and password). Hence, the future lies in biometric and behavioural authentication methods, which are not very susceptible to phishing, but also in the use of the EU Digital Identity Wallet, which will simplify and secure the enrolment process.

Click here for the company profile

Company	Worldline
WORLDLINE	Worldline is the European leader in the payment and transactional services industry. With innovation at the core of its DNA and thanks to a presence in 30+ countries, Worldline is the payment partner of choice for merchants, banks, public transport operators, government agencies, and industrial companies, delivering cutting-edge digital services.
Background information	
Year founded	1973
Website	https://worldline.com/en/home.html
Target group	Merchants/ecommerce Banks/FS Corporate Fintech Telecom
Supported regions	Europe
Contact	Claire DEPREZ-PIPON – claire.pipon@worldline.com
Company's motto	Digital payments for a trusted world
Member of industry association and/or initiatives	EMVCO, W3C, FIDO Alliance, EDPIA, EPI
Core solution	
Core solution/problems the company solves	Customer authentication Behavioural biometrics We offer a multi-factor authentication solution that brings security to all sensitive operations (payment, online banking, digital identity, etc.). This solution is combined with different fraud detection assets which prevent intrusion and attacks.
Technology	
	Cloud-enabled
Data input	

Online authentication	proprietary capability	third party	both
Behavioural biometrics			x
Physical biometrics		x	
Device fingerprinting	x		
Geo-location	x		
Remote access detection		x	
Mobile app push	x		
3-D Secure 2.0	x		
Hardware token		x	
One-time passwords	x		
Knowledge-based authentication	x		

Methodology	
Machine learning	Rule-based Supervised ML Hybrid
Decisioning	
	Manual review Case management Decision orchestration

Business model	
Pricing model	Transaction-based pricing model
Fraud prevention partners	Internal capabilities + inform Riskschield
Year over year growth rate	For business revenues, please refer to our corporate investor page https://investors.worldline.com/en/home.html Yearly growth: 80%
Number of employees	20,000+
Future developments	For more details, please contact our sales team.
Customers	
Customers reference	For more details, please contact our sales team.
	View company profile in online database*
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our **online company database**.

WORLDLINE

Worldline Authentication Solutions

Biometrics | AI | Security

How to optimise **user experience** while ensuring a high level of **security**?

In 2022

+500M
strong authentications

+2B
3DS transactions

- **Seamless authentication method**
- **Adaptable to your digital strategy**
- **Data collection for intelligent scoring**

www.worldline.com

WORLDLINE

claire.pipon@worldline.com