Brussels, 11 July 2017

THE ISSUE: HOW TO ORGANISE EFFICIENT AND FUTURE PROOF BANK – THIRD PARTY (TPP) INTERACTION UNDER PSD 2

Current status: the European Commission proposes upgraded screen scraping as fall-back

The European Banking Authority issued its final draft RTS[1] in February 2017 that the European Commission amended on 26th May. The most striking amendment aims at imposing a "fall-back solution" in case the dedicated interface offered by banks is not available or does not function properly. The objective would be to ensure a smooth transition from the current situation (screen scraping with TPPs impersonating customers) to standardized communication between TPPs and banks through Application Programming Interfaces (APIs).

The fall-back solution proposed by the European Commission allows TPPs to identify themselves towards banks and get access to the customers' financial data. This upgraded screen scraping is assumed to be cheap to develop and to not violate privacy rules.

Implications: consumer data at risk of being exposed against higher development costs

First, the solution proposed by the Commission means that TPPs will have access to all the data that are visible to the customer when he/she accesses his/her internet banking application, i.e., current account, savings account, insurances, loans or mortgages taken out, investment account, credit card account, joint current account, accounts on which the customer has a mandate (children, parents, companies, associations), pension account and all their related balances. Contrary to what data protection rules would mandate, TPPs will have this access without the bank having had the opportunity to ask their customers for their consent and to check that it was given. Second, the Commission's solution also means that banks will have double development costs (not one, but two interfaces have to be built, tested and maintained). The investment in the fall-back solution would, moreover, be wasted as the purpose of the fall-back is that it will not be used. Finally, the unintended side effect of the fall-back option is that consumers will get used to sharing their credentials with third parties, which is a bad habit to develop in a world where cybercriminals are targeting consumers to obtain their credentials.

It is therefore not surprising to see that banks, consumer organisations, new Fintechs and the European Banking Authority are strongly opposed to this fall-back solution for the following reasons, as stated by EBA in its latest opinion[2]:

It "*increases cost, fragmentation compromising the development of APIs, provides a competitive disadvantage to new entrants, a lack of improved technical reliability,*

[1] Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under PSD2

[2] https://www.eba.europa.eu/-/eba-publishes-its-opinion-in-response-to-the-european-commission-intention-to-amend-the-eba-technical-standards-for-open-and-secure-electronic-payment

incompatibility with PSD2's security requirements, supervisory constraints, and unclear consumer understanding and consent".

The way forward: using standard market practices - Application Programming Interfaces (APIs)

Application Programming Interfaces (APIs) are already largely used by all internet actors (Amazon, Google, Facebook) as they allow computers to talk to each other without any barrier. Access to payment accounts, as foreseen by the PSD2, will be no exception as APIs are based on open standards, open to all actors without discrimination and are recognised as the safest environment to date.

In order to take the concerns of incumbent TPPs into account and ensure their business continuity, the European Banking Authority, together with all National Central Banks, has, in its recent opinion, proposed:

- A requirement for banks to define transparent key performance indicators and abide by at least the same service level targets as for the customer interface (availability and quality);
- A requirement for banks to monitor and publish their availability and performance data on a quarterly basis;
- A requirement to make the interfaces available for testing at least 3 months before the entry into force of the RTS;
- A review of the functioning of the interfaces as part of the review planned for 18 months after the application of the RTS to ensure information access and sharing is working as intended.

Even if these additional requirements represent significant additional burdens on banks, the members of the EBF, ESBG and EACB, would be willing to support them as it would represent a clear choice in favour of APIs, which they believe are the best way forward to:

- Ensure fair competition between incumbent and new TPPs;
- Offer a secure environment;
- Empower consumers to decide the amount of data they are ready to share with anyone, in line with the provisions of the GDPR.

Imposing an upgraded screen scraping is contradicting all of these objectives and should be rejected to the benefit of consumer protection, innovation and security.

Request to Members of the European Parliament:

With the above in mind, we urge Members of Parliament to go along the lines proposed by EBA in its latest opinion and approach the European Commission to request the deletion of the fall-back solution.