PaymentsCompliance

Published on *PaymentsCompliance* (https://paymentscompliance.com)

In Depth: Card Authentication Row Escalates As EBA Asked To Delay Reforms

31ST OCT 2018 | WRITTEN BY: JOHN BASQUILL

European payments and retail groups have pleaded with authorities to let them use a payer's card details as one of two authentication factors for an online transaction, at least for a temporary period after next September's cut-off date.

From September 14, 2019, regulatory technical standards on security will require two-factor authentication on all online payments of more than €30, unless the provider's fraud rates are so low that an exemption is available.

A pillar of the revised Payment Services Directive (PSD2), those factors must be something the payer has, knows or is — in other words, possession, knowledge or inherence — and both must be from separate categories.

However, the European Banking Authority (EBA) has insisted that credit or debit card details — typically the card number and three-digit CVV code — do not constitute either a "knowledge" or "possession" factor.

"We strongly appeal to the EBA to revise their opinion to keep card number and CVV as a valid authentication factor and phase it out within the next three years to allow time for the industry to deploy alternative authentication methods without disrupting payments," said a letter submitted by a group of industry associations to EBA chief Andrea Enria on October 25.

Removing card details as a factor "will have a disastrous effect on remote commerce and will adversely impact customers, retailers, and all stakeholders of the payments ecosystem", it argued.

It was co-signed by six industry associations: the European Payment Institutions Federation, EuroCommerce and Ecommerce Europe, as well as the Merchant Risk Council, DigitalEurope and EMOTA.

Card Details As An Authentication Factor

The letter made the case for combining card details with a one-time password delivered to the payer's mobile phone. Extensive background transaction risk analysis would also take place.

Under the 3DS security protocol offered by major card schemes, fraud checks take place "behind the scenes"; the industry groups quoted a study in France that found fraud dropped to just 0.06 percent when that combination of measures was in place.

But if an additional factor is needed, as the EBA made clear in an opinion on authentication published in June, that would have to be either "knowledge" or "inherence".

The industry groups said an inherence factor, such as a fingerprint or other biometric, would "be challenging for issuers" as in most cases it would have to be developed within a year.

> "No prior recommendation, guidelines or consultation has prepared the industry for this very complex step change," said the industry associations' joint letter. "For example, not all devices have biometric hardware and not all consumers have access to them."

A position paper from Mastercard, finalised in September and seen by PaymentsCompliance, estimated that under two-thirds of Europeans have a smartphone and fewer than half have an online banking app.

"This means that a large portion of the European population, about 60 percent, risk being excluded from e-commerce, as they will not have access to an easy and convenient authentication solution," it said.

Legal experts pointed out that the second option, a "knowledge" factor, is also far from ideal.

"This would have to be a PIN or a password in order to complete your purchase with a card," said Andrea de Matteis, founding partner of De Matteis Law.

"This isn't favoured by the industry because people don't remember them. The user experience is terrible, and if you have many different cards you have to remember different passwords."

De Matteis said that retailers are reluctant to rely on passwords due to fears of transaction abandonment, while for issuers it is unclear how they would be enrolled with a password or PIN in the first place.

"Would you send them a letter, or perhaps enrol them through the online banking application?" he said. "It involves a lot of effort."

Mastercard suggested that customer abandonment "roughly doubles when a static password is required", estimating that during transition to the new authentication model dropout could be as high as 40-50 percent.

Extension Unlikely But Other Options Remain

That said, there are potential issues with the plea set out in the letter.

First, a knowledge factor has to be something only the payer knows, and that may not be the case with a card if online retailers have saved its details on file.

Second, PSD2 does not empower the European Commission or EBA to grant an extension to the effective date of the rules, nor a temporary exemption from certain provisions.

PaymentsCompliance understands that EU authorities have no appetite for agreeing to the grace period proposed by the industry groups.

Mastercard's position paper argued for an alternative that would still work without card numbers as a factor, however.

3DS 2.0, an updated version of the card schemes' risk analysis protocol, is currently undergoing testing and could be market-ready relatively soon.

According to Mastercard, the strength of fraud mitigation offered by the protocol is so strong that it should be seen as an inherence factor, equivalent to a biometric.

That is because there are more than 130 "data points" transmitted from the merchant to the issuer, such as the device, IP information, payer location, purchase trends and delivery address.

UK Finance, an influential industry body covering the country's banking and cards sectors, recently offered its support for behavioural analytics as an authentication factor in the form of new industry guidance.

Mastercard warned that if the updated 3DS protocol is not deemed to be an authentication factor, there are "no viable authentication alternatives".

"Migrating cardholders to a new authentication solution with another knowledge element, alternative to card data, will be very difficult in the very short timeframe before September 2019," it said, adding that stifled innovation, financial exclusion and extra costs to consumers could all be knock-on effects.

At least one question on this issue has been submitted to the EBA's online Q&A tool for PSD2, so if that question is accepted the regulator would be due to provide additional clarity within a matter of months.

TOPICS

Filter: Payments Regulation

Fraud & Security

Card Technology

GEOGRAPHY

Europe

SECTORS

Acquiring & Issuing

Banking

Cards

Payment Processing

CONTENT

Insights & Analysis