MIDAS Alliance response to EBA request for information regarding Payment Service Directive 2.

This document represents the summary response of the MIDAS Alliance to the consultation, following on from a roundtable discussion on the EBA request for information exercise held in London on the 3rd February. Ten organisations, including established banks, new entrants, and other payment service industry, were represented but this document should not be taken to represent the views of any of the organisations so represented, rather the summary of discussion from the perspective of the MIDAS Alliance.

1. With respect to Article 97(1) (c), are there any additional examples of transactions or actions implying a risk of payment fraud or other abuses that would need to be considered for the RTS? If so, please give details and explain the risks involved.

Not withstanding the view that it should be a business risk decision as to the levels of security (whether identity, authentication, communications) to be adopted in any given circumstance, there are a range of non-payment transactions and actions that can imply a risk of subsequent payment fraud if lower levels of authentication were to be deemed acceptable.

For example any request for a change of address, phone number or other personal details has a high degree of risk to subsequent payment fraud. Equally any access to information on activity on an account, whether such access itself were to allow a transaction or not, causes an increased risk of subsequent payment fraud through misrepresentation.

With reference to links to eIDAS it should also be noted that a range of security issues arise over the use of '£0 transactions' where the level of risk associated with allowing a weaker form of authentication is in no way associated with £0 in a linear value risk assessment.

Given the consultation's consideration of additional services, beyond traditional payment service providers, it was also believed that strong authentication requirements should be considered for other categories of intermediary, for example professional services such as accountancy, stockbroking etcetera, where an agent may be carrying out a payment transaction using strong authentication on behalf of their client on the basis of weak authentication.

2. Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can

be ensured that these data can only be controlled by the PSU?

As noted in the EBA's own SecuRe Pay definitions of strong authentication, applications of multi-factor security should not be capable of 'being surreptiously stolen over the internet'. This would suggest that the reliance on data generated by a physical token, such as a One Time Password, is not in itself adequate in this context. The roundtable discussed the scenario of relying on a passport as an identity document within the context of strong customer authentication. Given that there is no such thing as 100% security, and therefore businesses must make a risk based decision on the levels of authentication to use in any given circumstance, it was believed that there were a variety of levels with which a single possession element could manifest itself when in data form:

1) Passport number – easily replicated from memory;
2) Copy of passport – static file, too readily accessed from other use cases;
3) Time-stamped notarized copy of passport;
4) Video of passport being in possession;
5) Biometric check with passport issuing authority that passport image matches that originally enrolled;

Each level clearly increases the difficulty for an attacker to intercept and misrepresent the 'data' for their own purposes, though ultimately a man in the browser style attack may still be possible. That having been said, the theoretical possibility of interception should not be taken as suggesting that such security techniques should not be deployed as part of a layered defence.

3. Do you consider that in the context of "inherence" elements, behaviour-based characteristics are appropriate to be used in the context of strong customer authentication? If so, can you specify under which conditions?

Where our "inherence" elements relate to biometrics, it is possible that certain Behaviour based "biometric" characteristics could be appropriate in certain circumstances. Behavioural biometrics such as gait, typing style, dynamic signatures, and some (though not all) models of voice biometrics have been demonstrated that can have value in a strong authentication application. See also British Standards Institution Publicly Available Specification 92 (published 2012).

4. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to the independence of the authentication elements used (e.g. for mobile devices)?

There is a clear issue on the independence of authentication elements using mobile, where the biometric or knowledge based factor is only verified by the possessed factor, in particular when the additional factor exists in the assumed case of a mobile. Additional factors of authentication cannot be considered to be truly additional factors when the compromise of such a device can compromise any additional security metrics.

Such systems can add value, however, where the secondary (or tertiary etc) factor

is also communicated (i.e such factors are available centrally, rather than being purely locally assessed).

5. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?

The obvious challenge in managing dynamic linking is in the user experience. In a variety of fora it has been suggested that digital signatures, in the model of the UK CAP reader (also known as PIN Sentry) standard could readily be deployed to digitally sign any given online transaction.

However, the user experience of having to authenticate in such a manner would be almost certain to curtail the use of e-commerce, rendering such an onerous solution to be untenable.

6. In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?

MIDAS Alliance have held a number of wargaming sessions to agree on such a Nirvana, but these have not been readily apparent.

7. Do you consider the clarifications suggested regarding the potential exemptions to strong customer authentication, to be useful?

As noted above, the requirement for strong authentication should be considered sacrosanct, excepting the rare occurrences where a lack of strong authentication in one use case does not potentially weaken the re-use in another capacity.

8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?

The EBA should ensure that any requirements of strong authentication in a payment use case can tally with the wider non-financial use cases envisaged under eIDAS, or similar international interoperability standards (e.g. ICAO)

9. Are there any other criteria or circumstances which the EBA should consider with respect to transaction risks analysis as a complement or alternative to the criteria identified in paragraph 45?

White listing should not be seen as a panacea, as transfers from a strongly authenticated account could syphon off funds to a subsequently less secure environment (for onward re-distribution). The advent of ‘faster’ (effectively instantaneous) payments, renders this to be a highly vulnerable sector.

10. Do you consider the clarification suggested regarding the protection of users personalised security credentials to be useful?

The enrolment of users towards the issuing of personalised security credentials

does not appear to be adequately addressed in the current drafting. Similarly, even where the enrolment has been sufficiently managed, the distribution of credentials, whether physical or virtual, does not appear to adequately address the likely threat vectors at present, let alone those likely to emerge to threaten the payment ecosystem.

11. What other risks with regard to the protection of users' personalised security credentials do you identify?

Where the personalised security credentials are themselves capable of processing data (as with credentials stored on or relying upon mobiles, or other electronic devices) there is a risk of malware compromising the generation of further data. Whilst this should not necessarily rule out such means of managing credentials, such a risk should be borne in mind during the design of a strong authentication procedure.

12. Have you identified innovative solutions for the enrolment process that the EBA should consider which guarantee the confidentiality, integrity and secure transmission (e.g. physical or electronic delivery) of the users' personalised security credentials?

Security at enrolment is of greater concern from an Identity perspective, and hence the parallels with eIDAS developments are likely to be more prevalent in this area. Where anonymous payment services are being considered, or in purely pre-paid circumstances, it is possible that enrolment may entail complete confidentiality, but these are limited by wider KYC/AML concerns.

Enrolment to allow subsequent multi-factor strong authentication would ideally be carried out face to face to ensure no interception or diversion of security credentials, but where this is not practical to enrol at scale, such as for mobile only account opening, dynamic biometric capture, such as via video chat, can offer a greater degree of assurance than reliance on traditional document verification techniques.

13. Can you identify alternatives to certification or evaluation by third parties of technical components or devices hosting payment solutions, to ensure that communication channels and technical components hosting, providing access to or transmitting the personalised security credential are sufficiently resistant to tampering and unauthorized access?

Third party certification may prove to be too onerous a barrier to entry to allow innovative service providers to operate. Third party evaluation in advance of launching such new services, on the other hand, is clearly a logical step prior to the inevitable evaluation by a hostile third party seeking to compromise the system.

14. Can you indicate the segment of the payment chain in which risks to the confidentiality, integrity of users' personalised security credentials are most likely to occur at present and in the foreseeable future?

Weak enrolment controls currently appear to offer the most likely single point of failure, as has been witnessed with the roll out of some mobile payment services. This is likely to remain the case for as long as such processes are permitted to continue, though within the foreseeable future such controls are likely to be ameliorated by recommendations expected to emerge from the development of standards towards eIDAS levels of assurance.

15. For each of the topics identified under paragraph 63 above (a to f), do you consider the clarifications provided to be comprehensive and suitable? If not, why not?

Given the rapidly evolving manner of the threat, it will become essential for all the component parts of the payments ecosystem to evolve to address new challenges. Paragraph 63suggests a number of well-meaning approaches towards such an environment, but does not adequately address any meaningful solution. For a request for information this is, of course, perfectly understandable, but during the course of the standards development phase, this must be more properly addressed.

16. For each agreed clarification suggested above on which you agree, what should they contain in your view in order to achieve an appropriate balance between harmonisation, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?

As per 15, clarifications should emerge through the development of the standards during the course of the year.

17. In your opinion, is there any standards (existing or in development) outlining aspects that could be common and open, which would be especially suitable for the purpose of ensuring secure communications as well as for the appropriate identification of PSPs taking into consideration the privacy dimension?

British Standards Institution, alongside MIDAS Alliance, are in the process of developing a Publicly Available Specification towards the management of Mobile \Identity and Authentication Standards, with a view to addressing the issues raised by both PSD2 and eIDAS.

The timelines of this PAS are likely to be in advance of the EBA requirements later this year, and are intended to be fed into national and international transposition of PSD2 into Member State domestic legislation.

18. How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS)?

The management of additional credentials through AIS/PIS should be seen in the light of the wider requirements associated with eIDAS (qv).

19. Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalised security credentials as well as for common and secure open standards of communication for the purpose of identification, authentication, notification, and information? If yes, please explain how. If no, please explain why.

The inter-relationship between banking and eID credentials are already well documented (e.g. ENISA eID and Banking study, 2010), but the forthcoming classification of eIDAS credentials for inter-operability across all 28 Member States provides an excellent opportunity to align commercial and Governmental applications.

20. Do you think in particular that the use of "qualified trust services" under e-IDAS regulation could address the risks related to the confidentiality, integrity and availability of PSCs between AIS, PIS providers and ASPSPs? If yes, please identify which services and explain how. If no, please explain why.

The degree to which 'qualified trust services', as defined under eIDAS, can adequately be applied as a defence against organised criminals' assault against the payment systems of the EU, is currently an oen question, with much further research necessary before any level of trust can be established.

Much of this further research is already underway, and EBA should look to engage with these research communities of interest to tie in with these, currently largely academic, developments.