THALES

gemalto
a Thales company

Can innovative payment experiences survive the need for Strong Customer Authentication?

CNP (card-not-present) fraud and new regulations such as PSD2 (revised Payment Services Directive) pose significant challenges for pioneering retail payment initiatives. To ensure future success, merchants will need to identify the right strategy for swift and seamless validation of transactions; in particular, should merchants rely exclusively on the industry-standard benefits of 3-D Secure 2.0, or combine it with the additional control over the user experience that is offered by delegated authentication?

Introduction

As well as creating entirely new channels for customer interaction, the eCommerce revolution is profoundly changing our expectations of the physical shopping environment. Having grown up accustomed to instant, 24/7 fulfilment via a smartphone, millennials in particular are looking for similar standards of immediacy and personalization when they visit a store.

And that's precisely what the world's most dynamic merchants are delivering. An innovative array of smartphone-enabled experiences is emerging, primarily focused on check-out options including user-presented QR codes and scan and go. In addition, new mobile apps are offering consumers real-time, customized promotions and couponing, along with advice and information tailored to individual preferences.

This pioneering generation of transparent in-store payment journeys is being adopted enthusiastically by consumers. However, going forwards, merchants face strong headwinds, most notably in the need to provide robust fraud protection and ensure comprehensive compliance with rigorous new regulatory frameworks. In the EU, for example, PSD2 comes into effect as soon as September 2019. Potentially, initiatives such as this could fatally compromise exciting new customer experiences, just as they are beginning to gain traction.

In terms of both regulatory compliance and fraud protection, the heart of the issue lies in the requirement to authenticate customers, as quickly and painlessly as possible. To achieve this, two distinct strategies are available to merchants. One is to draw exclusively on 3-D Secure 2.0, created by the leading international payment processors and available to all domestic and international payment schemes. The other is for merchants to shoulder the responsibility themselves, by implementing a delegated authentication solution in their own application.

For each individual merchant, choosing the right approach will be critical to the sustainability of their efforts to create innovative and exciting journeys, in both physical and online environments. But, by positively embracing the need for a step change in customer authentication, retailers will do more than simply preserve the speed and convenience enabled by applications such as scan and go. With the correct solution in place, they can also ensure the outstanding levels of trust and confidence that are equally important to today's consumers.

1. In the brave new world of omni-channel retailing, what exactly do shoppers want?

Around the world, the desire for a radical shake-up of the shopping experience is clear.

In the US in 2018, half of all online transactions were undertaken via Amazon. The smooth, one-click checkout experience is clearly a key factor, reflected in the dramatic improvement in conversion rates it achieves, compared to other checkout modes.

Similarly, Uber has disrupted a long-established urban transportation model, primarily by offering a simple, app-based experience that enables instant vehicle booking and 'invisible' payment.

Recent consumer research further highlights the shifting landscape, both in-store and online. For example, in 2018, Forrester Research found that 65% of US consumers would use a self-checkout line, 32% would shop digitally, and 28% would utilize a self-scanning option. Similarly, in the same year, Acosta reported that nearly 50% of millennials (aged 18-35) were very interested in scan and go shopping experiences.

In a nutshell, many customers want more control, and the option of much faster, self-service checkout. Equally apparent is the central role now played by the smartphone.

In-store, shoppers are using connected mobile devices to compare price and product information, redeem coupons and other offers, geo-locate goods and, increasingly, pay for everything with a single click or scan.

65% of US consumers would use a self-checkout line

32% of US consumers would shop digitally

28% of US consumers would utilize a self-scanning option

50% of millennials (aged 18-35) were very interested in scan and go shopping experiences.

2. Meeting new expectations: fast and transparent self-service check-out, personalized service and support

A leading European retailer recently predicted that one third of all its check-out transactions would be scan and go within three years.

Given such powerful trends in customer behaviour and expectations, the emergence of exciting new smartphone applications, designed specifically to enhance the 'bricks and mortar' retail environment, should come as no surprise. And, for both consumers and merchants, these initiatives can deliver compelling returns. Time-poor shoppers avoid lengthy checkout queues, whilst reaping the benefits of real-time, personalized promotions.
For merchants, the ability to leverage customer smartphones facilitates straightforward and cost-efficient implementation of cutting-edge solutions. Furthermore, with payment processes now quite literally in the hands of shoppers, space previously dedicated to checkouts can instead be used for additional, revenue-generating product displays. In addition, cashiers can be redeployed as in-aisle advisors, boosting sales and further enhancing the customer experience.

Even at this early stage of implementation, these redesigned and reimagined 'phygital' retail offers are making a powerful connection with consumers. But for those merchants that recognize the potential to secure competitive advantage, the future is not without challenges. Uppermost among them is the escalating threat posed by fraud and, more specifically, CNP fraud.

3. Counting the cost of fraud

Here the figures speak for themselves.

Between 2012 and 2016, the percentage of total fraud accounted for by CNP transactions rose from 60% to 73%. (Source: EBA Fifth Report on Card Fraud, September 2018)

In Europe, fewer than 10% of total retail sales are currently conducted via eCommerce, yet it represents 73% of the sector's total card payment fraud. (Sources: Centre for Retail Research, ECB Card Fraud Report)

Clearly, issuers and merchants do not want to expose their business or customer base to the menace of fraud. In addition to direct losses, the impact on corporate reputations and the all-important quality of trust can be devastating. As a result, over the past few years, a broad range of tools have been deployed in the search for greater security, particularly for CNP transactions.

The industry tried authentication solutions to secure online accounts but none of them eradicates it

	PAYMENT SCHEMES 3DSECURE 1.0	FRAUD DETECTION TOOLS	GAFAS SINGLE SIGN ON
EFFICIENCY IN FIGHTING FRAUD	●●●◐ Relies on SMS code (1FA) – cases of fraud with SIM swap	●●○○ Not all merchants are equipped. No strong authentication, only range of indicators	●○○○ Relies on password (1FA) – can be hacked
USER EXPERIENCE	◐○○○ Poor UX: easy to forget passwords or SMS codes through unclear web pages	●●●○ Transparent for customers 3DSecure can be triggered only for risky transactions	●●●○ Smooth, easy to understand UX
DATA PRIVACY	●●●● No personal data exchanged	●●●● No personal data exchanged	●○○○ Users and merchants must agree to share their personal data with private companies

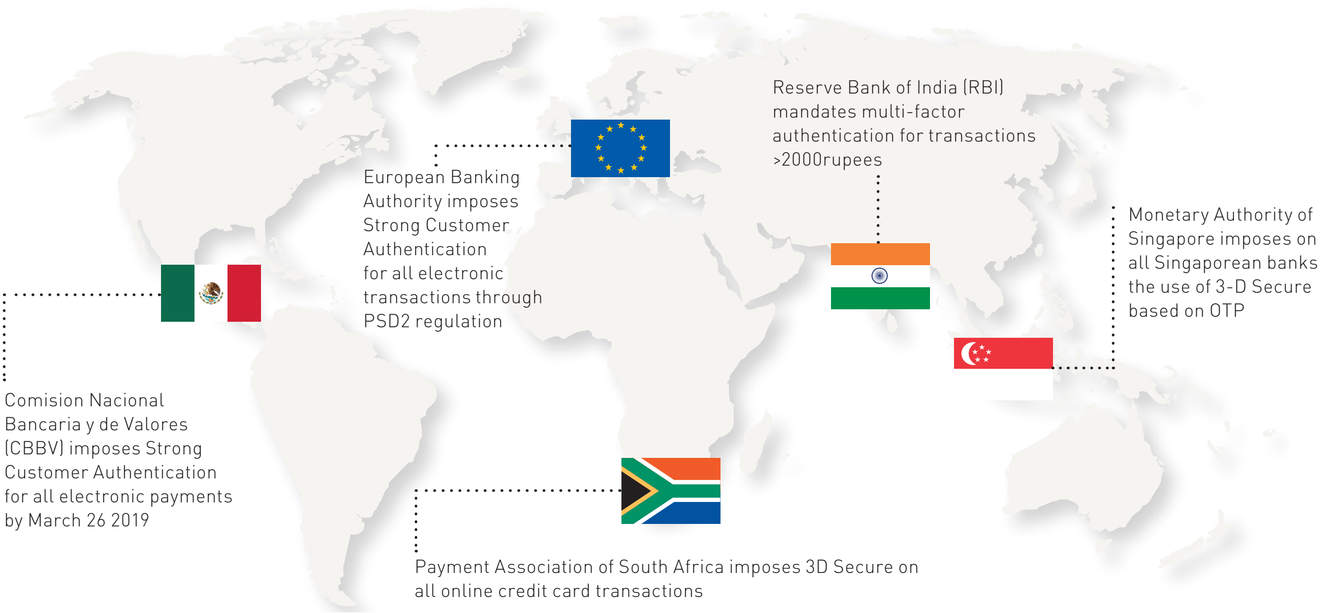
As the table demonstrates, each of these measures brings with it a mix of strengths and weaknesses. None has succeeded in eradicating the threat posed by increasingly sophisticated fraudsters.

Notably, adoption of 3-D Secure 1.0 by retailers has been limited. This is largely because of its negative impact on the customer experience; users are redirected to a new 3-D Secure window, and must enter a code received via SMS. As a result, the customer must either manage multiple message and web pages on the same handset or use two devices to complete the transaction.

4. Stricter regulation is a fact of life

With merchants and issuers struggling to stem the flow of losses, authorities have stepped in to protect consumers. Right around the world, more rigorous regulatory frameworks are being introduced.

Regulations are popping up all around the world to better protect the customers



European Banking Authority imposes Strong Customer Authentication for all electronic transactions through PSD2 regulation

Reserve Bank of India (RBI) mandates multi-factor authentication for transactions >2000rupees

Monetary Authority of Singapore imposes on all Singaporean banks the use of 3-D Secure based on OTP

Comision Nacional Bancaria y de Valores (CBBV) imposes Strong Customer Authentication for all electronic payments by March 26 2019

Payment Association of South Africa imposes 3D Secure on all online credit card transactions

In Europe, new legislation comes in the form of PSD2. Applying to all Payment Service Providers in the EU – issuers and acquirers – it becomes effective on September 14th 2019. Key requirements include mandatory Strong Customer Authentication (SCA) for all electronic payment transactions. In practice, that means 2FA (two factor authentication)

Comprehensive set of authentication factors in compliance with PSD2

What I Have

Device, token

What I Know

****

Built-in PIN code

Comes with a built-in mobile PIN security layer

Server side PIN or Password

Accepts server-based knowledge factor

What I Am

Fingerprint

Face

Comes with built-insupport for Fingerprint and Facial Recognition

Voice

Iris

Other biometrics solutions

Strong Customer Authentication is the combination of two factors drawn from the elements of Possession, Knowledge and Inherence

However, the RTS (Regulatory Technical Standards) that accompany PSD2 recognize the need to avoid creating unnecessary friction in eCommerce transactions. Consequently, it defines several transaction types that are exempt from its SCA requirements. These include contactless transactions worth less than €50, unattended terminals for transport and parking, recurring transactions, remote payments worth less than €30, and a range of transactions qualified as low-risk.

5. Strangled at birth?

Despite these measures, at first glance the implications of PSD2 appear wholly negative for the new breed of transparent, smooth and seamless customer journeys. With applications such as one-click, scan and go and QR code-based payments falling within the category of CNP transactions, any time and convenience benefits become irrelevant if the customer subsequently must validate the transaction with an OTP (One Time Password) sent via SMS, with a physical token, or through redirection to the relevant bank's application for authentication.

The good news for merchants is that solutions to this conundrum are readily available. So, whilst the issues surrounding fraud and regulatory compliance undoubtedly demand positive action on the part of merchants, they do not necessitate a retreat from innovation.

6.1 Weighing up the options – 3-D Secure 2.0

The 'de facto' response to the SCA requirements of PSD2 comes in the shape of 3-D Secure 2.0. Significantly, this is an EMVCo standard, and can be employed with any international or domestic payment scheme.

Compared to 3-D Secure 1.0, a key strength of 3-D Secure 2.0 is its risk-based approach. Only transactions identified as high risk are subject to step-up SCA. Furthermore, the use of out-of-band biometrics means that, where additional authentication is required, it has the potential to be convenient and intuitive for the end-user.

By leveraging data shared between merchants and issuers to identify and predict patterns of risk, it is anticipated that around 85% of all transactions that are undertaken in conjunction with 3-D Secure 2.0 will be exempt from step-up authentication. However, for many merchants, such a high percentage may not be possible immediately; low risk status will only be achieved over time, after a history of secure transactions has been built. The risk assessment relies mainly on machine-learning (ML) technology and the processing of tens to hundreds of transaction parameters. Many merchants are expected to struggle to extract such a long list of fields, and months or even years will be necessary to fine-tune the ML algorithms. Given current concerns over privacy and data protection, it is also likely that some merchants will be reluctant to share so much information on their customers with third parties.

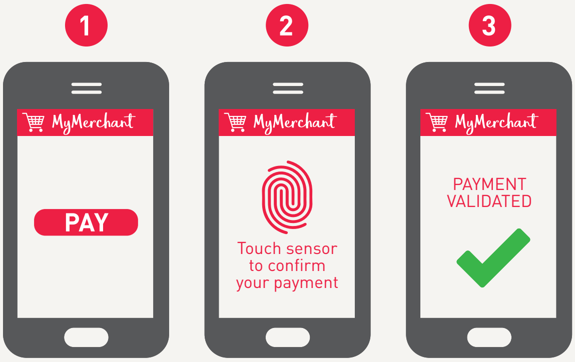
Although there are obvious benefits for merchants from letting issuers shoulder the responsibility (and liability) for SCA, for those interested in pursuing innovative in-store payment solutions, even a small proportion of transactions that do not qualify as low risk (and must therefore be redirected to the issuer's interface) will prove extremely problematic.

6.2 Weighing up the options – delegated authentication

But merchants do have a second option: taking on the responsibility for authenticating customers themselves. Significantly, this strategy offers the prospect of retaining full control over the user experience, with no danger of issuers' step-up authentication requirements being imposed on the customer. In itself, redirection represents a disruption to the customer journey. What's more, the degree of convenience provided by each issuer's SCA solution is likely to vary; some, for example, may require the customer to carry and use a physical token. With a well-designed delegated authentication solution in place, in-store or online shoppers need only scan their fingerprint or take a selfie with their smartphone to validate a transaction – all without ever having to leave the merchant's app.

The greater independence and control provided by delegated authentication does not mean a loss of support from issuers. Subject to certification, multi-lateral agreements can be secured with both international and domestic schemes. That said, in the short term at least, merchants will typically need to demonstrate a low level of risk to achieve certification. And, of course, pursuing this route means that liability ultimately lies with the merchant, not the issuer.

An intuitive and frictionless payment confirmation



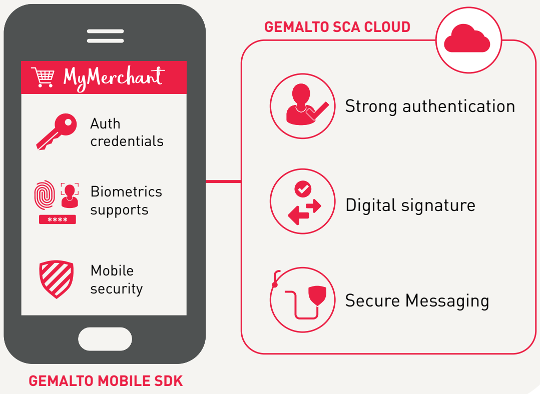
✓ **Instant authentication** with a simple touch or a selfie

✓ **Account takeover prevention:** SCA can be leveraged to secure Account log-in

7. The Gemalto offer: payment grade performance, effortless biometric validation

Where delegated authentication does provide a better fit for the merchant, proven solutions are ready to implement. Gemalto's offer here is a Cloud-based, Mobile SDK (Software Development Kit) that facilitates easy integration into the merchant's own app, speeding time to market. Fully compliant with the requirements of payment networks, and legislation such as PSD2, it is characterized by comprehensive support for biometrics and the implementation of the FIDO standard. Instead of clumsy, frustrating passwords and codes, customers can simply authenticate transactions using the biometric scanner on their smartphone; and, if a biometric sensor is not available, a PIN can still be used to complete the transaction. Payment validation becomes instant, frictionless and intuitive, and the same smooth process can be employed for access to accounts. Just as significant, these effortless journeys become an integral part of the customer experience created by the merchant, and offer the freedom and flexibility necessary to meet specific corporate and brand requirements. Added to this is the reassurance of highly secure, scalable, payment grade performance that can counter even the most sophisticated fraud attempts. Reflecting this, over seventy financial service providers worldwide already employ Gemalto's Mobile SCA solution.

Gemalto FIDO Mobile authentication overview



Conclusion: Treat SCA as an opportunity, not a threat

For retailers seeking to prosper against fierce competition from pure eCommerce players, standing still is no longer an option. Innovation is essential to meet demands for fast, personalized fulfilment, whether customers are in store or online. To maintain the growing momentum behind enhanced customer experiences, merchants should therefore adopt a positive and proactive approach to both fraud prevention and new regulatory regimes. In other words, embrace the challenges and opportunities that are now being presented. Unlike many of the previous tools that have been employed, biometric based authentication processes and sophisticated risk assessment techniques finally offer merchants the potential to combine frictionless usability with outstanding levels of protection and trust. So, whether their strategy is fully served by industry-standard 3-D Secure 2.0, or a more customized, delegated authentication solution, all merchants should recognize that Strong Customer Authentication is not an obstacle to change. Indeed, it has a vital role to play in the creation of exciting and secure retail environments that can inspire and engage the new generation of digital native shoppers.

➔ **GEMALTO.COM**

THALES

gemalto
a Thales company