ESBG

EUROPEAN ASSOCIATION OF CO-OPERATIVE BANKS

0362/2017 **15 May 2017**

ESBG – EACB public position

Screen scraping under PSD2: the wrong answer to consumer privacy and security, and jeopardizing innovation, certainty, level-playing field, and proportionality

---

The European Banking Authority (EBA) released in February 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[1]" to be made available by account servicing payment service providers (ASPSPs) to account information and payment initiation service providers. The final draft RTS are currently under review by the European Commission. The over 5.050 European savings, retail and cooperative banks are deeply concerned that the adoption and entry into force of this final draft RTS could be delayed, and the market significantly altered, by recent proposals to make mandatory – instead of the above mentioned dedicated interface – existing "screen scraping" practices also used by non-regulated, non-supervised third parties.

We see 6 reasons that should matter to all stakeholders in society, especially consumers and policy makers, why the dedicated interface approach as specified in the final draft RTS should be approved as quickly as possible in their present form:

1. **Account holder privacy?**
   The General Data Protection Regulation (GDPR) empowers the account holder to control the use of his/her personal data. ASPSPs, as custodians of both European consumers' funds and data, have to ensure that third parties only access such data which are defined in the Revised Payment Services Directive (PSD2) and with the explicit consent of the account holder. Contrary to the assertion of the signatories of the "European Fintech Manifesto[2]" – who wish to continue the consumer privacy invasion perpetrated through screen scraping -, the interface specified by EBA in the final draft RTS is aimed at allowing the European

[1] EBA final draft RTS, Art. 27 and 28

[2] Manifesto for the impact of PSD2 on the future of European Fintech, 5 May 2017

consumer to exert the above control – whilst at the same time enabling licensed third parties to access the payment account in line with both GDPR and the PSD2, for a certain service in accordance with the account holder's explicit consent.

2. **Security?**

The European savings, retail and cooperative banks take cybersecurity very seriously, and would assume that all policy makers and legislators do so too. In the absence of a pan-European reporting on security incidents, it is impossible to verify the claim of some third parties that screen scraping never was the cause of a security incident. At any rate, society presently only looks at the beginning of the curve of cyberattacks, which are prone to accelerate notably with the transposition of PSD2, as unaware account holders may hand over consent to not always bona fide third parties, at times hiding behind fake yet real-looking URLs. Also, the 12-13 May "WannaCry" hacker attack made it obvious that financial infrastructures have to be operated under clear roles and responsibilities, which per se exclude unidentified access such as screen scraping. Today over 90% of the attempted log-ins[3] on the websites of the world's top banks are not made by humans but by automated criminal "botnets" using stolen personal details to pry their way in, and account takeover fraud jumped 45% in 2017 in the UK alone[4]. This should be a sufficient cause for concern for anybody who takes security seriously. The practice established by a number of third party providers of asking consumers to hand over to them bank log-in details makes it easier for criminals to succeed with phishing fraud. It is therefore not responsible to promote a 15 year old technology (screen scraping), as a valid response to the ever growing challenges of the security environment (not even under the recently revised guise of "secure screen scraping", which rests on insecure URLs), especially not when the first line responsibility to refund customers for any mishaps lies with ASPSPs and not with third party providers.

3. **Innovation?**

One objective of the revised Payment Services Directive (PSD2) is to foster innovation. Against this background, it is odd to see certain stakeholders campaigning for the continued use of a 15 year old technology (i.e. screen scarping), when new technology (APIs), capable of meeting all PSD2, GDPR, and EBA RTS requirements, is already widely applied in the payment industry and will lower the threshold for new fintechs to enter this market. Any flexibility for third parties to choose screen scraping will keep the European market reliant on 1990's technology and may only benefit a few, existing "fintech" providers whose investment in screen scraping has already been recouped manyfold.

3 Shuman Ghosemajumder, CTO, Shape

4 Cifas, the not-for-profit data sharing and prevention agency

4. **Certainty?**
   The PSD2 has to be transposed by 13 January 2018, and the GDPR enters into force on 25 May 2018. Clearly, the final RTS cannot be inforce by these dates: currently a possible date of spring 2019 is being mentioned. This already significant legal vacuum creates serious issues for ASPSPs in meeting account holders 'privacy and security expectations. Any further dithering by the European Commission and Parliament to adopt EBA's final draft RTS will only prolong this uncertainty to the European consumer's detriment – whose whole bank data the so far non-regulated and non-supervised third party providers will be able to continue and exploit without the account holder's knowledge and consent, as they have for the past 15 years.

5. **Barriers to remain?**
   The European Commission traditionally places much emphasis on the necessity of removing barriers to entry. But it should also be wary not to create barriers to remain. Should the European Commission and Parliament make a "new screen scraping interface" mandatory (for 2 or more years), then all (over 5.050) European savings, retail and cooperative banks would have to invest in, operate and maintain 3 interfaces: their regular, existing customer interface, a new, API-based TPP interfaces[5], and a new "screen scraping" interface. If ASPSPs are required to provide more than one interface for third parties, the related investment and maintenance costs have to be considered. This will cause a strong distortion of competition as especially smaller ASPSPs will be disproportionately forced to provide an additional interface for third parties. In the absence of revenues for this kind of interface, it is unlikely that all ASPSPs will continue to service this market, or have to recover their costs from payment service users.

6. **Proportionality?**
   The European Commission has to ensure that the obligations it places on market participants are proportionate to the objectives to be achieved. The draft RTS mandate that ASPSPs make available an interface for interacting with third party providers and impose several quality requirements to ensure their technical availability. This being the case, a mandate to have available at all times an additional "new screen scraping interface" – solely justified by the potential unavailability[6] of the "dedicated interface" – places disproportionate costs at the burden of ASPSPs, which they cannot recover, and thus fails the proportionality criteria.

[5] Also referred to by EBA and the Commission as the « dedicated interface »

[6] To illustrate the iniquity of this argument, it should be highlighted that the European regulator never showed any concern to the availability of the ATM infrastructure – which in the past was a far more critical element of society than third party access will be in the coming future

Furthermore an analysis of today's interfaces record would evidence close to 100% availability, thus the purported contingency requirement is grossly overestimated. At any rate such a disposition would also ignore the recently announced supervisory Guidelines on Security Measures for Operational and Security Risks under PSD2 provide for requirements to ensure the continuity of services under severe disruption.

In summary, the European savings, retail and cooperative banks, Members of ESBG and EACB, urge both the European Commission and Parliament to adopt the draft RTS in their present form and therewith to enable consumer privacy to be protected in line with the promise of the GDPR, to adopt a future-proof approach to minimize the risk of cyberattacks, to provide with a sense of urgency certainty to all market participants, and to remain consistent with their pledges with respect to level playing field, proportionality, and calls for innovation.

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 ; Elisa Belvilacqua, Head of Communications, elisa.bevilacqua@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 : James Pieper, Senior adviser, Communications, James.Pieper@wsbi-esbg.org