FUTURE
OF EUROPEAN FINTECH

The Future of European Fintech Alliance – Commenting on EBA's opinion on the European Commission's amendments to the RTS on authentication and communication under PSD2

Introduction

The Future of European Fintech Alliance (the Alliance), consisting of 72 European fintechs, challenger banks and fintech associations, has reviewed the EBA's opinion on the RTS on authentication and communication dated 29 June 2017. The EBA disagrees with the European Commission's proposal to allow TPPs to use the customer-facing online interface of the ASPSP in case the dedicated interface offered by the ASPSP is unavailable or does not function as it should. The EBA instead puts forward an "alternative approach".

The natural solution to the question about dedicated interfaces would be to make it symmetrical - ASPSPs' choice to offer a dedicated interface or not should be reciprocated by TPPs' choice to use it or not. This solution would ensure that the intentions of PSD2 would be achieved. The European Commission's proposal already compromises on this principle to the detriment of the TPP, saying that the TPP must as the general rule use the dedicated interface if provided by the ASPSP. However, the EBA's approach is fully siding with the ASPSPs, removing all de facto possibility for TPPs to provide services in case the ASPSP has technological problems. This is utterly unacceptable.

Hence, the Alliance is deeply concerned about EBA's reasoning and alternative approach, both of which are flawed and based on unclear, opportunistic and in some instances factually questionable arguments. The EBA's approach ignores market and technological reality and does not provide any contingency for the case of an ASPSP-provided dedicated interface not working, and even less so provides TPPs any alternative means of providing its services with minimal interruption. As such, the EBA's approach is putting the very existence of European TPPs at severe risk. We note that despite the obligation of the EBA to make a particular effort in obtaining the views of non-bank actors (Recital 108, PSD2), the EBA has consistently chosen not to take into account comments from such actors when crafting this "alternative approach" and has not had any consultations whatsoever with the non-bank community.

We have never quite understood on what basis the EBA wants to outlaw a PSD2- compliant direct access. The only properly communicated "rationale" for the EBA's view can be found in paragraph 32 (page 11) of EBA's final report on draft RTS dated 23 February 2017, where they say this view is based on "a number of provisions under PSD2, especially on TPPs' identification, the requirements on secure communication by the ASPSP and by the AISPs, PISPs and PSPs issuing card-based

payment instruments, on relying on the authentication procedures, and on restrictions on TPPs in accessing to data [sic] and accessing information from designated payment accounts and associated payment transactions".

Those "arguments" were difficult to understand and we now note that the EBA seems to have let go off several of them as they are not repeated in the new opinion dated 29 June 2017. In particular, the EBA seems to have finally understood that TPPs indeed can identify themselves vis-a-vis ASPSPs perfectly well also within the context of direct access via the customer-facing online interface. This is a point we have repeatedly made and we are happy to see that the EBA has now understood it (with identification, the existing direct access, also referred to as screen scraping, technology is perfectly compliant with PSD2). Also, the EBA now seems to acknowledge that TPPs relying on the authentication procedures of ASPSPs are obviously fully PSD2-compatible with direct access.

However, in order to still rationalise its position to outlaw direct access (which is a position in direct violation of PSD2, inter alia recitals 32, 33 and 93, the latter of which explicitly states that the RTS "should be compatible with the different technological solutions available"), the EBA has now come up with a number of new "arguments". Most noteworthy, the EBA seems to have recently changed its legal assessment of PSD2, and now states that ASPSPs will be required by law to ensure that TPPs can access only certain data (we note that the EBA has not taken this position in any of its previous communications). Additionally, the EBA now puts forward a number of other "arguments" which as we will show below are increasingly abstract, ignore empirical evidence and again at times are factually questionable.

The above circumstances suggest that EBA's position to generally outlaw the only functioning technology used by fintechs to provide PIS and AIS today is based on a political view, and that different arguments to underpin it are chosen on an opportunistic basis.

We also note that several of the new "arguments" as well as the new suggestion that somehow banks would need to build an "adapted" version of its online banking platform to accommodate the fallback solution, almost literally reflect inaccurate talking points used by the banking lobby over the last few months. Again, the EBA has not made any effort whatsoever to obtain the views of non-banking actors despite its decision to fundamentally alter the RTS and their rationales compared to the final report issued by the EBA itself in February. As such, the Alliance cannot help but wonder what interactions the EBA has had with the bank-community in the process of drafting this new opinion.

Below follows a more detailed analysis of the EBA's opinion.

1. General comments on EBA's reasoning

The EBA now states that under PSD2, "ASPSPs will be required by law to ensure that TPPs can access only the data necessary to provide a given service to their customers", and that "if ASPSPs were to choose to provide such access based on their existing customer interface, this interface would need to be modified to comply with PSD2".

This is a completely new position taken by the EBA, which did not exist in its final report on the draft RTS dated 23 February 2017. The EBA does not at all explain how they have arrived at this new interpretation.

In any event, the position is not consistent with what PSD2 actually says. *In fact, the responsibility to only access data relevant for providing the service per Articles 66 (3)and 67 (2) PSD2 rests with the TPP,*

not the ASPSP. Articles 66 (4) and 67 (3), which lay out the obligations of the ASPSP do not contain any obligations on the ASPSP to ensure that only certain data can be accessed. In fact, Article 66 (4), which regulates the obligations of the ASPSP in the context of PIS, actually explicitly states that the ASPSP shall provide or make available information (i.e. allowing the TPP to "pull" data).

Indeed why does the EBA think that Article 66 (3g) and Article 67 (2f) PSD2 even exist? These clauses would have no raison d'être if the licensed TPP does not ex ante have potential access to more data than is needed to provide the service. In a "dedicated interface" context, the words "use" and "access" would be superfluous as then the TPP would only get limited data from the ASPSP!

As a further observation on the legal mandate of the EBA, we note that all provision of PIS and AIS today, by both non-banks and banks, is based on so called screen-scraping. Recital 93 PSD2 states that the RTS should be "compatible with the different technological solutions available". If the TPP identifies itself unequivocally towards the ASPSP, screen-scraping becomes fully PSD2-compliant. What legal basis does the EBA have to - despite this fact - outlaw the only currently working technology for providing PIS and AIS?

In the context of the discussion about data protection, it must not be forgotten that all TPPs are subject to data protection legislation in the same way as ASPSPs are, and act on behalf of and with the consent of the customer. Despite this, it seems the EBA for some reason, when it comes specifically to TPPs, wants to outsource enforcement of data protection legislation to banks. ASPSPs do not have, nor should they have, the role of an enforcement authority, but that is the job for data protection supervisory authorities. In case the implicit assumption should be that licensed entities, which do not have a bank license are not able to comply with the law and law enforcement needs to be "delegated" to banks, we would not have any non-bank PSPs to begin with! The "data protection" argument has been misused many times already as a pretext for incumbent banks to continue to monopolise the consumer's data and making it maximally difficult for the consumer to benefit from products and services offered by the incumbent bank's competitors.

To illustrate how absurd the notion is that banks should control TPP software used by PSUs when accessing the online bank, let's look at the case of e.g. the operating system and web browser used by the PSU when logging into the online bank. These are software solutions provided by unregulated companies and are almost always based on closed-source code, implying that banks have no possibility to audit it. Why does the bank not have an obligation to check whether Google, Microsoft and similar software providers are abusing customer data from the online bank? In this context, it becomes clear how flawed the suggestion is that ASPSPs would have the responsibility to ensure that TPPs do not abuse customer data, and indeed a major double standard is exposed - or maybe the incumbent banks only need to monitor software providers that compete with the bank?

2. Reviewing EBA's observed "negative consequences of a fallback option"

"Cost increases"

We do not understand this argument at all.

There is no increase in cost as there is no obligation on the ASPSP to ex ante filter data since PSD2 as explained above puts no such obligation on the ASPSP. ASPSPs can in real time identify TPPs using the same identification mechanism they would use for their dedicated access. Hence, the cost for banks to maintain the fallback option would range from zero to a very limited cost.

We also do not see why TPPs should have to "pay to be able to access the dedicated interface and the customer-facing interface of any given ASPSP". Pay whom? The ASPSP, in the absence of contracts? Or does the EBA mean that the TPP needs to invest in being able to access both interfaces? Let's be clear - any such cost, which the market will ensure is cheap through the development of market-driven APIs, where private actors bundle together multiple ASPSP-connections, which are offered to fintechs through an API, will be minuscule relative to the cost stemming from a dedicated interface not working and the TPP having to idly sit and see its business die instead of accessing accounts via the customer-facing online interface!

"Increased fragmentation"

We are of the exactly opposite view. The fallback option is in fact the only option that will ensure the development of properly working dedicated interfaces as it provides a de facto "benchmark" setting the "minimum" level at which the dedicated interface needs to operate. This crucially creates an incentive to develop dedicated interfaces that work and work well.

In fact, we have seen several prototypes of dedicated interfaces in the process of being developed by European traditional banks and they are poorly designed by conscious decision. As just one example, the French banking community's prototype for a dedicated interface is based on a so called redirect according to which the TPP would need to redirect the PSU to a domain hosted by the ASPSP as part of the payment process, thereby fully losing the control over its own product. The same goes for the "open banking API" developed by the Nordic region's largest bank, Nordea.

Why is it too much to ask that if a bank-provided dedicated interface does not work, the TPP can rely on access via the customer-facing interface, a technology via which hundreds of millions of payments and account aggregations have been done without one single instance of data leakage or compromise of credentials to the detriment of a consumer? Well-functioning APIs do not exist and the results from the ERPB working group on PIS are rather sobering as to the likelihood of ASPSPs actually developing such APIs. It is necessary with inherent "competition" from the customer-facing online interface for such development to materialise.

"Competitive disadvantages for new TPPs"

Based on the direct access model, a strong growing European fintech market sector has developed over the last few years. Currently, 72 members of the Alliance support the compromise of a fall-back solution, because they:

- know how protective of their positions and the status quo incumbent banks are, and how much effort and resources such banks and consultants are currently allocating towards thinking up dedicated interfaces that will worsen the user experience, restrict information, making it difficult for customers to use PIS/AIS, encouraging users to "opt out" of so doing, extract fees from TPPs etc etc.

- know the technological challenges facing the traditional banks and as such want to minimise their dependency on the banks' technologies; in fact fintechs' success has often been a direct consequence of the fintech being able to provide services based on new and agile technology that must not be "contaminated" by the banks' legacy technology;

- have suffered from incumbent banks' illegal blockades and obstructions and understand that many banks are looking to foreclose the market by means of taking full control of how de facto PIS and AIS will work in technological detail, and

- know that already today there are many fintechs planning to act as API-providers or "technical processors" (to borrow a term from the world of cards) by bundling bank integrations into one API that is offered to other fintechs. In this way the market will develop several different "APIs" which actually work and compete with each other rather than granting ASPSPs full control over an API which may be much poorer than their customer-facing online banking interface.

Incumbent banks wishing to take the „tech" out of fintech are the only ones benefitting from EBAs proposal. ***Let's be frank - does not the incumbent banks' very unwillingness to accept a fallback solution if the dedicated interface does not work in itself say a lot about such banks' intentions? It seems that banks do not trust their own promise of a well-functioning interface.***

We also want to remind the EBA about what PSD2 actually says - recitals 33 and 93 in particular emphasise the need for technology and business model-neutrality - when did it become the mission of the EBA to "invent" a market that has already existed for 10+ years in order to "allow new entrants" (likely to be banks!) to enter it? Indeed we suspect we will have to wait for a long time to see the EBA suggest something similar as concerns other types of products from which banks today generate revenues - can we expect the EBA to suggest to "invent" the technology and regulation of granting loans, forcing all European banks to implement a new technology platform and as such compete with new fintechs from scratch?

Finally, there is as we speak additional evidence gathering that ASPSPs are looking to curtail the business-models of AIS and PIS:

At the meetings of the Euro Retail Payments Board (ERPB) Working Group on PIS, bank representatives' made every effort to impair the service currently offered by PIS and AIS. Bank representatives have argued inter alia that (i) PIS and AIS can no longer be combined in one session (meaning that the consumer would have to log into his account several times for checking the account balance, initiating the transfer etc.); (ii) banks are allowed to force TPPs to use a redirect (which would disrupt and degrade TPP non-bank services), and (iii) PIS should not be allowed to let the consumer decide from which account to initiate the transfer, e.g. making it impossible for a consumer in a non-EUR country to use its EUR-account if paying a EUR-based merchant (with resulting FX fees). Furthermore, non-real-time banks are neither capable nor willing to provide an interface that contains the data quality that allows PIS to give merchants a payment confirmation on which they can rely on.

Chris Skinner has published an article[1] about this phenomenon where he writes that:

> *"Banks are scared. They've seen the rise of the new world of open APIs, apps and analytics and know that their organisations are not yet ready or fit to change to that world. What to do? Well, the easiest thing to do is block access to the bank's data. If third party fintech firms cannot get access to the customer's financial data, you can severely limit what they can do. Brilliant … and it's just what banks are doing."*

[1] Chris Skinner: How banks are getting around open banking and PSD2 - https://banknxt.com/59535/banks-open-banking-psd2/

“No improvement to technical reliability”

We are surprised that the EBA again is basing its recommendations on incorrect facts. The customer-facing online banking platform is one of the most critical pieces of infrastructure maintained by any bank and as such downtime is minimal. The two core reasons for this are (i) that ASPSPs have an economic incentive to provide the best possible experience to their customers and have an accumulated experience over many years in doing so; if the online bank does not work, the bank’s customers will be very upset and forced to visit the bank branches, which is something that banks over many years have discouraged, and (ii) that the customer-facing online banking infrastructure has been developed over many years and experiences large volumes of transactions, meaning that the infrastructure as such is extremely well stress-tested and integrated into all backend systems maintained by the bank. A dedicated interface on the other hand would imply a new technological stratum to be developed and maintained by the bank and this new stratum carries its own new and specific risks.

To illustrate this point, let us share with the EBA an example from reality, the Swedish Swish API. Swish is a Swedish mobile app that enables users to make instant direct payments from their bank accounts (PIS). It is owned by six large Swedish banks. There are two different Swish solutions: Swish Privat (a solution for person-to-person (P2P) payments which was launched in December 2012) and Swish Handel (an ecommerce solution allowing consumers to pay online stores (B2C) when shopping online which was launched in January 2016).

Having been launched in January 2016, Swish Handel was due to technical malfunctioning temporarily shut down in May 2016. After further investigation, it was announced that the service would be suspended until at least late August 2016. In September 2016, the service remained deactivated and the it was not until January 2017 that the service was fully functioning again.

Swish Handel is built on the basis of a dedicated interface (API) used by PSPs that distribute the Swish solution to merchants. This API makes up a perfect example of a potential “dedicated interface” offered by ASPSPs.

The events around Swish Handel illustrate the multiple problems inherent in making TPPs reliant on a dedicated interface offered by ASPSPs:

- Swish Handel worked well for several months before going down, illustrating that while a dedicated interface/“API” may seem to work well at first, technical problems can

  happen at any time, e.g. as in the case of Swish in connection with an update to the system.

- Despite Swish Handel being a commercial product on which banks make money, it took until January 2017 until the system was fully up and running again. No online bank has ever had a similar amount of downtime because the online banking platform is one of the most critical pieces of infrastructure for any bank.

- Given that the Swish API covers as many as 10 of Sweden’s largest banks, a TPP which would have been forced to use the Swish API would quickly have been gone out of business given the impact on revenues and relationships with merchants.

Needless to say, the customer-facing online banking interfaces of the different banks cooperating in Swish continued to work perfectly fine throughout the time the API was down.

Notwithstanding any legal obligation on banks to ensure that a "dedicated interface" should perform at the same level as the online banking platform, technical problems can and will happen. It only takes such temporary problems to get a TPP out of business as the TPP has ongoing costs and clients that rely on the service. It must not be an alternative that the survival of TPPs are made dependent on the hope that in an Utopian world a dedicated interface would consistently perform at the level of online banking.

Again, the EBA seems to completely ignore technological reality and empirical evidence when crafting its recommendations. Why was the only EBA-hosted hearing where TPPs were allowed to share its views with the EBA focused on identification only? Why was there no hearing on the topic of dedicated interfaces? Or did this discussion take place only between ASPSPs and the EBA?

"Incompatibility with PSD2's security requirements"

Again, the EBA is very unclear. What does it mean that the fallback option would "probably negatively affect security" and with which security requirements in PSD2 would it not be compatible?

TPPs have provided services in an unregulated market for 15 years and there have been hundreds of millions of payments and account aggregations done. How many instances of consumer data being leaked or credentials compromised by the TPP have there been during this whole time? The answer is zero.

Empirical data over 15 years show that in fact PIS and AIS via the customer-facing online interface does not at all present any particular security risk. And security will now be further increased as TPPs under PSD2 are required to identify themselves towards ASPSPs, making it easy for ASPSPs to deny access to any unlicensed TPP, whose systems and security standards are not audited and supervised.

Some banking lobbyists have compared the fallback option to an unlocked door to the vault on the side of the heavily fortified main door. Such allegory is completely flawed as the keys to the door are exactly the same - under PSD2 TPPs will not be able to get into the "side door" without unequivocally identifying themselves vis-a-vis the ASPSP!

Given the TPP is identifying itself towards the ASPSP, to which scenario is it being referred when stating that ASPSPs may be "treating any access to the customer interface as a security risk, thus blocking such access in compliance with PSD2"? Shall this suggest that ASPSPs should be allowed to unilaterally "suspect" a security risk of a properly identified licensed TPP and stop their access?

The EBA's "argument" when scrutinised seems to be crafted with the intention of scaremongering, making reference to abstract concepts such as a "coordinated cyber-attack". A coordinated cyber-attack is a hypothetical possibility, but it is independent of the interface used; both dedicated interfaces and customer-facing interfaces can be attacked. Please note once more that TPPs will not be able to access any interface in an unorderly fashion, but will have to always identify themselves. Hence, unless a number of licensed TPPs decide to collectively coordinate a cyber-attack, we do not see what the scenario of a "coordinated cyber-attack" refers to. As an observation on consistency, if EBA were to consistently apply the implicit assumption that licensed PSPs must be prevented from the hypothetical scenario that they may collectively engage in criminal actions, we are not sure any PSP, let alone any ASPSP, would be allowed to operate.

Also, it should be noted that the fallback scenario must of course be enabled at all times. This could not work in a way, where ASPSPs have to "activate" it only as and when they realise themselves that their dedicated interface has not responded within 30 seconds. Once more: fallback has to be to the exact same regular, always-on, customer-facing interface - not any additional third interface that is different again and could be turned on and off by the ASPSP. Anything else would not make sense.

If EBA was actually interested in safety, it would have made it a requirement on the dedicated interface to provide certainty on execution to the TPP so as to remove the risk of non-payment. The EBA seems to mean that the risk for non-payment should rest with the TPP, but if that is the case, how can the EBA at the same time force the TPP to unconditionally rely on a dedicated interface which likely removes the possibility for the TPP to check that payment is actually being executed?

"Supervisory constraints"

Again, we have difficulties understanding the argument. Does the EBA suggest that supervisory authorities as a general rule should intervene on an ex-ante basis? As far as we understand, that would indeed be a novel approach and for most parts probably a practically impossible one across the financial system unless maybe if the supervisory authority has a continuous monitoring of all systems of the supervised entity.

Secondly, what does the EBA mean that "intervention ex post might be equally difficult"? The TPP would be obliged to report usage of the fallback solution to the competent authorities. The competent authorities could then request the log files from the TPP. This to us seems as if intervention ex post would actually be quite straightforward.

Again, the "argument" is very unclear and does not stand up to scrutiny.

"Unclear consumer understanding and consent"

This argument exposes the EBA's political agenda in its core.

Firstly, why does the EBA assume that TPPs (licensed payment institutions) are unable to comply with the relevant legislation? The same rules on consent apply to TPPs as to any other PSP, and these are outlined in Article 64 PSD2. Is it only PSPs competing with the banks' interchange fees from cards that should be ex ante assumed to be incapable of complying with legislation?

Secondly, the PSU gives consent to the TPP to access its payment accounts. The TPP has to inform the PSU about the provision of the service. There is no distinction between a bank-owned and not bank-owned provider.

It seems the EBA has difficulties comprehending that customers may want to use innovative payment methods and account information services instead of bank-provided products. The EBA is effectively saying that it believes that the TPP is not going to comply with the law and/or that European consumers are not able to understand and use new payment methods and services and as such should not be allowed to use them. Indeed with such "friends" European innovation and competition certainly need no enemies!

3. Review of EBA's proposed alternative approach

EBA's alternative approach is no "alternative" at all but simply the same approach the EBA proposed in its February final draft RTS with some cosmetic additional requirements on the ASPSPs.

The fundamental issue still exists: TPPs are forced to stay down when - not if - the ASPSP's dedicated interface does not work.

No system works 100% of the time but what matters is if the services offered by the TPP work at the same time as when services offered by the ASPSP work. A consumer trying to make a PIS payment through a TPP does not care if it did not work because of the ASPSP being down. However, if the consumer's card offered by the ASPSP worked at that same time, then the consumer will opt to use that payment method in the future. TPPs would be technologically discriminated against.

Consumers and merchants expect their payment providers to work. Even temporary disturbances cause them to switch to alternative solutions for future payments. ASPSPs cannot be given the power to cause such additional disturbances to their competitors, even if they are only "by mistake".

EBA's alternative approach demonstrates that the EBA has a limited understanding of how technology and PIS/AIS work in practice. Its approach is utterly flawed, which is illustrated by the following points:

- What does the EBA suggest the TPP does if the dedicated interface stops working after some period of time? Please refer to the Swish "case study" referred to above; that API worked for two months and then stopped working for more than six months. With EBA's "alternative solution" the TPPs would during this time have to sit and idly watch their businesses die, while knowing that direct access via the customer-facing online interface is in the meantime working perfectly fine. Should the TPP just sit and wait for the API to work again (in the case of Swish for more than six months)? Does the EBA realise that TPPs, while like any other companies having costs, are unable to derive any revenues unless they are able to provide their services? Does the EBA realise that already today millions of European citizens pay and manage their finances through innovative TPP solutions? Does the EBA realise that PISPs have e-merchants as customers and that such e-merchants expect the PISP to be able to have working coverage of all larger banks?

- Does the EBA think that ASPSPs will take a bona fide approach to the provision of dedicated interfaces? Is the EBA not aware that the activities of TPPs across Europe are every day being illegally obstructed by banks, despite the clear message of PSD2? The illegality of such actions have already been proven.[2] The EBA seems to completely ignore empirical evidence and the economic incentives at play.

- The EBA wants to review the functioning of the interfaces 18 months after the application of the RTS to ensure they are working as intended. Does the EBA realise that TPPs have costs and customers who expect the product to work? If the interface does not work, TPPs will have been out of business for many months before the "review" is even initiated.

[2] See https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/05_07_2016_Sofortüberweisung.html?nn=3591568

- We note that it seems now understood that what matters is not only the “availability”, but also what data is being provided, and there are actually even more critical factors, e.g. data accuracy. How will the EBA ensure that sufficient accurate data is made available via the dedicated interface to allow for reliable and comprehensive PIS and AIS?

Conclusion

Five years ago, the European Commission intervened to stop the banking sector’s attempt to monopolise PIS and AIS. Then PSD2 was drafted to allow their TPP competitors’ common practice of direct access to continue, albeit under regulatory supervision to ensure their security standards going forward. Exactly these core provisions of PSD2 are now getting undermined and contradicted through EBA’s 2nd level legislation. The banking lobby appears to have good enough influence to drive it their way.

The natural solution to the question about dedicated interfaces would be to make it symmetrical - ASPSPs’ choice to offer a dedicated interface or not should be reciprocated by TPPs’ choice to use it or not. This solution would ensure that the intentions of PSD2 would be achieved. The European Commission’s proposal already compromises on this principle to the detriment of the TPP, saying that the TPP must as the general rule use the dedicated interface if provided by the ASPSP, and that the TPP can only use the fallback solution if the dedicated interface malfunctions. However, the EBA’s approach is fully siding with the ASPSPs, removing all de facto possibility for TPPs to provide services in case the ASPSP has technological problems. This is utterly unacceptable.

The EBA’s approach is putting the existence of European TPPs at grave risk. TPPs are providing services based on direct access via the customer-facing online interface, an established technology perfectly compatible with PSD2. Why can the EBA not agree to the very easily understandable principle that in case an ASPSP provides a dedicated interface that does not work, then the TPP will be allowed to use the existing well-proven technology of direct access?

This is why the Alliance call upon the European legislator to stick to the European Commission’s compromise which has been crafted based on input from all stakeholders and to rebut the one-sided approach taken by EBA, which even falls behind its own proposal from earlier this year.