PSD2: THE ROAD TO STRONG CUSTOMER AUTHENTICATION (SCA)

J.P.Morgan

INTRODUCTION

The Second Payment Services Directive (PSD2) was officially published by the European Commission in December 2015, following on from the First Payment Services Directive (PSD1), which was implemented in 2009. The drive to upgrade PSD1 was due to a number of wide-ranging changes in the payments space, which necessitated a regulatory response.

One of the areas of concern for European regulators was security. Since PSD1 was first implemented there has been a huge rise in ecommerce in Europe, coupled with an increased use of mobile phone payments and other transaction methods designed to speed up the shopping process. In turn, this has resulted in major increases in the incidence of consumer fraud in Europe, with these rates now at record highs[1]. For example, in the UK, in 2016, nearly £309 million was lost to card fraud in ecommerce transactions alone. This compares to just £13.6m in 1998[2].

As a result, PSD2 has included a specific mandate that focuses on Strong Customer Authentication (SCA) as a way to improve security for the consumer. One example of SCA is two-factor authentication. This is the title given to a security system that, as its name suggests, relies on two stages, not just the password alone. The traditional way of adding a second stage is by introducing something that only the user knows – such as the ubiquitous "what is your mother's maiden name?" question. But, increasingly, the second-stage of authentication can be something that the user possesses (such as a mobile phone) or is – a fingerprint, iris recognition or voiceprint.

GETTING INTO FLOW

However, the implementation of two-factor authentication for online transactions risks disrupting the buying experience. When customers are shopping online, they want a quick, frictionless process. Having to halt this to answer a number of security questions can potentially result in shoppers abandoning the purchase.

SCA means authentication based on the use of two or more elements

Knowledge

(i.e., something only the user **knows**)

E.g., password

Possession

(i.e., something only the user **possesses**)

E.g., mobile phone

Inherence

(i.e., something only the user **is**)

E.g., finger print

Consequently, PSD2 has included a number of provisions that allow merchants to offer 'frictionless flow' for certain transactions, determined by the size of the purchase and the fraud rate of the acquirer. Frictionless flow allows for these transactions to be passed through to the issuer without the need for SCA. Adding the option of frictionless flow is designed to ensure the consumer has more protection from fraud, but without unduly disrupting the buying experience.

THRESHOLDS FOR FRICTIONLESS FLOW ON REMOTE CARD TRANSACTIONS

TRANSACTION SIZE	FRICTIONLESS FLOW
Transactions up to €500	Frictionless flow allowed if acquirer's fraud rate is less than 0.01%
Transactions up to €250	Frictionless flow allowed if acquirer's fraud rate is less than 0.06%
Transactions up to €100	Frictionless flow allowed if acquirer's fraud rate is less than 0.13%

SCA INTERPRETATIONS

However, with PSD2 there are a number of areas concerning SCA and frictionless flow that remain open to interpretation. European regulators now need to implement the new directives in a way that protects consumers whilst also enabling an effective ecommerce environment. As Brian Gaynor, Executive Director for Product Solutions in Europe at J.P. Morgan, states: "SCA is designed to reduce consumer fraud, without adversely affecting ecommerce. This is why you need to allow frictionless flow in some instances, but it is important to find the right balance."

There are three important areas for scrutiny:

1. Payments initiated by the payee
2. Trusted beneficiaries – whitelisting for card-based payment instruments
3. Transaction risk analysis (TRA) – implementation issues

Notes:

[1] FICO, 'E-commerce Growth Drives Rise in UK Card Fraud.' Available at: http://www.fico.com/europeanfraud/united-kingdom. Accessed October 2017.

[2] FICO, 'E-commerce Growth Drives Rise in UK Card Fraud.' Available at: http://www.fico.com/europeanfraud/united-kingdom. Accessed October 2017.

J.P.Morgan

PAYMENTS INITIATED BY THE PAYEE

When PSD2 was first released there was much discussion focused on the requirement to challenge transactions and ask the consumer for SCA. After all, while this may be desirable from a security point of view, merchants also want the sales process to be as seamless as possible. As Gaynor explains, it became a hot topic in the industry. "Initially, when PSD2 was first released, it seemed that you'd have to challenge every transaction and ask the payer for SCA. This would have had huge implications for ecommerce – not least because many payments are actually initiated by the payee. This realisation has resulted in the creation of a common framework so that one method of payment isn't preferred over another."

Some examples of payee-initiated transactions include magazine subscriptions or mobile phone bills, where a recurring sum is taken from a customer at a fixed date. These are so commonly used that there is a strong case for these transactions to be as frictionless as possible.

SCA CHALLENGES

That's not to say that there shouldn't be any challenge at all. J.P. Morgan supports the preference for SCA to be applied when a recurring payment agreement is first set up and/or the initial payment is authorised. Subsequently, SCA should not be applied to any successive transactions initiated by the payee. After all, consumers don't want to have to complete SCA every time a utility or mobile phone bill is paid.

In this instance, there may be no need to apply SCA even if the transaction amount varied from month to month. In addition, there may be no value limit applied either. So if a bill was regularly around €50 a month and then went to €500 in one month, there may be no requirement to apply SCA. Although, as Gaynor points out, in practice it would still need to go through the authorisation process.

Another important distinction is that whereas PSD2 already provides an exemption for direct debits (which refers to payments that go directly out of a customer's bank account) our preference is that this exemption is extended to all fixed recurring payments, irrespective of the payment method used (e.g. even if it is credit card rather than direct debit).

CARD ON FILE A STICKING POINT

There are also other anomalies with PSD2 also raises questions around card on file that need to be clarified. For example, when a merchant is holding a card on file the interpretation is that SCA would be applied whenever a transaction is made. Even though the transactions are coming from the same card, SCA will be needed every time. Such a situation would add friction to the process and contradict the main reason that a consumer would let a merchant store their card details online, namely ease of payment. Meanwhile, how will the directive handle e-wallets, which are growing in popularity? In these cases, it would be up to the merchant to initiate SCA – as with a card on file situation – which again could be problematic for the customer experience.

TRUSTED BENEFICIARIES

A further possible exemption for SCA is for those merchants that are absolutely trusted by customers. With cards left on file where all the buyer's details are installed, it's a very simple process to make a purchase and allows consumers to complete the buying process without distraction. This in turn can help boost growth and adoption for the merchant's services.

Industry preference[4] is that issuers have a whitelist of trusted beneficiaries – the companies that would not be required to use SCA. The problem lies within the lack of agreed mechanism as to how companies can be treated as trusted beneficiaries. As Gaynor points out: "The idea of trusted beneficiaries is that the consumer can say that they don't want to have SCA – they can opt out because they trust the company-but the difficulty arises when they do this. The problem is that there isn't an agreed, standard mechanism yet as to how the merchant can flag this with their issuing bank."

ADDING AN OPT-IN

One option would be that when a consumer is completing an initial transaction, there is a tick-box, giving the consumer the choice to flag to the issuer that they consider the merchant as a trusted beneficiary. With this opt-in process, each issuer can then build a whitelist of trusted beneficiaries for every consumer.

There are some challenges though. Many companies have various subsidiaries and different branches – a company's UK office may be an entirely different legal entity to its German one, for example. How does an issuer create a whitelist that handles all these different firms? Does a list include the parent company – and, by extension, all the others? There are many clarifications needed.

Notes:
[3] European Banking Authority. 'Consultation on RTS specifying the requirements on strong customer authentication and common and secure communication under PSD2.' Available at: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2?p_p_auth=JWETWh5R&p_p_id=169&p_p_lifecycle=0&p_p_state=maximized&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=2&_169_struts_action=%2Fdynamic_data_list_display%2Fview_record&_169_recordId=1617934. Accessed February 2018.
[4] UK Authentication Steering Group, 11th January 2018

TRANSACTION RISK ANALYSIS (TRA) – IMPLEMENTATION ISSUES

There is another option available for merchants that are wishing to limit the amount of SCA requests from customers. If a merchant (or more accurately, its acquiring bank) has a sufficiently "good" fraud rate, they can use transaction risk analysis (TRA) instead of SCA. This involves examining a variety of factors and determining whether a transaction is fraudulent. Says Gaynor: "Typically this analysis takes in a lot of different elements: geo-location, previous patterns of expenditure; more or less anything that could be interpreted as part of risk." On the back of the TRA, the merchant/acquirer can then claim an exemption to the need to challenge with SCA.

WHAT IS FRAUD RATE?

Fraud rate is defined as the total value of unauthorised and fraudulent remote card transactions, divided by total value of all remote card transactions

WHAT IS A 'GOOD' FRAUD RATE?

If an acquirer has a fraud rate of lower than 13 basis points (bps), they could use TRA for transactions for up to €100

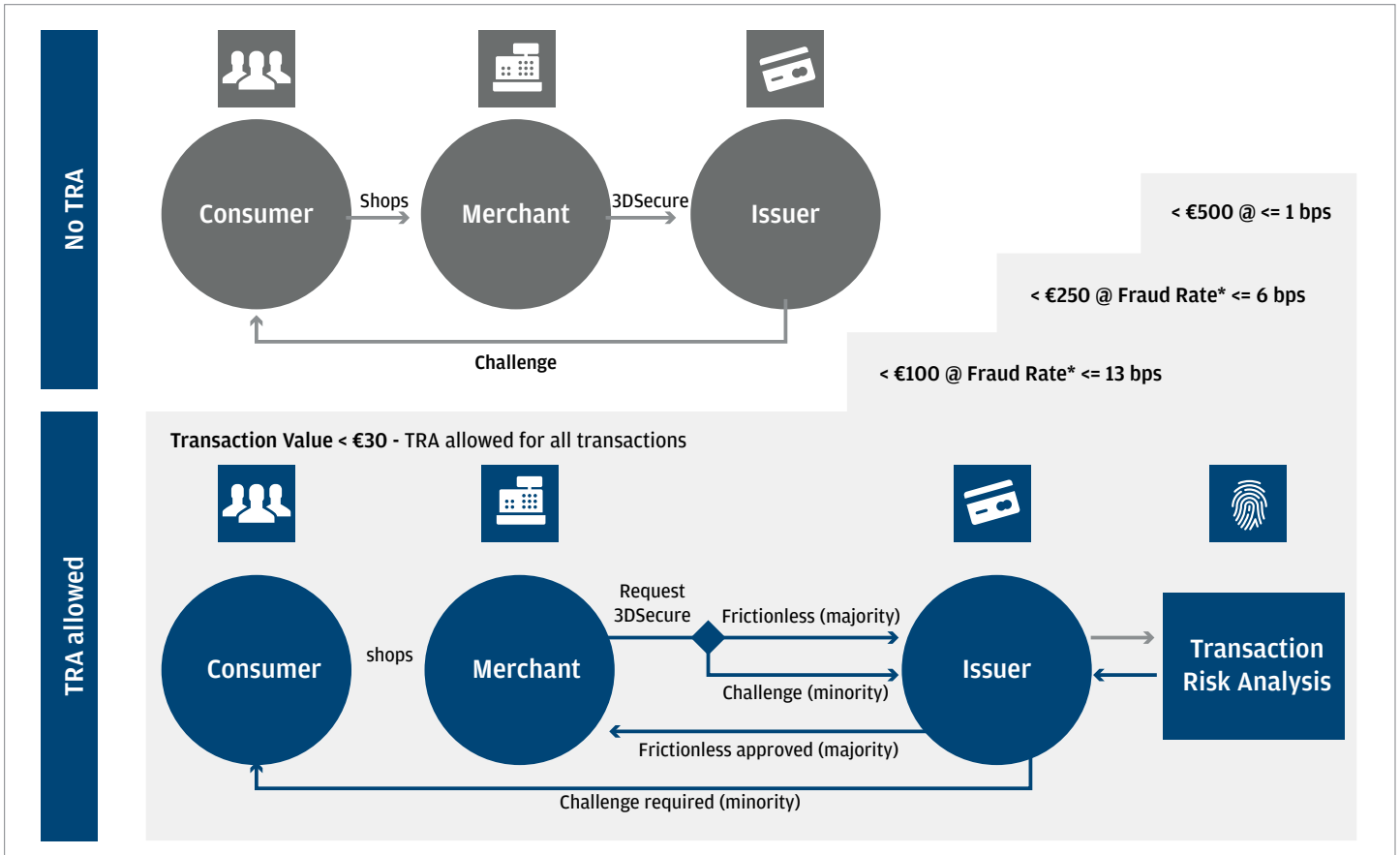
In essence, TRA comes into play when a merchant is sufficiently happy with a consumer's transaction history and other variables and so is confident there is no fraud. However, even though the merchant's acquirer can claim the exemption for TRA, it is the issuer that has the final decision and can turn down the request and demand SCA.

BALANCING SECURITY AND CUSTOMER EXPERIENCE

TRA should allow merchants to provide a better buying experience for the consumer, without compromising their security. One clear response has yet to be formulated by all stakeholders. Different issuers have varying levels of acceptable TRA coming from the acquirer; some will be more risk averse, repeatedly turning down the TRA exemption. There may also be variations from country to country. Meanwhile, certain industries are known to be riskier, adding further complexity.

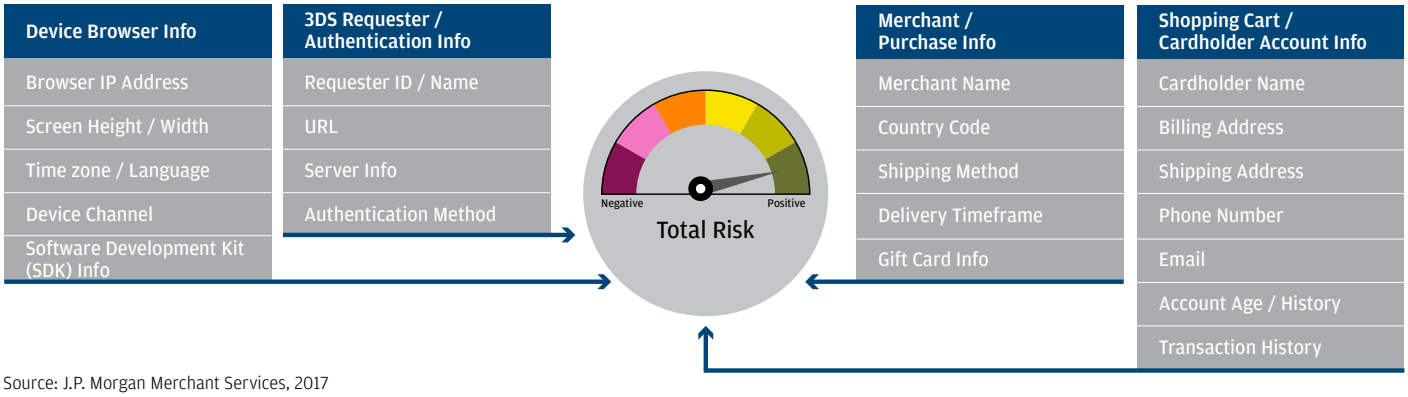
The fraud rate of the acquirer is crucial in determining whether TRA can be used instead of SCA. If an acquirer has a poor fraud rate, then they will have to use SCA for all transactions. In contrast, if an acquirer has a fraud rate of lower than 13 basis points (bps), they could use TRA for transactions up to €100. It is hoped that this will spur acquirers to improve their fraud rates so they can offer a more frictionless experience for customers.

TRANSACTION RISK ANALYSIS (TRA) ECOSYSTEM



*Reference Fraud Rates for Remote Card Transactions per Payment Services Provider
Source: J.P. Morgan Merchant Services, 2017

Risk-based user authentication



Source: J.P. Morgan Merchant Services, 2017

LIABILITY REMAINS A KEY QUESTION

Ambiguities exist around the crucial question of liability, and the UK Authentication Steering Group[5] has asked for further clarification of this issue. Under the current guidelines, if a consumer passes a 3D-Secure (3DS) challenge, then the liability for that consumer's transaction passes to the issuer, and it is their fraud rate that will be penalised in the event of a transgression. This is because 3DS is a form of SCA that is created and primarily implemented by card schemes. On the other hand, when a TRA exemption is claimed, the liability for the transaction remains with the acquirer, and it is their fraud rate that is at risk.

J.P. Morgan agrees with these principles surrounding liability but has requested greater definition and use-cases to aid with implementation. We also support the idea that a merchant's fraud rate should be based on the aggregate fraud rate of their acquirer's entire portfolio. This is positive for the industry as it means that the acquirer has to closely police all of the merchants it works with, as any fraudulent transactions will impact its overall fraud rate.

This aggregated fraud rate could have an impact on marketing. While rates will be hidden from the general public, acquirers may use these as a selling point for merchants, who will want to use the more secure acquirers for their transactions.

CONCLUSION

The key with all interpretations of SCA is to find the right balance between protecting the consumer, without impacting the seamless ecommerce market. Clarifications from the regulators will be important to ensure that balance. How PSD2 is eventually implemented is yet to be seen but there is likely to be some divergence between markets in Europe. As J.P. Morgan's Gaynor states, "there are always going to be different interpretations of regulations in different countries. The ultimate goal of this European Union (EU) regulation is to promote increased competition and innovation, so it will be interesting to see if PSD2 can achieve this in the coming years. What is clear is that it will take close co-operation between the many different stakeholders in the payment sector to make the regulation a success both for the industry and consumers".

NEXT STEPS FOR MERCHANTS

- Plan for 3D Secure
- Evaluate your fraud rates
- Question if you need to implement TRA
- Understand your exemptions
- Contact your J.P. Morgan representative for further details

[5] 11th January 2018

IC19-372 04/19