THE UKCARDS ASSOCIATION

==========

EBA Consultation Paper on Implementation of Guidelines on Security of Internet Payments

Response from The UK Cards Association
(*For Plenary Review*)

14 November 2014

==========

Author: Duncan McEwen

THE UKCARDS ASSOCIATION

1. Background:

On 20 October 2014, the EBA published a *"Consultation Paper on the Implementation of draft EBA Guidelines on the Security of Internet Payments prior to the Transposition of the Revised PSD2"*, inviting comments to the proposals as put forward on the specific question as is detailed below. The consultation runs until **14 November 2014**.

The EBA document states that comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

2. Details Submitter:

Your Name: Duncan McEwen

Your Organisation: The UK Cards Association

3. Consultation Question:

Question: Do you prefer for the EBA Guidelines a) to enter into force, as consulted, on 1 August 2015 with the substance set out in this consultation paper, which means they would apply during a transitional period until stronger requirements enter into force at a later date under PSD 2 (i.e. a two-step approach); or b) to anticipate these stronger PSD2 requirements and include them in the final Guidelines under PSD 1 that enter into force on 1 August 2015, the substance of which would then continue to apply under PSD 2 (i.e. a one-step approach).
Answer (a) or (b) including justification): The UK Cards Association ('UK Cards') preferred starting point based on the two options presented, would be to pursue option (a) as part of a *'two-step approach*' going forward. Based on the simple premise that it would be non-sensical and unsatisfactory in trying to pre-empt or anticipate the final outcome of the PSD 2 negotiations as they currently stand. We would instead align any implementation period to what the Payments Council has proposed; awaiting finalisation of the PSD 2 text and then review of the SecuRe Pay recommendations against these new requirements, before issuing draft guildines and/or technical standards allowing for a longer period of implementation. More generally, UK Cards has repeatedly asserted its concerns in previous responses at the EBA and ECB's overly prescriptive approach; demonstrated once more by reference to the supporting draft guidelines which we believe will likely hinder innovation rather than support it. UK Cards has commonly stated that a better policy would be to work towards guidance being based on a set of achievable outcomes rather than through prescribed sets of rules.

4. **Response Template**

N°	Issue	Comment	Reasoning
1	General	Amendment	We believe the proposed guidelines will stifle innovation rather than encourage it, and is fundamentally based on a consultation process through one preferred viewpoint (i.e. the banking industry) and supported by an outdated mode of thinking; to where the direction of technological security solutions are now moving. It should not be forgotten that the *SecuRe Pay Recommendations* are based on a consultation process that began in circa. 2010. A missed 'generation' in technological terms which in many ways has failed to move with the times. UK Cards has consistently asserted that a better policy would be to adopt a framework that tries to articulate a broad set of overarching outcomes (e.g. the principle of strong authentication) which all industry players can adhere to, but be supported with underlying guidance of how this objective might be achieved. Thereby, leaving it to the market (*i.e. issuers, banks, PSPs etc*) to have the freedom to innovate by adhering to a stated outcome based on what new technologies might potentially be available (e.g. use of geo-location, device biometrics) coupled with customer verification and the full range of behavioural tests that could be applied. This could offer an equally strong set of authentication practices in addition to the customary and historical *two-factor* model. UK Cards belief is such an approach would avoid the unwanted effect of the market being told *'what to do'* based on an imposed set of requirements forced upon it. Rather than having a supported outcome that the market can adhere to but also be given the freedom to find alternate ways to achieve that 'end'; creating the underlying conditions and a regulatory environment that is supportive of innovation. UK Cards fear is that by adopting an entrenched position, built around a regulatory framework that is based on a prescribed set of rules (with strict and outdated definitions being written into legislation) will go to undermine the wider socio-economic benefits and opportunities that an increased digitalised payments age might offer to all parties. And support

			the clear objective the ECB is attempting to facilitate (e.g. an increase in cross-border payments across all payment channels). A similar shortcoming is the ECB and EBA's demarcation in treating the internet and mobile payments as something distinct and separate. With each having to conform to separate requirements based on whatever mobile device has been chosen or is in use. Instead it would make more sense for issuers, PSPs etc to undertake a risk-based assessment that considers 'digital' in the round, and across the full suite of channels made available, as part of a more holistic evaluation. UK Cards would urge both these forum groups to take notice of the regulatory developments that have been witnessed in some of the more developed and advanced e-commerce markets in recent years (e.g. UK) and to begin replicating those regulatory trends that are currently in situ. A good example is with the FCA's *'Project Innovate'* initiative, which is introducing a regulatory model purposefully designed to foster innovation; that is both flexible in design and sympathetic in identifying policies and processes that can change as the technology changes and innovative business models emerge. It provides a clear endorsement and move away from the tired model in having a prescribed *'one-size-fits-all'* and static regulatory approach which has proven ill-equipped to cope with the ways that commerce is now changing. Most notably because of the increasing digital demands being made by consumers and how their own individual payment behaviours are evolving. Such an approach would better cater for the 'level playing field' that all participants want and should be adhering to; avoiding the effects and pitfalls of 'disproportionality' which is arguably a natural bye-product of poorly thought-out regulation. There is a very real danger that the ambiguity surrounding the strengthening authentication requirements for payment transactions with the continued uncertainty as to the final requirements likely to be incorporated into the final PSD 2 text, could cause the 'uneven' yet mandated regulatory framework that UK Cards and its members are fearful of.

2	General	Amendment	A central pillar of the proposed guidelines is the requirement for strong customer authentication. Obviously, this is an inherent feature for any credible payments process to securely protect access to sensitive payment data. Balancing the subtle practicalities between achieving sufficient levels of security yet off-setting this against acceptable customer convenience. In the last two decades many security solutions have been implemented, only to be rendered obsolete as technology has evolved, and been replaced with 'safer' and updated solutions. Similarly, authentication solutions have evolved, as new threats have appeared and the preferred platform for internet payments has changed from PCs to mobile devices. The fundamental point is that as a specialist field it is an area that has proven itself as highly dynamic and fast changing. As an example (pursuant to the issuance of the SecurePay Recommendations) has been in the way tokenization has developed as one of the prevalent security solutions in any future e-payments system. Similarly, the future role of biometrics is another evolving area coupled with the evolution in digital security being based on *'risk-based authentication'* practices, all of which might be hindered by the current requirements in their prescribed form. UK Cards would therefore urge that these new developments are taken into account when finalising the guidelines; coupled with an appreciation that any strict definition prescribed in legislation is likely to become quickly outdated, as new security solutions are developed and adopted into the retail payments environment. The aim of fostering the establishment of a harmonised and EU/EEA-wide minimum level of security' is not the answer to what is undoubtedly a global issue. For any security measures to be effective they need to be implemented globally and by all parties as part of an emerging digital payments ecosystem.