FUTURE
OF EUROPEAN FINTECH

12-Sep-2017

Member States' Financial Services Attachés
European Council

In reply to the FIDO Alliance letter on PSD2 dated 31-Aug-17:

We understand the legitimate interest of the FIDO Alliance members to leverage on PSD2 to promote the standards supported by their Alliance and ultimately sell products and services that support those standards.

Unfortunately, their letter is built on several fundamental misunderstandings of PSD2 and the RTS, which are leading to a number of misconceptions that need to be corrected. It demonstrates how important it is to first understand the level 1 regulations of PSD2 and then the level 2 RTS specifications underneath. Following the numbering of FIDO's observations, we would like to comment as follows:

1. There are hardly any APIs in place today allowing consumers to authorize TPPs to access their bank accounts. Indeed, enabling one's direct competitors to provide services by means of purpose-built APIs is even as a concept completely novel. This is an utterly unproven territory in stark contrast to the 15 years of using direct access through the – over the years – strongly solidified and secured customer-facing online banking interfaces, which is used by almost every TPP today. It would be grossly negligent to force everybody using brand-new APIs provided by direct competitors without the possibility to fallback to direct access in case the APIs would not function. When the first elevator was built, no one would have dared abolishing staircases. Even now, 137 years later, no one does. Recommending such action to the politicians responsible for ensuring a smooth transition into the future financial services market in Europe is mind-boggling, and could easily lead to a perception that this is just about promoting FIDO standards.

2. The so-called "fallback option" of the European Commission is <u>not</u> about allowing single-factor authentication. This is a complete and utter misunderstanding of the current RTS text. Strong customer authentication

(SCA) is the general rule as stipulated by PSD2. The RTS defines very narrow exemptions for that, and the "fallback option" is not part of that.

Furthermore, when customers manually access their online banking they will be subject to the same exemptions and strong customer authentication requirements as TPPs independently of their means of access.

The fallback option is about allowing the TPP to access accounts via the customer-facing online interface of the ASPSP, so that the non-discrimination principle of PSD2 can be upheld. However, importantly, the authentication procedures are the very same, independently of whether the TPP is accessing the account via a dedicated interface or the customer-facing online interface.

FIDO is right however, that static passwords can be phished or hacked easily and are not enough to secure valuable financial assets. It is indeed important to understand this, and this is the very reason why 2nd factor SCA is stipulated in PSD2.

FIDO is also right on the fact that databases storing passwords represent a risk if not managed correctly. This is why TPPs are becoming supervised by regulators. It is unfortunate and surprising that the banking industry requested to eliminate the requirement for ISO-27001 for credentials management. And it is further surprising that the EBA accepted such request based on the technology neutrality principle, when ISO-27001 is not about technology, but about procedures.

We should also note, that databases can be made highly secure, otherwise there would be high concern about critical data, including enough data to perform transactions, hosted in the databases of a number of prestigious FIDO Alliance members.

3. TPPs transmitting static passwords is common practice and after hundreds of millions of transactions over 15 years, there is not one single incident of a TPP behaving fraudulently or leaking data. This is an empirically-backed fact. If worrying about security, it seems to us that several other payment methods, having a much worse safety record, should be outlawed first. We challenge the FIDO Alliance to present fraud data from TPPs over the last 15 years and benchmark it against the fraud data of the financial services and payment mechanisms offered by their members.

   The solution to the problem of phishing is not trying to stop people sharing passwords, which are inherently weak anyway as we just established, but to add 2nd factor SCA, which is exactly what PSD2 is doing.

   In addition, FIDO is perhaps not aware that passwords will be shared with regulated entities that will be inspected. It is unlikely, to say the least, that phishing attempts will be done by licensed entities.

4. Exactly because letting TPPs "log in as if they were a consumer" was perceived as a risk, PSD2 stipulates that they will now have to identify themselves properly as licensed, security audited and supervised financial

services entities before accessing any account and data the consumer has given consent to.

It is unfortunately another misunderstanding of FIDO that such “impersonation” would be allowed. The very contrary is the case, also for the fallback.

Furthermore, it is yet another misunderstanding that multi-factor SCA must be turned off when using direct access. To the contrary again, PSD2 stipulates SCA, and the RTS does not exempt that for using direct access neither as standard nor as fallback. Again, the fallback is about the interface used for access, not about the authentication procedure which is the same in both instances.

Moreover, PSD2 is not about redirect services like iDEAL or MyBank. They are not in scope and not Payment Initiation Service Providers (PISPs) by that definition. As a matter of fact, any API requiring a mandatory redirect of the consumer to the bank’s website, would not be compliant with PSD2. PSD2 allows TPPs to design its own user interface and not have the banks squeeze into the middle.

The “Transaction Risk Analysis (TRA)” brought into the RTS was driven by the acquiring (merchant) side. Issuing PSPs (banks) however, have all the power they need, because they have the last word and can overrule any SCA exemption request from the acquiring side. Hence, if they don’t trust the TPPs TRA, they can insist on SCA.

5. The solution to phishing attacks is not to tell customers that they shall not transmit their credentials (which are not secure anyway) through third-party provided software. If so, how could they transact online at all, given the need to use operating systems, web browsers or native apps from companies, which are not regulated and most of the time not even European and in some cases obliged by the Patriot Act to share customer credentials and personal data upon request from non European Governments. It is naïve to think that this could stop the fraud, especially after more than 20 years of trying this without success. This realization actually led to the creation of the FIDO Alliance many years ago.

   Instead, the solution is to <u>add</u> security to such insecure static passwords, which is exactly what PSD2 is doing:

   - stipulating SCA, i.e. multi-factor authentication
   - banning impersonation, by forcing TPP identification
   - licensing TPPs, to allow for security audits and supervision

In summary, it is worrying to see that an authentication specialist like the FIDO Alliance could misinterpret PSD2 and the RTS in so many ways. This may well be due to the omnipresent smoke and mirrors campaign of the European banking lobby, which is doing its best to mix up everything under the derogatively used term “screen scraping” to confuse everybody in their attempt to annihilate fundamental clauses in the already enacted PSD2 with 2nd level RTS stipulations to their liking.

Facts however, are:

- “transmission of credentials” is specifically and purposely allowed under PSD2
- “impersonation” is banned
- “direct access” is compliant with PSD2 and all RTS draft versions so far and, according to recitals 32 and 93 of the Directive, accessible to TPPs at any time
- mandatory “redirection” (to the bank website) is not PSD2 compliant
- “fallback” does not bypass any PSD2 or RTS stipulations (including authentication) and is a safety net avoiding single points of failure – not just for the beginning, but for many years to come
- “screen scraping” is just a way to automate user browsing and must not be confused with any of the other terms above

All existing bank-independent TPPs rely on direct access, which is protected by PSD2 stipulating that both direct and indirect access (API) should be allowed in parallel. Allowing direct access just for “fallback” is already an unnecessary compromise to please the banks. Campaigning against it without saying what else could save a TPPs existence in case of an API failure is irresponsible and threatening the stability of the European financial industry beyond banks.

Sincerely,

The Future of European Fintech Alliance

About the “Future of European Fintech” Alliance

Future of European Fintech brings together European fintech companies and associations that are seeking fair regulation of their services under the Payment Services Directive 2 (PSD2). We are now at a crucial moment in the finalisation of the technical standards of PSD2. We strongly believe that if some of the proposed standards are adopted, specifically those in relation to how fintechs communicate with banks on behalf of the consumer, they will have a severe adverse impact. They will have a negative impact on competition, they will jeopardise consumer control over their own financial data, and they will have a critical negative impact on the future trajectory of innovation in Europe. We therefore engage in this industry-wide and important effort to safeguard the future of European fintechs. We do it for the benefit of all European consumers, for continued growth and innovation in e-commerce and for continued European leadership in this field.

https://futureofeuropeanfintech.com/