Image: mattjeacock / iStock / Getty Images Plus / Getty Images

Chris James Consultant Solicitor
mail@chrisjames.me.uk

Confusion and consternation over the EBA's Regulatory Technical Standards on strong customer authentication

The EU's Second Payment Services Directive ('PSD2') requires merchants to put into place what it terms 'strong customer authentication' to help reduce payment fraud. Under PSD2 the European Banking Authority ('EBA') is mandated to produce, *inter alia*, Regulatory Technical Standards ('RTS') specifying the requirements on strong customer authentication and common and secure communication under PSD2, and the EBA has duly released a draft of such RTS. All of this is relevant for e-commerce retailers, as while strong customer authentication plays a role in fighting fraud, burdensome requirements when making payments could put consumers off buying goods on a retailer's website. Chris James, a Consultant Solicitor, analyses the EBA's draft RTS on this issue and the industry reaction so far, and what this all means for e-commerce retailers.

Occasionally this author forgets his wallet when shopping. Of course, retailers' staff are typically far too polite to allow me to put my shopping back on the shelves, and I end up abandoning my basket at the till. I'm a little better at online shopping but that's not to say that I have never started an order never to complete it. No hassle for me, and no-one must put those goods back on the shelves. At scale, though, and considering the investment needed to attract and convert customers online, abandoned e-commerce baskets continue to be a major headache for e-commerce retailers.

Baskets abandoned - security to blame?

Market research provider Baymard Institute cites an average documented online shopping basket abandonment rate of over 69%[1]. The reasons given for abandoning shopping baskets are several, but this article is specifically concerned with the subject of e-commerce payment security. According to payment processor Worldpay's Global Online Shopper 2014 report, up to 18% of online shoppers leave without checking out due to 'excessive payment security checks[2].' That statistic tells only half the story.

According to the same survey, a broadly equivalent number of baskets are abandoned due to the user's nervousness over the perceived lack of payment security of the website[3].

So, for every user who is frustrated by having to complete an onerous checkout process, there's another who is grateful for the additional protection against having their card details pilfered. This ambivalent attitude to payment security is shared by retailers themselves:

- Mindful of chargebacks on fraudulent transactions it would be a particularly cavalier seller to oppose a measure that reduces fraud. Retailers are also conscious of customer perception: 'Maintaining the trust and confidence of their customers is of paramount importance to all retailers' says the British Retail Consortium[4].
- In practice, however, the desire to become an online fortress is tempered by the commercial imperative not to unreasonably impact on end user convenience, and thus sales (or 'conversion') rates. By way of example, take the anti-fraud measure 3D Secure, which powers Verified by Visa and MasterCard SecureCode. It's unpopular, often criticised for being a 'conversion killer.' Anyone who has used it can understand why. Shoppers are unsure of its value (a later report from Worldpay states that '58% of online shoppers feel that their payments are secure online but 56% believe that extra security checks like Verified by Visa and MasterCard SecureCode are necessary[5]'), and some retailers positively hate it. This is especially the case for those who need a light-touch sales process that does not distract the user from consuming the services for which they are paying: for example gaming companies.

Big data: a better way?

Many in industry argue that the increasing use of big data analytics offers a more sophisticated and less intrusive approach to reducing payment fraud than asking the consumer to jump through hoops. The ability to capture and process data from multiple different sources - the retailer, the payment network, the payment service provider, the card issuer and a whole host of value-added data providers such as the mobile telcos - is driving the development of the next generation of anti-fraud measures, many of which are invisible to the end user.

Market research provider Baymard Institute cites an average documented online shopping basket abandonment rate of over 69%.

As the European payment industry organisation Vendorcom puts it: "Initial adoption of 3D Secure by both merchant and consumer alike was poor; shopping cart abandonment where 3D Secure was implemented soared; merchants with 3D Secure chose to turn it off at peak seasonal periods (e.g. Christmas) to avoid cart abandonment. What we then saw was a steady evolution where, based on solid behavioural profiling, 3D Secure was only required when consumers were initiating a transaction outside of their normal span of behaviour. The blanket application of 3D Secure has now all but disappeared from the consumer experience as merchants and acquirers alike have chosen to implement a more risk-based approach, authenticating customers in the background and thus achieving a commercially sensible balance between mitigating risk and ensuring a low friction consumer experience[6]."

PSD2 and strong customer authentication

Vendorcom made that statement in response to the EBA consultation on its proposed RTS 'specifying the requirements of strong customer authentication and common and secure communication under PSD2.'

PSD2 is, as the name suggests, the EU's second attempt at harmonising payment services across the Union. PSD2 governs payments and payment security, and in particular, it calls for 'strong customer authentication.' This is defined as follows: '"strong customer authentication" means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.' (Art 4(3) PSD2).

The requirement to apply strong customer authentication is far-reaching. Article 97(1) of PSD2 requires strong customer authentication where 'the payer:

- (a) accesses its payment account online;
- (b) initiates an electronic payment transaction;
- (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.'

In short, PSD2 requires two-factor authentication, perhaps of the type consumers are already used to when logging into their online account, for most other payment account interaction, including making payments.

Recognising the complexity of implementing these requirements in a diverse payments ecosphere, and agreeing with the industry that certain low-risk activities can be exempted (see Recital 96 PSD2), PSD2 delegates the obligation to create RTS on the EBA (Article 98(1) PSD2) to flesh out the details.

The EBA's RTS

The EBA has dutifully obliged, and put its draft RTS out to consultation in August 2016[7]. Cue a deluge of industry responses, which - with respect to strong customer authentication - tend towards two broad themes:

1. practical implementation: along the lines of "this is all very complex; we don't understand how to implement these RTS"; and
2. along the lines of with regard to the exceptions, where do these RTS permit a 'risk based approach?'

This article will take each theme in turn.

Practical implementation

A short overview of how the EBA proposes strong customer authentication to work is as follows:-

1. A transaction-unique 'authentication code' must be generated (Art 1 RTS) for any required application of strong customer authentication.
2. The authentication code is generated from inputs including 'a valid combination of authentication elements, i.e. based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others' (paragraph 22(b) of the consultation).
3. That authentication code 'shall be characterized by security features including, but not limited to, algorithm specifications, length, information entropy and expiration time,' with certain additional requirements that the code must meet, including that 'no information on any of the elements of strong customer authentication categorized as knowledge, possession and inherence can be derived from the disclosure of the authentication code.' (Art 1(2) RTS).
4. There are several specific technical requirements to the authentication procedure, including a 'time out,' 'maximum number [...] of attempts,' data encryption and systematic fraud detection including 'parameterised rules' (e.g. blacklisting, profiling).
5. There are specific requirements in respect of dynamic transaction linking (Art 2 RTS), and in respect of each of the authentication elements (knowledge, Art 3 RTS; possession, Art 4 RTS and inherence, Art 5 RTS), as well as additional rules around independence of those elements (Art 6 RTS).

An interesting aspect, and one which evidences the difficulty the industry faces in putting these RTS into practice, is that the requirements in respect of knowledge and possession require 'mitigation measures' to prevent unauthorised disclosure (Art 3(2) RTS) and unauthorised replication (Art 4(2) RTS) respectively.

Remember that strong customer authentication applies even to the initiation of a payment remotely, not merely direct account access, and so any implementation needs to be pragmatic.

The required extent of these mitigation measures is not clear. For example, what about the use of SMS to establish a factor?

In other contexts, where two-factor authentication is used, short numeric codes sent by SMS are commonly employed to 'prove' possession of a particular mobile device. SMS is an insecure, plain text medium that is vulnerable to interception, a problem that is not straightforward to mitigate, at least technically. The use of SMS, despite this flaw, is founded on the basis that two-factor authentication reduces the risk of compromise of any single factor, and so this risk is acceptable.

The RTS do not appear to acknowledge this idea; it is not clear whether this is intentional. Arguably, more modern 'push messaging' allows for a fully encrypted substitute to SMS to be deployed; the RTS may be seen to be encouraging this practice instead. Of course, this solution is only suitable for users who have a device that will support it; and there are many users who may not use a smartphone or who may use an unsupported smartphone.

Remember that strong customer authentication applies even to the initiation of a payment remotely, not merely direct account access, and so any implementation needs to be pragmatic. Any payment institution (e.g. a card issuer) that takes a conservative, clunky, approach to the implementation of strong customer authentication is likely to invoke the ire of retailers and acquirers, who are likely to see a drop in completed transactions. Will PSD2 become the new 'conversion killer'?

Risk based approach

Further, it's not enough for strong customer authentication to be provided only by the issuing payment institution. The technical implementation of strong customer authentication needs to be supported by every participant in the payment cycle. A simple four-party card acquiring relationship will involve the cardholder, the cardholder's issuer, the merchant, and the merchant's acquirer.

To avoid the 'conversion killer' problem, the merchant's acquirer (the 'payee's PSP' in PSD2-speak) has every interest in applying the same 'risk based approach' as taken with 3D Secure - noted above.

In its consultation, the EBA stated that: "the EBA understands that Article 74(2) of PSD2, which allows the payee or the payee's PSP the option not to accept [strong customer authentication], only applies during the short-time transitional period between the application date of PSD2 (13 January 2018) and the application date of the RTS under consultation (in October 2018 [at] the earliest). During this transitional period, 'where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider.'" (Consultation, op. cit.)

So, the EBA is of the opinion that a risk-based approach is out, unless it complies with the RTS. This opinion has drawn robust responses. For example, the European Payments Council replied: "We do not perceive the legal basis authorising the EBA to state that Article 74(2) of the PSD2 would only apply during a transitional period. Art. 74(2) is in no way time bound, or limited, as suggested by EBA [...] There is no language within PSD2 to support this proposition that Art. 74 (2) is made redundant by EBA excluding any risk elements from the draft RTS. As we believe that such risk based analysis and exclusions are clearly contemplated, and required, under the mandate provided at Art. 98, by failing, or refusing, to cater for risk, we believe the EBA has exceeded that mandate[8]."

Several other respondents comment that the exemptions defined in the RTS are too narrow, arguing that:

- the threshold below which strong customer authentication need not apply (according to Article 98(3)(b) of PSD2) is set too low (€10 per transaction, up to a cumulative €100 limit since the last application of secure consumer authentication, Art 8(2)(d) RTS);
- that the cumulative limit is difficult to implement across different acquirers and payment channels which - for example - may not be able to report transaction amounts in real-time; and
- by imposing strict monetary thresholds, the RTS do not give sufficient weight to limb (a) of Article 98(3) PSD2, which permits exemptions according to 'the level of risk involved in the service provided.' E.g. is online grocery shopping likely to see fraud rates as high as those for online gaming?

The EBA might counter that, if payment credentials are stolen, the risk profile of the service that they were stolen from is rather less relevant than the ability to re-use those credentials elsewhere. Protecting the retailer whilst preserving its conversion rates is only one part of the bargain; consumer protection is equally important.

Further, the EBA should be commended for daring to deliver forward looking and technically intricate rules, acknowledging that technical concepts such as 'information entropy' play a role in reducing fraud.

At the time of writing, the EBA is considering responses to its consultation. As Harriet Russell of the FinTech practice of Paul Hastings (Europe) LLP put it: "The EBA's response to the concerns raised in the consultation is keenly anticipated." Confusion abounds in the industry, and it's likely that the final adoption of the RTS will be delayed as the EBA seeks to clarify its work. Here's hoping that the final version injects a healthy dose of pragmatism into this controversial subject.

1. http://baymard.com/lists/cart-abandonment-rate
2. http://bit.ly/2ksOWLa
3. Ibid.
4. https://www.ft.com/content/e656b098-00c3-11e6-99cb-83242733f755
5. See: http://bit.ly/2ksMioC
6. http://bit.ly/2jlVrxG
7. http://bit.ly/2eemEB5
8. http://bit.ly/2jYlUCo