FUTURE
OF EUROPEAN FINTECH

The Future of European Fintech Alliance welcomes the European Commission’s amendments to the Regulatory Technical Standards on Authentication and Communication under PSD2

The Future of the European Fintech Alliance, comprising 72 companies and associations across financial technology and digital financial services and including multiple banks, welcomes the European Commission’s revisions to the EBA RTS. While not achieving the optimal solution, the amendments seem to strike a balance which is essential for Europe’s fintech industry to be able to continue to play a role in retail payments and account information services.

We note that the European Commission adopts the same principle as the EBA in that the ASPSP (bank) can decide whether it wants to provide a dedicated interface or not; if a dedicated interface is offered, the TPP should use it. In our view, the optimal approach would be to reciprocate the ASPSP’s free choice of providing a dedicated interface with the TPP’s free choice to use it or not.

While such symmetry has not been ensured, the revised RTS however do make clear that in case the dedicated interface does not perform as it should, licensed Fintechs and TPPs can rely on the customer-facing online interface as a fallback-solution. This extremely important amendment means that European Fintechs are not put at the technological mercy of their very competitors, but as a fallback can rely on an established interface which in any event is continuously maintained by the
If a bank has the ability to monopolise the information flow to a TPP through a dedicated interface, then there will be no economic incentives to do it properly. On the contrary, there are several incentives for not doing it well, as a TPP can be seen in many instances as the bank’s competitor. Will banks in general do their best effort to favour their competitors? Business logic simply does not support it. This is the reason many banks have been and are continuing to obstruct the services of TPPs in many EU countries. If, on the other hand, a bank’s dedicated interface has to face the competition of its own customer-facing interface, then there is an incentive for doing it well. Naturally, banks are providing their customers the best possible interface to keep them happy, and this will be the benchmark for the dedicated interface if both are available to TPPs. If the TPP is not able to leverage the customer-facing online interface, then European Fintechs will be forced to idly stand and see their businesses die in case a dedicated interface has technological problems.

The Future of European Fintech Alliance however also notes that the RTS on many topics leave significant room for interpretation. Clarifications in the following areas would be very welcome:

1. TPPs must be allowed to verify on an ongoing basis that the fallback solution is working

The TPP needs to be able to test the fallback/contingency interface at any time to ensure that the TPP can seamlessly use it when needed. The TPP could only switch back to direct access where it has a back-up system constantly up and running. Such a system cannot be built within a matter of hours or days but needs ongoing maintenance. Hence, without constant access at least for the purpose of testing and training, the “fallback” solution will not work.

Constant access to the fallback-solution is also needed to allow the TPP to compare and know when a dedicated interface does not offer the same level of availability and performance as the interfaces made available to the payment service user for directly accessing its payment account online in line with Article 33 (3), Article 32 (1) RTS and to maintain technologies for fallback option access.

2. ASPSP must not be allowed to force the TPP use a redirect-domain

The current AIS and PIS solutions on the basis of direct access allows consumers to use the same TPP-provided interface throughout the entire session, i.e. TPPs are not forced to “redirect” their customers to a web page hosted by the ASPSP. This is absolutely crucial in order for TPPs to be able to provide a service adapted to different environments (desktop, mobile, in-app, watch, PoS terminal) and which is sufficiently user-friendly. If a PIS/AIS product was forced to redirect, the consumer would be moved between different websites - that are seldom optimised for every device - in a confusing and time-consuming way. TPPs need to be allowed to stay in control of their products.

3. ASPSP interfaces must allow for both AIS and PIS to be used in the same session

Article 30 RTS suggests that the interface should accommodate both AIS and PIS, but leaves open whether the two types of services can be provided within one session. It should be clarified that the same interface solution has to be available for **PIS and AIS and combinations thereof** in the same session. TPPs must not be forced to split their services into separate sessions for account information and payment initiation services, but need to be allowed to do both in one session.

4. ASPSP should not provide less information on initiation by means of limiting the information provided to PSUs

According to Article 30.1c of the RTS, PISPs shall receive „all information on the initiation of the payment transaction and all information accessible to the account servicing payment service providers regarding the execution of the payment transaction“. This is an important principle in order for the TPP to be able to verify execution of the payment and must not be abused by means of the ASPSP deciding to provide the PSU with less information than before and using that as a benchmark for what information should be provided to the TPP.

5. TPPs must be allowed to rely on the authentication procedures of the ASPSP also when using the fallback solution

We note that Article 33.3b states that TPPs can only use the fallback solution when “they are enabled to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user“.

This text must not be misinterpreted as if the ASPSP can somewhat block usage of the fallback solution by not “enabling” the TPP to rely on all authentication procedures; TPPs should as a general rule be “enabled” to do just that in accordance with Recital 30 and Article 97 PSD2.

6. Same level of availability and performance needs to include data quality and functionality:

Data quality should be the same as for direct access, i.e. the information has to be 100% synchronised in time and fully symmetric as to its content allowing TPPs to serve clients as well as they do today.

We note that one way to ensure this principle and maximise probability for equivalent operating performance is if the dedicated interface offered by the ASPSP is based on the same API as the ASPSP’s customer-facing mobile app application.

Functionality should be the same as for direct access, i.e. the interface allows in the same way for new services and innovative designs, notably also for combinations of AIS and PIS. Thus, where a TPP proposes a new design to the ASPSP, but the latter cannot deliver the appropriate data or format via the dedicated access, direct access should be available.

7. The fallback should be to the unlimited customer-facing interface

Some banks are complaining that with the fallback option, ultimately they will be forced to maintain three different interfaces. The dedicated interface, the customer-facing interface and the fallback interface. We cannot see why this would be the case as in the fallback scenario TPPs “shall be allowed to make use of the interfaces made available to the payment service users for directly accessing their payment account online” (Art. 33 (3) draft RTS). Consequently, the real customer facing interface should only be modified to allow for the identification of TPPs. A “third” interface claimed by some banks would defy the purpose of a fallback interface as it would enable them to provide a different service level than for their own customers directly.

8. TPP activities are supervised by competent authorities - not the ASPSP

The extent of data accessed by TPPs is limited by (i) the explicit consent they obtain from the user, (ii) the stipulations within PSD2 and the RTS, and (iii) the ongoing supervision of competent authorities, e.g. based on data access logs, they may request. ASPSPs will no doubt monitor such data access, but it is not within their remit to deny it for any reason, once the TPP has identified himself properly as a PSD2-licensed PSP. Obviously, ASPSPs are free to challenge any TPP activity vis-a-vis the competent authority, but it must be clear that they cannot deny access based on their suspicions of non-compliance, e.g. lack of user consent.

9. Standards of Communication must not be set by banks only

It remains unclear what “**standards of communication** issued by international or European standardisation organisations” means per Art. 30 (3) draft RTS. It should be clarified that (i) this does not include idiosyncratic solutions that are neither “common” nor “open” in the sense of Art. 98 PSD2, and (ii) that bank-only organisations cannot be “standardisation organisations”, because they do not represent/invite all stakeholders and do not provide for open and transparent procedures as stipulated, e.g., by DG COMP’s Horizontal Guidelines on standardization agreements.

10. RTS and PSD2 should accelerate security for access of Other Accounts and not restrict it

In order to serve consumers' needs, TPPs today, with explicit consent of the user, collect data from different accounts including credit accounts, savings accounts, stocks, life insurance etc. and have innovated on such data since many years.

It should be made clear that if users give explicit consent to TPPs to access data related to such accounts, and if such access is not specifically forbidden by Member States, TPPs should be able to use secure authenticated direct access to retrieve such data without discrimination.

11. Services built on data and explicitly requested by the payment service user must be allowed

It has come to our attention that some actors have interpreted Article 67.2 (f) PSD2 in a very restrictive way which would prohibit a third party to make use of data that has been retrieved by the AISP, even if the user explicitly makes the request and gives consent. This interpretation would go against the spirit of PSD2 as well as the GDPR and would severely hinder innovation.

AIS have provided many additional services for several years that make use of aggregated data, with explicit user consent and following data protection rules. These additional services respond to consumers' needs, are key parts of the business models of AIS players and are already creating major economic value and benefits.

It should be clarified that companies providing AIS services should be allowed to use, access and store account information data in order to provide **additional services explicitly requested by the payment service user**, in accordance with data protection rules.

12. SCA managed by AIS every 90 days should be able to substitute SCA managed by ASPSP

The forced SCA managed by ASPSPs every 90 days will seriously limit competition, innovation and user friendliness. SCA managed by ASPSPs during an ongoing use of AIS by users is a strong barrier in the user experience (as an example, the user may be sleeping when ASPSPs request an SCA at the AISP's connection).

It should be clarified - in this particular case - that SCA managed by AISPs can substitute SCA managed by ASPSPs.

13. Real time information are crucial for AIS's users

While instant payments are not yet available, real-time information is already crucial for AIS to cover consumers' needs. The limitation to request information no more than four times in a 24-hour period erects an artificial barrier that will disable AISPs to provide services as good as ASPSPs. More concretely, ASPSPs will be able to push data to their clients in real-time while AISP users will have to wait for the next AIS authorized connection to be aware of financial movements on their accounts.

It should be clarified that AISPs are allowed to always connect every time there is new information on ASPSP interfaces if users have actively requested once for all to AISP.