14th November 2014

European Banking Authority
Tower 42 (level 18)
25 Old Broad Street
London EC2N 1HQ
United Kingdom

Dear Sir/Madam,

Consultation on Guidelines on Internet Payments Security ("Guidelines")

We thank the European Banking Authority (EBA) for the opportunity to respond to the above consultation.

Background

iSignthis BV is a provider of strong customer authentication solutions, and has already contracted with several Payment Service Providers (PSPs) in order to assist them with meeting their compliance requirements. We anticipate that our first compliant implementation will be no later than February 2015, consistent with the Assessment Guide[1] published by the European Central Bank (ECB) in early 2014.

As a cloud based solution provider, we are in a position to assist PSPs to meet the Strong Customer Authentication requirements of the EBA, including PSPs such as issuers, acquirers and payment integrators, including processors, gateways and technical service providers.

There is an awareness within many PSP's of the 'SecuRE Pay'[2] requirements, but such awareness is not as yet the case with merchants or consumers.

However, it is our view that the proposed requirements of the PSD2 are not well understood within industry at this point in time, particularly as the final text is yet to be agreed by the European Parliament.

Guidelines

Underpinning the Guidelines are the requirements for Strong Customer Authentication, which comprise identifying the customer, and then linking the customer's payment instruments to two-factor authentication.

[1] http://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf
[2] http://www.ecb.eu/press/pr/date/2013/html/pr130131_1.en.html

The draft EBA Guidelines, together with the ECB Assessment Guide, provide a clear set of requirements for PSP's. It is understood from these that any PSP in the payment chain that does not implement Strong Customer Authentication will be considered the 'weakest link', and will therefore be required to suffer the consequences of any fraud by refunding other PSP's.

It is our understanding that the payment schemes, as governance authorities, have yet to foreshadow any changes to their rules to accommodate a liability shift regime, per requirement 7.6.

These rules will have great impact on the operation of the Guidelines in practice, and we would urge the EBA and the Central Banks to require early publication of these rules, including a consultation period.

Whilst the PSD2 and Guidelines are technology neutral, it is in our view crucial that this approach be reflected in the payment scheme rules, which presently reflect use of payment scheme proprietary technologies and interfaces, and arguably restrict competition and technical innovation. Due to the historical influence of the payment schemes and their governing rules the PSP's are potentially misguided in the SecuRE Pay and PSD2 requirements, until such time as the rules are updated to reflect the changing position.

Discussions between iSignthis BV and various PSP's indicate that in some circumstances the PSP's are confused about their compliance status. Presently, to our understanding, no legacy system installed prior to 2014 meets the EBA or EBA requirements.

For example, 3D-Secure is presently implemented in almost all cases as a one-factor (1FA) system, and it will need major enhancements, with associated time and cost impact, to comply to meet the new Guidelines.

Additionally, 3D-Secure is very much Visa and MasterCard centric, and relies upon the issuers taking action first, before an acquiring PSP can meet their compliance obligations. Alternative technologies such as iSignthis allow acquiring side PSP's to meet their compliance requirements independent of issuers, whilst allowing issuers a means to interface with iSignthis enabled PSPs at any time. iSignthis is able to incorporate legacy 1FA 3D-Secure systems as one of the two factors in the iSignthis system.

Assessment

What is unclear is whether the ECB Assessment Guide is intended as self-assessment by PSPs, or, to be used as a benchmark by an independent auditor/assessor.

It is unclear who may act as an assessor, and what their qualifications would need to be. We would propose that the assessment role be performed by a Payment Card Industry (PCI) Qualified Security Assessor (QSA)[3], with specialist training or understanding of the Guidelines, and registration as may be required.

Assuming that a PSP is assessed as compliant, what remains unclear is the means by which the 'refund' will be arbitrated and managed in the case of a non-compliant PSP being required to refund a compliant PSP.

Whilst the Guidelines call for the payment schemes to manage this process, the payment schemes are already potentially conflicted, as they hold multiple roles within the payment chain. The roles of the payment schemes vary and include governance, processing, authentication, consulting and standardization.

In our view, it should not be up to the payment scheme to determine if a PSP meets the requirements of the Guidelines, as that will conflict the payment schemes even further. It is our understanding, from discussions with the ECB, that the European Payments Council (or its successor), could be tasked with managing such a compliance or accreditation scheme, for both PSPs and compliance assessors. We believe that it would be of benefit to the market if the EBA could provide early guidance on this.

Interfaces

The Guidelines place responsibility for implementation on both issuers and acquirers. However, it is acquirers and acquiring side payment integrators that are likely to be impacted most by the Guidelines, as a result of their role in the payment network.

The Guidelines allow issuers, acquirers and payment integrators to implement their choice of Strong Customer Authentication, provided that they 'support technologies allowing the issuer to perform strong authentication'.

[3] https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

As the market develops, a likely scenario is that the issuer, acquirer and payment integrator may have chosen different technologies by which to achieve compliance. A payment integrator, who interfaces with multiple issuers, acquirers and accepts multiple card schemes may be faced with the prospect of needing to implement a host of technologies, which is not practical.

It is our view that the EBA could mandate that a standard interface be defined by an appropriate body to allow for intercommunication between competing strong customer authentication systems, and across the various card schemes. The card scheme proprietary communications are not suitable for this task, as economies of scale and new technologies will likely span multiple card schemes, as is the case with iSignthis.

European or National PSP Register

It appears to be the case that the definition of a PSP has been extended from the PSD1 to include payment integrators such as technical service providers, gateways and processors, many of whom are not presently registered with, or regulated by, the EBA or national regulators. It is unclear if the EBA or the national regulators intend to establish European or national registers of PSP's.

Competition

Whilst competition is not the specific focus of the EBA, it is submitted that the authority should however be mindful of the perils of 'bundling', 'tying' and the dangers of competitive foreclosure. We are strongly of the view that all actors in the payment chain act in a means that is transparent and fair, and not bundle or tie authentication with other services in a manner which is contrary to either Article 101 and/or 102 of the *Treaty on the Functioning of the European Union* and national competition legislation. Indeed, there is strong support in European law for unbundling following *inter alia* decisions in the Microsoft cases and the formulation of specific directives requiring it in the telecommunications sector.

Conclusion

The implementation of Strong Customer Authentication and the 'SecuRE Pay' recommendations are feasible within the August 2015 timeframe, despite some ambiguity regarding implementation as noted above.

We do not believe that the stronger requirements of the PSD2 are sufficiently understood at this point in time.

It is our view that the final EBA guidelines under PSD1 should enter into force, as consulted, on 1 August 2015 with the substance set out in the consultation paper, which means they should apply during a transitional period until stronger requirements enter into force at a later date under PSD 2 (i.e. a two-step approach);

The focus in our view should then be on further enhancing PSP understanding, followed by raising awareness with merchants and consumers of the impact of the August 2015 'SecuRE Pay' compliance date.

We look forward to the outcome of the consultation.

Yours faithfully,

N. Karantzis
iSignthis B.V., Amsterdam