ESBG

EUROPEAN ASSOCIATION OF CO-OPERATIVE BANKS

0460/2017 **21 June 2017**

ESBG - EACB Position Paper

Input to EBA on the Commission's amendment of the draft final Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication

The European savings, co-operative and retail banking community is calling on EBA to reject the amendment proposed by the Commission regarding a fall back to the dedicated interface for TPP access

1. Executive Summary

Via this Position Paper, ESBG and EACB are calling on EBA to reject the amendment proposed by the Commission regarding a fall back to the dedicated interface for TPP access. The European savings and retail banking community is arguing that the Commission's promoted fall back to the dedicated interface for TPP access:

- Ignores the functioning of the online banking architecture, and hence will in most instances never be able to provide a "fall back" functionality;
- Proposes conditions for application (e.g. 30 seconds) in an environment (end-to-end communication over multiple channels with several parties involved) where actual responsibility for malfunction and/or failure is at best very tedious to allocate with certainty;
- Is totally askew with the many resilience and business continuity obligations already placed on and observed by ASPSP sector, under due supervision of their competent authorities;
- Does not assuage any concern with respect to customer protection, privacy, or security, and more generally will not allow ASPSPs to comply with their obligations under the GDPR (in addition, because of the resource burden involved, competent national authorities are very unlikely to effectively monitor TPPs' compliance with the RTS as amended by the Commission);
- Is disproportionate in terms of resources, direct costs, and ancillary costs (including cost of capital) to the objective pursued, notably in the absence of any evidence that ASPSPs are not capable of providing a quality service with respect to the dedicated interface.

In the case that EBA does not fully share the position of ESBG and EACB, the ESBG and EACB are suggesting a compromise proposal to avoid costs for ASPSPs - and in consequence for PSUs - for the maintenance of a fall back interface if not required.

2. Introduction

The European Banking Authority (EBA) released in February 2017 its "Final draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under PSD2" (final draft RTS), which i.a. specify a "dedicated interface" to be made available by account servicing payment service providers (ASPSPs) to account information and payment initiation service providers. ESBG and EACB very much support the philosophy underpinning EBA's approach and the related technical implications, which draw a fair balance between the requirements of PSD2 and the protection of consumer data, privacy, and security. In addition, the costs of building and deploying the interface defined in EBA's final draft RTS are proportionate from the perspective of both payment service users and account servicing payment service providers.

On 26 May the European Commission issued amendments to EBA's final draft. Although the European Commission reconfirms the mandatory use of "dedicated interfaces", it now also opens the door to less secure communications by mandating a fall back option very much akin to screen scraping, allegedly to ensure business continuity, which in fact is one step back. It is now up to the EBA to react to the latest proposals from the European Commission. The European savings, retail and cooperative banks are deeply concerned by the business, operational, and risks and cost issues that the introduction of this fall back poses to the supply and hence demand sides, in the absence of any proper understanding of the online banking environment and its evolution.

3. What the European Commission now requests

As admitted by the European Commission, the use of screen scraping triggers in particular data protection risks. Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) would continue to access all online banking data of the customer, and view the very same data that the customer is able to view when accessing the online banking site himself. This access goes much further than the data that AISPs and PISPs actually need for their services. More importantly, the access generally goes beyond what the customer thinks he has agreed to when making use of the AISP and PISP services.

PSD2 has therefore put in place a framework to contain this risk. It requires that banks put in place a communication channel that allows AISPs and PISPs to access the data that they need in accordance with PSD2, and that requires banks and AISPs and PISPs to identify themselves when accessing these data.

ESBG and EACB welcome the Commission's confirmation of this position, which we have been advocating since the first draft of the RTS. ESBG and EACB reiterated in particular in their joint 15 May 2017 position paper that screen scraping under PSD2 is the wrong answer to consumer privacy and security, and that it jeopardizes, without possible remedy, innovation, certainty, level-playing field,

and proportionality. By introducing the fall back option (or "spare wheel option" as the Commission calls it), the European Commission gives rise to their own concerns again. The fall back option can be considered the same as mandating that a secure vault needs to be equipped with an easy to open security door for cases that the secure front door is not working properly. In addition to this the easy access door is very expensive to install and maintain and will duplicate the access cost for the vault owner. It goes without saying that this is not acceptable and that this is in fact one step back. .

The ESBG and EACB believe that it is not possible to implement screen scraping techniques while at the same time ensuring both that the Third Party Provider (TPP) identifies itself reliably and only the data requested is passed through. Indeed screen scraping (i.e. the browser interface for the user) is defined by the following two characteristics:

1) it has no mechanisms for a TPP to identify itself with a certificate (i.e. only a user with his secret credentials);
2) the screen presented to the user in online banking contains lots of data beyond what is needed for PIS/AIS and beyond what the user has given consent for.

Thus screen scraping and TPP-identification/data-redaction are fundamentally incompatible.

4. Remaining and new issues with the Commission's amendment

Apart from the various risks associated with screen scraping practices, we see the following 13 issues that should matter to all stakeholders in society, especially consumers and policy makers, when screen scraping is allowed as a fall back option.

a) The reality of online banking architecture

The typical technical architecture of a bank consists of a back office, where all data is kept and where operations are performed, and one or multiple front offices that are used to interact with the bank customers and the bank employees. Back offices and front offices are connected with each other via mid-layers. The customer interface, the dedicated interface and the (newly) required (by the Commission) fall back interface are all front offices that are interacting with the same back office. This means, that in the very unlikely event of a failure in the back office, none of the front offices would be able to interact with the back office. Introducing additional interfaces will not solve this issue! On the contrary, in the very unlikely event of a failure in the back office, it is in the banks' best interest to solve this issue as it impacts the banks' clients, staff and operations. An additional interface is of no value in this case. What is the point of having a spare wheel if the engine is broken?

Banks have designed their front offices in such a way that they are robust and scalable, that they provide the necessary convenience to the end-users without compromising security, and that they can be continuously be available to fulfil the needs of the end-users. The dedicated interfaces will be made available under similar principles as this is in the interest of the banks' customers. As a result, it is very unlikely to expect that one of the front ends will not operate at the same level of

availability and performance as the other interfaces that are made available, unless one of the interfaces is being targeted or misused by external parties that have other goals than to serve the interests of the banks' customers. If the latter is the case, it does not make sense to mandate an additional lower security fall back interface that might aid criminals to commit fraud and thus impose certain risks with respect to consumer privacy and security.

b) Comparing levels of availability and performance

In a new recital, the European Commission defines inadequate performance as the case in which the dedicated interface does not operate at the same level of availability and performance as the interfaces made available to the account servicing payment service provider's payment service users for accessing their payment accounts online. In that case, both the Account Servicing Payment Service Provider (APSP) and the TPP are required to report that fact to their respective competent national authorities without delay. This seems to imply that both interfaces need to be monitored and compared continuously because otherwise it cannot be assessed, if possible at all, whether both interfaces have the same level of availability. This raises two questions:

1. The main question here is how payment service providers will be able to monitor whether the "customer interface" is operating at the same level as the dedicated interface. Will there be continuous attempts to access customer data? And if so, under what customer mandate will this data be accessed? Or, will a TPP during a customer interaction, at any first hiccup of the dedicated interface immediately revert to the customer interface with that particular customer request? Will the TPP inform the customer of this different approach before doing so?
2. How to assess whether the level of performance is "the same"? We would argue that the latter is impossible to establish considering that the user makes a different kind of use of the customer interface then TPPs do. For PSU's the customer interface is the place where they find all information and relevant transactions, regarding the different contracts he/she has with its bank, including those not in scope of PSD2. It is a tool to manage his/her entire relationship with his/her bank. The TPP does not have this same relationship or these same contracts with the users' bank and thus does not have the same use for the customer interface. Indeed, the TPP can only act towards the users' bank based on a dedicated consent to perform dedicated functions limited to the PSD2 scope. The TPP interface has to reflect this and will have different functionalities accordingly. This being the case, levels of performance will be difficult to compare.

c) Effective outages

In their amendments the European Commission define an outage as the case where the dedicated interface is unavailable for more than 30 seconds during a communication session between payment service providers within the dedicated interface. In that case, under the amendments of the European Commission, PISPs and AISPs would be allowed to make use of the interfaces made available to the payment service users for directly accessing their payment account online, which basically means that they are allowed to fall back to screen scraping practices until the

dedicated interface is functioning back again. The main challenges here are around the actual definition of an outage. Who is going to measure this 30 second timeframe and what source is considered the only truth? The issue could be on the ASPSP side, but it could be on the TPP side too, or in the communication channel the TPP chose to access the ASPSP. Who will decide, how and when, who's at fault? There can be instances where 1000 sessions are running perfectly fine in parallel on the dedicated interface, but where a single next session faces slow responses that may last over 30 seconds – does this justify a fall back to screen scraping? And does this mean that this PSP then can revert all their traffic to the customer interface? And how does the TPP inform the customer that it would gain full access to the remote banking services of the customer and secure consent to proceed – and provide proof of this consent to the ASPSP?

d) Unrealistic 30 seconds benchmark

The 30 seconds trigger after which the fall back would have to be activated – in addition to being very difficult to apportion in terms of responsibility – see above – makes no sense from a business practice perspective. The mechanism required to continuously verify the dedicated interface availability every 30 seconds may result in the fact that all TPPs may or should make continuous calls in less than 30 seconds to that interface. This could cause the side effect of performance degradation phenomenon (or even maybe a dDoS) thus contradicting de facto the ratio behind the request (unless expensive countermeasures and infrastructure empowerment to ensure same performance on each platform). Indeed, even the CPMI Guidance on cyber resilience for Financial Market Infrastructures (so at infrastructure level, a level far more critical to the economy than any single ASPSP…) only requires with respect to "Response and recovery:: … an FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a cyber disruption". The 30 seconds mandate is hence fully disproportionate, arbitrary and discriminatory on ASPSPs.

e) Required safeguards

In the case that TPP wants to use a fall back, ESBG and EACB want to strengthen that specific safeguards are in place in order to ensure that, only under the right conditions, a TPP can access the PSU interface. More specific, ESBG and EACB want to see requirements included in the RTS that, in case a TPP wants to access the PSU interface claiming an outage of the dedicated interface, this TPP should first report this outage to the competent authorities. Upon confirmation of the outage by the competent authorities, the TPP can access the PSU interface. This will also allow the competent authorities to track performance by both TPPs and ASPSPs.

f) Additional burden required for ASPSPs to log interactions

Given the interest some stakeholders have in screen scraping due to made investments it is expected that even any small hiccup of the dedicated interface will be explained as an outage or non-compliance of the dedicated interface. For ASPSPs, in order to dispute these future attempts successfully, data warehouses with full and clear logs and audit trails will be required in order to proof that the dedicated interface has been functioning properly. This will also crowd out smaller

PSPs as they might not have the resources to build two parallel systems – hence forcing the industry to create two systems would create an uneven playing field.

The associated costs with this burden of proof probably far exceeds the cost for a spare wheel. Furthermore – most EU carmakers today sell their new cars without the spare wheel since the tires are of such good quality that the normal car user will likely never need the spare wheel. If a customer wants to have the spare wheel anyway – it comes at additional cost.

g) Discretionary use of the fall back

According to the European Commission, fall back is also justified in cases where the dedicated interface does not operate in compliance with the requirements under their proposed amendments to the RTS. Also monitoring compliance with these requirements is no exact science – because of the multiple parties potentially causing a failure - so that practitioners who prefer screen scraping might interpret compliance in their own interest. What source will be considered trustworthy in case of disputes?

h) The Commission amendment requires ASPSPs to maintain 3 interfaces

Although it sounds like in the fall back option just the customer interface is used, in fact additional requirements have been stipulated by the European Commission, for example in terms of identification. Furthermore the ASPSP would need to secure that the spare wheel does not reveal any other data to the TPP than the payment account data according to the PSD and therefore it will be materially different from the customer interface and have the same risk of non-access as the dedicated API has. This effectively means that three interfaces need to be maintained by the banks: the dedicated interface, the customer interface and the spare wheel. It goes without saying that a requirement to maintain all these separate interfaces is disproportionate. As per our statement from 15 May 2017, the European Commission has to ensure that the obligations it places on market participants are proportionate to the objectives to be achieved. This being the case, a mandate to have available at all times spare wheel places disproportionate costs at the burden of ASPSPs, which they cannot recover, and thus fails the proportionality criteria. Furthermore an analysis of today's interfaces record would evidence close to 100% availability, thus the purported contingency requirement is grossly overestimated.

i) Inconsistencies between the general obligations for communication interfaces (art. 30) and the envisaged fall back solution

Since any change to the technical specification is expected to be made public to TPPs (art. 30.4) three months in advance, and since the fall back interface is essentially the same basic version of the official home banking, this means that any simple changes to layout, workflow, or UX (eg. different log-in sequence) must be communicated in advance to the TPPs. This could have some negative impacts:

- reveal possible industrial secrets or business strategies that compromise exclusivity and competitiveness on the market

- difficulty in making comparative A/B tests unless duplicating and communicating to the TPP each version of the experimental interface
- any change on platform or technology (eg. upgrading to a newer version) means double costs of development and maybe licensing.

j) The Commission's mandate for a fall back completely ignores other obligations that the banking industry already complies with – under due supervision

Under the same CPMI Guidance on cyber resilience for financial market infrastructures already referred to above, "resilience depends on effective security controls that protect the confidentiality, integrity and availability of its assets and services. …FMIs [are] to implement appropriate and effective controls and design systems and processes in line with leading cyber resilience and information security practices to prevent, limit and contain the impact of a potential cyber incident". And as reiterated by Y. Mersch, Member of the Executive Board of the ECB in his 6 December 2016 speech, "any technology-based market infrastructure service needs to be mature enough to meet high requirements in terms of safety and efficiency. These requirements are taken very seriously by the ECB in its role as operator but also as one of the European authorities overseeing the safety of the financial markets…". Additionally, EBA draft guidelines Guidelines on security measures for operational and security risks ask contingency and business continuity plans to be put in place in the context of PSD2.

k) Access log files to be made available by TPPs are no mitigation of the issue!

In the (new) Art; 33.3(e), the Commission proposes that "TPPs "document and provide, upon request and without undue delay, the log files of the data that are accessed through the interface operated by the ASPSP for its PSUs to the ASPSP, to their competent national authority". In effect, for an ESBG or EACB Member maintaining e.g. 20 million payment accounts, this would require, for a single event of non-performance of the dedicated interface for 31 seconds, thus having had to revert to the Commission's back up, to having to request, and analyse thoroughly, the log files for these 20 million PSUs from an unknown number of TPPs, in order i.a. to make sure that the ASPSP's obligations under the General Data Protection Regulation have not been infringed by TPPs. The related competent national authority would also have to verify these 20 million log files. Both processes are wholly unrealistic in terms of both resources, total costs, and timeline, and thus disproportionate and unworkable. This disposition has hence to be abandoned, and as it will be impossible to ascertain that TPPs have not infringed on ASPSPs' obligations in terms of the GDPR, the contemplated fall back must be discarded.

In addition, the integrity of such logs – in the absence e.g. of an external audit – may be difficult to ascertain.

l) A governance and supervision issue?

At face value, the Commission's amendment in effect outsources the supervision of ASPSPs to TPPs, as the latter would – on the basis of a mere claimed non-availability or malfunction during a period even slightly over 30 seconds, and regardless of what triggered that unavailability, e.g. even by coincidence a distributed denial of service (DDoS)… - be able to force ASPSPs to switch

to an insecure channel – the Commission's proposed fall back, in effect a slightly altered version of screen scraping. Thus, the protection, privacy and security of account holders would be put in jeopardy in the absence of any intervention of the supervisor, e.g. to ascertain that the ASPSP is truly accountable for the incident, and that the incident is of such a nature that it cannot be remedied easily and that another solution is required in order to maintain financial stability.

m) An as of yet non assessed but potential material impact on cost of capital for ASPSPs

The implementation and operation of 3 distinct interfaces (customer, dedicated, and fall back) as a consequence of the Commission's amendment complicates ASPSPs' operational environment and hence increases the operational risk footprint of every ASPSP individually. Under BCBS rules, an increase in operational risk has as corollary an increase in the cost of capital – a much unwelcome additional consequence for a non-sense requirement.

5. A new, additional issue:

Recital (24) of the Commission's amendment disposes that "For reasons of legal certainty, it is appropriate that this Regulation be applicable from the same date as Articles 65, 66, 67 and 97 of Directive 2015/2366". This provision requires urgent clarification. ESBG and EACB request instead the following drafting "For reasons of legal certainty, it is appropriate that this Regulation be applicable from 18 months after its entry into force date, in accordance with Article 115 (4) of Directive 2015/2366".

6. Conclusion

In this Position Paper, ESBG and EACB demonstrate that the Commission's promoted fall back to the dedicated interface for TPP access:

- Ignores the functioning of the online banking architecture, and hence will in most instances never be able to provide a "fall back" functionality;
- Proposes conditions for application (e.g. 30 seconds) in an environment (end-to-end communication over multiple channels with several parties involved) where actual responsibility for malfunction and/or failure is at best very tedious to allocate with certainty;
- Is totally askew with the many resilience and business continuity obligations already placed on and observed by ASPSP sector, under due supervision of their competent authorities;
- Does not assuage any concern with respect to customer protection, privacy, or security, and more generally will not allow ASPSPs to comply with their obligations under the GDPR (in addition, because of the resource burden involved, competent national authorities are very

unlikely to effectively monitor TPPs' compliance with the RTS as amended by the Commission);

- Is disproportionate in terms of resources, direct costs, and ancillary costs (including cost of capital) to the objective pursued, notably in the absence of any evidence that ASPSPs are not capable of providing a quality service with respect to the dedicated interface.

In summary, the European savings and retail banking community calls on EBA to – on the grounds exposed above – reject the amendment proposed by the Commission regarding this fall back interface.

In case EBA does not fully share the position of ESBG and EACB, EBA should consider the following compromise proposal to avoid costs for ASPSPs - and in consequence for PSUs - for the maintenance of a fall back interface if not required:

1. EBA should **define a minimum average availability rate** of the designated interface which should be based on the average high availability rates of today's PSU interfaces. If ASPSPs comply with the defined minimum availability rate they must not maintain a fall back interface.

2. Competent authorities should **analyse statisitics** from the monitoring the availability and performance of the dedicated interface made available by ASPSPs (Article 32).

3. If competent authorities **identify a permanent significant gap** between the defined average minimum availability rate by EBA and the real availability rate of the designated interface, ASPSPs should **report the reasons for this non-compliance and the appropriate measures to become compliant** with rate proposed in step 1 without undue delay. In addition the ASPSP should **report the availability rate of the PSU interface for the same period** in order to compare any discrepancies between the availability rates of the two interfaces.

4. In case the ASPSP replies he **will not be able to comply with the average minimum availability rate of step 1 and there is a noteworthy difference between the availability rates of the two interfaces** TPPs should have the **right to gain PSD2-compliant access to the account by using the PSU interface** as proposed by the Commission until the minimum availability rate is provided by the ASPSP.

EACB - The voice of 4,050 co-operative banks, 79 million members and 210 million customers. The European Association of Co-operative Banks (EACB) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 4,050 locally operating banks and 58,000 outlets, they serve 210 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 81 million members and 749,000 employees and have an average market share of about 20%.

Contact EACB : Marieke van Berkel, Head of Department, Marieke.vanberkel@eacb.coop; Pablo Lahoz, adviser payments, Pablo.lahoz@eacb.coop

ESBG – The Voice of Savings and Retail Banking in Europe. ESBG brings together nearly 1000 savings and retail banks in 20 European countries that believe in a common identity for European policies. ESBG members represent one of the largest European retail banking networks, comprising one-third of the retail banking market in Europe, with 190 million customers, more than 60,000 outlets (includes branches), total assets of €7.1 trillion, non-bank deposits of €3.5 trillion, and non-bank loans of €3.7 trillion. ESBG members come together to agree on and promote common positions on relevant regulatory or supervisory matters. Learn more about ESBG at www.wsbi-esbg.org

Contact ESBG: Diederik Bruggink, Senior adviser, Payments, diederik.bruggink@wsbi-esbg.org