www.pseconsulting.com
+44 (0) 20 3771 8520

Blog
By Chris Jones
14th March 2016

Does the EBA's risk based approach to Strong Customer Authentication destroy frictionless card payments?

There has been a flurry of excitement since the publication of the EBA's draft Regulatory Technical Standards (RTS) on 23rd February 2017. While there is much to consider within its 153 pages, the focus of this blog is on Article 16 and the new Transaction Risk Analysis approach to exempting transactions from Strong Customer Authentication (SCA). Specifically, we are seeking to assess whether the Reference Fraud Rates levels are realistic in the current European card payments landscape. Such an assessment is vital for merchants and their acquirers who are seeking to opt out of SCA and retain the frictionless check-out experience for customers.

Before getting to the detail of the fraud level analysis, it is worth reiterating the basis of the EBA's new risk based approach. The most significant change, introduced by PSD2, is that all transactions must apply SCA unless they qualify for a narrow set of exemptions set out in the RTS. Elsewhere in the document there are exemptions for value, trusted beneficiaries, recurring transactions with the same value and payee etc., but here we are concerned with the risk based exemption defined in Article 16 where the "transaction [is] identified by the payment service provider (PSP) as posing a low risk" based on their transaction monitoring mechanisms. It is a bold approach for a regulatory body to micro-manage the payments industry to this degree and there is a sliding scale of exemptions based on each PSP's ability to achieve fraud levels below those defined in the following table:

SCA Exemption Threshold Value	Reference Fraud Rates	
	Remote Card-Based Payments	Credit Transfers
€500 or below	0.01%	0.005%
€250 or below	0.06%	0.01%
€100 or below	0.13%	0.015%

By way of illustration, if a PSP has a fraud level of 0.2% they cannot exempt transactions from SCA beyond the standard €30 limit (Article 15). If a payment provider could reduce its fraud levels to 0.05% then they could choose to exempt transactions up to €250 which would be the vast majority of volume for most PSPs. At this stage it is worth emphasising that only a PSP (either an issuer or acquirer) can exempt a transaction, not the payer or payee (Comment 53). This contrasts with the current approach where merchants decide whether to opt in to the issuer authentication and liability shift services offered by card schemes.

So far so good. Most people within the payments industry have applauded the introduction of a risk based approach in the draft text. The use of fraud levels seems to be an appropriate method of objectively testing risk. The devil is, as they say, in the detail, and it is this detail that is explored further below.

Fraud Scope Definition

The first question is "how does the EBA define fraud?". Article 16(d) uses the following definition "the total value of unauthorised or fraudulent remote transactions … divided by the total value of all remote transactions for the same payment instrument, whether authenticated [using SCA] or under any relevant exemption on a rolling quarterly basis". To this we also need to add two important components:

- *Comment 46* which states that "mail order and telephone orders (MOTO) are out of scope of the principles of SCA and therefore not subject to the RTS requirements".
- *Comment 55* which states that transactions by EEA users with merchants outside the EEA, and transactions by non-EEA users with EEA merchants are also out of scope.

What we are left with, therefore, are domestic and intra-EEA eCommerce remote transactions, which is a substantial subset of the total remote transaction base mentioned in Article 16. In the UK, for example, 33% of remote card transactions are MOTO, and typically have higher fraud levels.

Current Fraud Levels

Having reviewed the definition, we must now assess if the proposed thresholds are realistic given current fraud levels in the card industry. We will use a UK example again as relevant data is available in the public domain. At first glance, the top-level figures quoted by organisations such as Financial Fraud Action UK (FFA) are in line. Although in 2015 this figure was 0.08%, the definition used by the FFA includes all remote transactions (including MOTO) as a share of all card transactions (including face to face). When we strip out MOTO and face to face transactions, the figure rises to around 0.12% (again using FFA figures). This levels gets the average UK PSP to just below the first 0.13% level defined by the EBA and would enable transactions under €100 to be exempt. However, this analysis still contains out of scope non-EEA transactions, which are not split out in public domain data. Excluding these, typically riskier transactions, should reduce overall fraud levels further, making the thresholds more achievable.

PSP Requirements to Apply Exemptions

Before we get too excited, there are still a number of requirements which PSPs need to implement in order to offer the above exemptions:

1. **Real time fraud monitoring** needs to be implemented (Article 16(b)). This is in addition to Article 2 which mandates that all PSPs must carry out some form of transaction monitoring
2. **Fraud audits and reports** need to be developed and available to the relevant competent authority. (Article 16(e))
3. **Fraud calculation approach documentation** needs to be made available to the relevant competent authority (Article 16(f))
4. **Notification** to the competent authority is required if a PSP intends to use this exemption (Article 16(g)). In addition, if a PSP's fraud levels rise above the €100, 0.13% hurdle rate for two consecutive quarters they cannot use the exemption, and must alert the competent authority.

Acquirers have two further considerations if they wish to offer Article 16's exemptions to merchants:

1. Transactions are likely to be covered by the liability shift principles laid out in Article 74(2) where the acquirer is responsible for transaction losses where no SCA was applied. These are broadly in line with the current liability shift principles embodied by card scheme rules where transactions are not issuer authenticated. The main difference being that only the acquirer can exempt transactions from SCA not the merchant.
2. There are circumstances where the issuer may still seek apply SCA where it has identified a "materially increased risk of fraud" (Comment 85, Article 18(5)). In this case the transaction is

likely to be declined (ideally providing the appropriate decline code) and the merchant would need to re-try. Given the poor customer experience this generates, one would hope this would occur rarely. The possibility of this outcome means acquirers should inform merchants that exempt transactions may require re-try with SCA.

So, is the EBA's approach to risk based exemptions to SCA fair and appropriate? At this stage, the answer appears to be yes, just. The rules are very tough, given where the industry and merchant practice is at present. Many PSPs will need to invest to drive their fraud levels below the €100 threshold, particularly through investments in real time fraud monitoring. Despite this, Article 16 also creates opportunities for acquirers to offer new risk based SCA exemption services to merchants. If the industry can meet these requirements, and reduce current fraud levels, Europe can look forward to retaining many of the benefits of frictionless payments that we enjoy today.

For more discussion on topics related to the PSD2, SCA, and account access from players such as Adyen, Bambora, Bird & Bird LLP, Compliancy Services, Mastercard, PayPlug, Pay360, SafeCharge, and Walker Morris please come along to our conference. More details are available here.