&

ETPPA

The Unintended Consequences of PSD2 RTS

An assessment of PSD2 Implementation Challenges and Risks

May 2019

About ETPPA

The European Third Party Providers Association (ETPPA) is the European trade association of bank-independent PSD2 TPPs. ETPPA is an international not-for-profit association (IVZW/AISBL) organised under Belgian law. The Association will not undertake commercial or competitive activities, or collect data on commercially sensitive matters. The Association will comply with all applicable laws and regulations that apply to its activities and also ensure compliance with competition, anti-trust and similar laws and regulations.

ETPPA formalises the former Future of European Fintech (FoEF) coalition, which was created ad-hoc at the beginning of 2017 to represent the interests of TPPs in the negotiations around the PSD2 RTS on SCA & CSC, which was proposed at that time. Due to the alignment of the 75 members of that coalition, representing a large share of existing TPPs, FoEF was able to counter the banking lobby activities and achieve a "relatively" leveled playing field.

Despite level-1 (PSD2) and level-2 (RTS) legislation being in place now, a significant number of open questions and issues remain, and have to be resolved via level-3 guidance and working groups, which have been established to that extent. ETPPA represents the bank-independent TPP interests in such discussions.

About FDATA

The Financial Data and Technology Association (FDATA) was established in Europe to advocate for Open Banking in 2013, during the negotiations to add account aggregation to PSD2. and then formally incorporated in 2014. It is a member organisation, is not for profit and has a charter to develop open secure market access to innovation across all financial verticals, including payments and payments data, but also loans, mortgages, savings, investments, pensions and insurance. Customer access to these financial verticals via Third Party Providers is described collectively as Open Finance.

In 2017 FDATA was established in North America and advocates for Open Finance in Canada, Mexico and the USA. In 2018 a mandate from FDATA members was provided to form FDATA in Australasia and in Asia where it has now established operations.

FDATA plays a significant role in sharing information on best practise implementations of Open Finance between policy makers and regulators across many markets and is a strong advocate of the rights of customers in their data, the role of explicit consent, clear liability models, properly tested dispute resolution mechanics, appropriate technical standards, conformance testing and implementation capability.

Executive Summary

For the Third Party Providers (TPPs) of Europe, the next stage of PSD2 implementation holds a great deal of promise, but now an even greater degree of material business risk. **This is sure to directly cause serious end-customer detriment and will destabilise the market of TPPs who use Open Finance in their business models. There is time to take action, but not much time.**

The Regulatory and Technical Standards (RTS) to apply to PSD2 which were drafted by the European Banking Authority and finalised by the European Commission were difficult to agree due to the complexity of reconciling competing requirements, particularly in the consideration of the potential deployment of APIs, identity and security.

These are tough issues, and it is not the intention of this document to try to allocate blame. The intention is to highlight the outstanding material issues, the significant customer and business detriment that ensues from not solving the issues, and to suggest practical steps to take us to a good market facing outcome, that also reduces risk, complexity, inverse incentives and costs for the participants, where possible.

PSD2 tries to simultaneously introduce a framework to encourage innovation in Payment Initiation Services (PIS) and Account Information Services (AIS), whilst also introducing a raft of new payment security measures on the Account Servicing Payment Service Providers (ASPSP) that affect not only AIS and PIS, but also their Payment Service User's (PSU) interfaces .

Introducing all of these measures at the same time is creating a number of unintended consequences, will interrupt the critical services of many millions of customers (both consumers and small businesses), severely impede the businesses of TPPs and create a range of unnecessary risks for ASPSPs.

The impact of these unintended consequences have been exacerbated by the timelines for RTS having been set before any experience had been gained from the challenges of implementation. The maturity cycle of the API delivery in the UK by the CMA9 has illustrated that a three month window for the TPPs to widely test the production environments of the ASPSPs is significantly short. This is in fact aggravated by the fact that most ASPSPs have interpreted that going live by June the 14th is enough to be granted an exemption before September 14th. When in fact it does not allow for the need for a three month live test period requested by the RTS to apply for an exemption.

The lack of centralised visibility of what the ASPSPs are planning to deliver, simply means that TPPs and regulators cannot yet approximate the extent of the timeline problem, or the variety of market risks that are being carried.

Most actors that operate in the market are keen to see a transition to high performing and functionally rich APIs, and away from technologies using PSU interfaces for access to occur. Nobody should however infer that support for the movement to newer technologies means that TPPs are in favour of this being done in a way that impairs the access of TPPs or their customers. The guiding principle of 'no deterioration' should hold fast; there is no point in pushing for technically led innovation and improvement whilst making the customer experience worse and the TPP business performance metrics decline.

There needs to **be an order imposed** that puts the needs of customers first, and finds a way to manage the unintended consequences of rules that have been set. There is a certainty that RTS requirements for Strong Customer Authentication (SCA) will set two opposing forces in the same legal text. New SCA will undoubtedly introduce obstacles to TPPs and break connections with customers. In other words, ASPSPs are required to both introduce SCA and to not introduce obstacles. These are, in most situations, made to be incompatible requirements by the current market context. Given that the market functions well without this new SCA, this paper will seek to explain why practical steps need to be introduced to tether new SCA introduction with adequate steps to provide rights of access under PSD2 and also protect the customer from the harm of being severed from their TPP services that is delivered using non-payments data that is outside the scope of PSD2.

The market also needs adequate time to work together to resolve some of the deeply functional and technical conundrums. The dates imposed by RTS are widely known by market actors and regulators to be incompatible with their resolution. Firms on all sides of the market are under considerable stress. The human cost is high. We need to stop working towards a bad outcome imposed by rules set whilst the information was inadequate, use the best information now available, reset and work towards a good outcome in a composed and structured manner.

ETPPA and FDATA would suggest the following practical measures to Reduce Risk:

- NCAs to ask ASPSPs to report on intentions in respect of Dedicated v Adjusted Interface, and to indicate whether they have non-payment customer data held as protected resources in their digital channels
- Coordinated by the EBA, NCAs to remove the cliff edge for customers and TPPs by announcing a delay in the requirements for new SCA to be implemented on the grounds of reducing customer detriment.
- Markets to work with their NCAs to develop incentives and plans to widen scope, whilst also providing a period of customer transition, which could reasonably be measured for each ASPSP individually on the basis of being compelled to implement new SCA 12 months after they have provided a fully functioning API access to all of their protected resources in a manner which their NCA finds acceptable.
- The ASPSP would be prohibited from using new SCA to block TPP access during the transition.
- AISPs should be able to manage every 90 Days SCA for payments and non payment accounts instead of the ASPSP.
- In order to be exempted, all APIs to include the full range of functionalities as identified by the API Evaluation Group to enable ASPSPs providing dedicated interfaces without obstacles for the TPPs' continuation of PSU services without degradation in both functionality and quality.

- Until APIs include all API EG functionalities, TPPs allowed to continue accessing all customer-facing online interfaces and identify themselves based on HTTP Header

Three Sided Problem

ASPSPs that make up the vast majority of payment transactions in the EU are large banks. For reasons that are well known, large banks carry engineering complexity and often have legacy technology issues. Large banks that are intending to deliver a dedicated interface (API) and then seek exemption, have already locked down their specifications for the RTS timetable.

The dedicated interfaces that have since March 2019 been made available by banks in many instances do not meet the requirements needed to get an exemption. The interfaces often lack both the necessary functionalities (e.g. support for all authentication methods and all account types) and the necessary performance (e.g. the speed with which an PIS or AIS request is processed is often slower than what is the case for the PSU interface).

The European API Evaluation Group delivered important output. The time spent working through the issues was valuable, but its report was too close to the key 14th March 2019 date by which ASPSPs seeking to focus on delivering an API based method of meeting PSD2 obligations were required to deliver both production and testing facilities. The EBA is still working through adjustments to requirements (some of which were prompted by the API Evaluation Group output) in their Q&A tool. These outputs need to then be updated into rules in each member state.

Furthermore, the EBA has so far only clarified the so-called "explicitly legally required functionalities", whereas any obstacles, which are TPP-specific, e.g. mandatory redirection for PSUs, which are used to deliver a one-screen-one-click experience, are leading to "implicitly legally required functionalities", which must also be identified and added to the APIs, before such TPPs can use them.

The implications of changes in regulatory scope cannot be translated in to technology implementations in the time available. Failure to implement the required changes will leave 'Obstacles' that diminish the businesses of TPPs and create impediments to good customer experiences and better customer outcomes.

The timetable for RTS is set by the legislative process of the European Parliament. PSD2 is a maximum harmonisation directive. This creates a three sided problem as follows:

1. Scope of delivery is largely locked and time pressure is critical
2. Current delivery scope impedes TPPs by creating Obstacles, which is not allowed
3. There seems to be no time or willingness to make the legislative changes to alter the RTS time table.

Unfortunately the sides are leaning against each other and one of them needs to give.

Concern relating to Inverse Incentives

There is consensus across the market that functionally rich and available APIs represent the modern best practise. Most ASPSPs that are in the process of trying to deliver APIs that are acceptable to the TPP market and compliant with the guidelines set by their regulator, are hoping for an exemption to also having to build an 'adjusted' PSU interface as fallback. The proper application of the RTS would see most of these fail, having already failed to comply with first deadline on the 14th March. If TPPs are to be given the 3 month testing window (which is shown by the UK implementation experience to be already at least 9 months too short) before the ASPSP applies to their regulator for an exemption, then the regulator will not have sufficient time to review each case before the deadline.

It is not the interests of anyone in the market to incentivise ASPSPs who are striving to deliver an API to give up. If they are forced to adjust their PSU interfaces in a complex way, there is perhaps limited value in the compliant ASPSP then investing in the API. Therefore, it must be confirmed that TPP identification compliance can be achieved via so-called 'HTTP header signatures', which allow ASPSPs to avoid any adjustment if they so wish. If an ASPSP has also introduced new SCA on their PSUI, through which they directly serve their customers, they will also need sufficient time to engineer their authentication servers to permit the (now identified) TPP to access the interface when the customer is not present. There is danger of the ASPSP providing no access whatsoever to regulated TPPs.

The market needs to ensure adequate testing by both TPPs and regulators to ensure no obstacles or deterioration afflicts the TPP. It is obvious therefore that the desired outcome of the policy makers and regulators (that we progress to an API ecosystem where the APIs fully accommodate the recommendations set out by the API Evaluation Group) needs more time, and some encouragement for ASPSPs to complete and then stabilise their API.

The other obvious inverse incentive is in the customer journey. Mandatory redirection allows ASPSPs who offer the poorest customer journey via TPPs to suffer the least competition. Already in the UK API delivery, we can see significant differences between ASPSPs' Authentication Journeys. Regulators need to be aware of the utmost importance of leaving room for innovation and differentiation for TPPs in this area; redirection must not be the only option. On the one hand, allowing innovation to drive greater efficiency of customer experience is clearly important, whereas on the other, no standards allow the worst performers to hide.

The Immediate Consequences of Strong Customer Authentication

Strong Customer Authentication (SCA) flows from the RTS and applies to forms of payments and access to payments data. ASPSPs are required by the RTS timetable to implement SCA across their PSU interface, and also allow TPPs to rely on that by the 14th September. There is nothing necessarily stopping any ASPSP from choosing

to implement SCA any time before that date. The intention of SCA is to protect ASPSPs by improving their security arrangements.

TPPs that need to use the PSU interface because APIs are not functioning correctly (APIs that did not obtain an exemption or because they stopped working) will suddenly find on September 14th that SCA has been implemented and their access methods no longer work. This is because no testing environment has been provided by ASPSPs for SCA through their PSU interfaces. TPPs will need to adapt their access method for hundreds or thousands of connectors simultaneously without any documentation and / or testing environment causing a significant business interruption.

Whilst the SCA element of RTS has been widely criticised by the TPP market from the start and throughout, some of the issues are coming into sharp relief now that we better understand the full range of repercussions. **The product access enabled is too narrow in scope, the technical standards not narrow enough and their unilateral implementation by ASPSPs across current regulatory timelines will ruin businesses and cause serious customer detriment across 2019 and beyond. Conversely it will not make an immediate material difference to the security of ASPSPs due to the implementation inconsistencies that will be outlined below.**

SCA Scope

PSD2 focuses on payments and access to payments data. In terms of access to financial data, it guarantees the right of consumers and small businesses to share their payments data with regulated actors of their choosing, to prevent ASPSPs from seeking to prohibit competition and third party innovation. In the EU, and for circa 15 years, TPPs have been using many types of whole market financial data, including payments data, to building services that help end customers. This activity has taken place in the unregulated space and is in very wide use across many customer types and business models. Many ASPSPs had active campaigns to prevent customers from using such services, often citing that the customer data belonged to them. When TPPs pursued the objective of coupling access to payments data to PSD2, on the basis of payments data being a stepping stone to a wider 'Open Finance' policy, the drafting of the RTS had not commenced. The SCA implications of RTS completely spoil the 'one step at a time' proposal for rolling out the broader policy.

AIS models work when the customer is not present, by accessing the financial data using an in force customer Consent to collect their data for whichever service is being offered. Dynamic or multi-factor SCA pushes the customer to be present to insert their credentials. PSD2 requires the ASPSPs to design systems to enable the TPP to access the customer's **payments** data when they are not present. The RTS seeks to enhance the security of protected resources in payments. The practical application of SCA by ASPSPs will mean that the SCA they apply to their PSU interfaces will restrict the ability for TPPs to access non-payments data. They will implement the SCA at the front gate of their PSU interfaces, therefore applying it to both payment and non-payment financial data. It is not in the interests of ASPSPs, or their direct customers, to put a lower level of security on the front gate to

enable non-payment data to be gathered, then apply SCA elsewhere in their digital channel for the payments data. This would force the customer to log in twice to get to the payments data. As the non-payments data is not yet within the regulatory scope, the ASPSP is not obliged to go out of their way to be helpful. **In short, all of the myriad non payments data in ASPSPs - such as banks - will shortly be restricted by technology, whereas it is not restricted by regulation.**

Why this matters

There are many serious examples of customer detriment that will ensue if this issue is not addressed.

Customer Detriment - Example 1 - Managing the accounts of small businesses

Most small businesses, sole traders and contractors use cloud based accounting software. When you set up in business, the chosen bank typically supplies a current account a savings account. The common practise accessed by millions of small businesses in Europe is for the accountancy software to preload the current account and savings account, automate the bookkeeping and balance the books. We expect circa 50% of savings accounts not to be made available to TPPs because they are not also payment accounts. So the customers of these TPPs will no longer be able to enjoy the automation they have enjoyed and revert back to a manual process to load the savings account data. Certain alerts and information exchanges will be disabled. It was not the intention of RTS to ruin small business accounting systems and force the customer to regress to manual bookkeeping.

Customer Detriment - Example 2 - Managing money and making financial decisions

Across Europe many millions of customers use Money Management applications. SCA creates restrictions on access to savings and investment products provided by ASPSPs which will mean that customers can no longer automate the tracking of their savings or investment goals, or be able to rely on their TPP to push reminders or alerts to keep them on track. Similarly, loan or mortgage data held by firms who are also ASPSPs (such as all the banks, building societies and credit unions) will not be available to TPPs due to SCA, creating issues for customers who may not adequately manage their household budget, be reminded to seek better terms or make payments at the correct time. It is imperative that in the absence of adequate provision of human financial advice, which only a small percentage of customers receive, that data is not restricted from flowing to the applications that help customers. It was not the intention of RTS to make it difficult for consumers to manage their money and make better financial decisions.

TPP - Example 3 - Providers of Financial Products

Many new innovations have come to market where the TPP is also a regulated actor for the manufacture and distribution of regulated financial services, where their innovation is predicated on adequately knowing their customer, both at the point of initial sale and most importantly throughout the life of the product. The ability of the provider to make adjustments to the proposition based on changing customer circumstances or needs is inhibited by restricting access to data that they currently use in their models and for adequate record keeping. In short, for the digital distribution of financial products, 'Open Finance' facilitates treating customers fairly and

regulatory compliance. It was not the intention of RTS to make it difficult for best practise to be employed in the digital distribution of financial products.

TPP Example 4 - Commercial and Contract Issues

Outwith the customer detriment and regulatory issues, TPPs have agreements with suppliers and customers which will be damaged by the non-fulfilment caused by SCA restricting access. Simply put, TPPs will no longer be able to fulfill their commercial and contractual obligations with their customers and suppliers. Given that PSD2 was an attempt to improve the conditions for innovation and competition, this backwards step is unwelcome and financially damaging to firms, penalising the most innovative. It was not the intention of RTS to force firms into financial difficulty and induce breaches of contract for the supply of services.

90 Day Re-Authentication

The imposition of 90 day re-authentication on end customers who use the services of TPPs **has no merit.**

- It has nearly zero positive impact on the security of ASPSPs. This was the objective of the rule.
- It is a serious hassle for customers, many of whom have used services provided by TPPs for many years without this imposition. There will be challenging customer education objectives to deliver, as this doesn't have a logical explanation.
- It is anti-competitive:
    - Only TPPs and not ASPSPs are disconnected from the data of their customer if the customer fails to login. This means customers can rely on time bound services supplied by their ASPSP but not their TPP.
    - In no other market are firms provided with control of the market access of their competitors.
    - It will materially diminish the business viability and commercial metrics of TPPs, and particularly in a variety of passive use cases, such as money alert or money management services.
- It is perfectly reasonable to rely on TPPs, who will all be regulated actors when RTS comes into force, to regularly remind customers that they are connected and providing a service. This is the norm anyway, as it is in the interests of the TPP and the customer to have engagement.
- It will drive poor customer outcomes. Customers will either get frustrated at constant prompting to login (Bank by Bank, for payment accounts and non-payment accounts, every 90 days), or forget to login and be disconnected from potentially critical services that are protecting their financial health.

The easiest way to solve this in the short term, is to require TPPs to remind customers, via push notification or alternative, every 90 days that they are still connected, rather than forcing the customer to login with their ASPSP to enable TPP service to perpetuate. The TPP can notify the ASPSP that they have reminded the customer of their in-force Consent. This is in line with the recommendation of the European API Evaluation Group. It is a practical and simple step to solve the issues listed above. It will need some time for the market participants to engineer into their specifications.

SCA in Adjusted Interfaces is really hard to accomplish

Whilst much work and thinking has gone to the development of plans for APIs to support PSD2 implementation, not nearly enough work and thinking has gone into making proper plans for providing an Adjusted PSUI instead of an API, which is a valid alternative. Given that the RTS timetable is too short for the successful delivery of APIs that don't introduce Obstacles, it is highly likely that the vast majority of ASPSPs in the market providing an API will be asked by their regulators to support a fallback via their PSUIs adjusted interface, or they will themselves choose this path to compliance.

A number of technical solutions that have been discussed allow account aggregation by AIS providers when the customer is present to deal with SCA in the Consent, Authentication and Authorisation flow. Putting aside the issues of the 90 day reauthentication, the 'day 2' technology solution options for customer not present access is more challenging than regulators have realised.

The current market access model for TPPs typically involves the AIS provider, or their Technical Service Provider (as their agent) storing static login credentials and then passing these through a PSU interface when the customer is not present. Whilst PSD2 sought to protect the right of the TPP to pass through credentials in the Level 1 final text, the clarifications in the RTS seems to step back from this.

PSD2 Article 67 (b) states that the AIS provider must
'ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels;'

Whereas Chapter II of the RTS introduces authentication codes, dynamic linking (to enable authorisation in the payment flow) and a requirement to keep the Knowledge, Possession and Inherence elements of an SCA flow strictly separate to avoid the compromise of one element afflicting another.

Chapter III of the RTS on exemptions from having to apply SCA, says in Article 10 that Payment Service Providers will be 'allowed not to apply SCA' to AIS access between the 1st access and the 90 day reauthentication. It does not say that they are 'not allowed to apply SCA.' This means that the RTS has effectively contradicted the intention of PSD2, as if the ASPSP applies SCA, which they may as well choose to do, they effectively block the TPP provider from transmitting the personalised security credentials.

It is clear that there is now an obligation on the TPP to identify themselves to the ASPSP when the RTS comes into force. That is not really the difficult piece, and various techniques, including the 'HTTP header' or a special field on the customer facing site or app for the eIDAS token to be inserted have been widely discussed.

The real challenge is when SCA has been designed by the ASPSP for their PSU interfaces in such a way that there is a dynamic element which only the customer has access to. Some TPPs have supposed that the ASPSP would only impose dynamic SCA every 90 days to enable simple access. This might not always be the case and there is no obligation on the ASPSP not to use SCA for all connections. If the access is biometric, for example, an additional technology layer will be required for TPPs to pass through the authentication gateway.

Various suggestions have been put forward to enable AIS to gain customer not present access to an adjusted PSU interface, in the aforementioned case, including

- Session IDs being generated from the initial Consent and Authentication flow that can be stored and presented as an alternate type of password, that is not the customer password.
- Long lived cookie keys that keep a web session open for 90 days rather than the usual (say) 15 minutes (for payment accounts but can also be a solution to keep non payment accounts access).
- Some kind of OAuth2 token designed to work with PSU-interface access methodology.

The issue is that the engineering challenges of implementing these by ASPSPs is significant. It is not clear how these changes can be done without introducing some security vulnerabilities as they appear to be more of a workaround than a proper design. The security engineers will have to write new business logic into their customer facing authentication server. This is a non-trivial task and won't be done in a one or two month window if ASPSPs fail their exemption application, and indeed may not be acceptable to ASPSPs' information security teams. If ASPSPs implement SCA without solving these issues, they will of course completely impede any form of customer not present access for AIS providers to payments data (which are most of the AIS use cases).

It is clear that the RTS seeks to improve security measures, but the SCA detail is inconsistent, at least in the short term, with the intent of PSD2. The unintended consequences of the SCA detail leave the ASPSP protected from competition, the customer with diminished services and the TPP market widely disrupted.

EXEMPTIONS AND TRANSITION TIMETABLE IS COMPLETELY MISSING FROM THE RTS

If the ASPSP was to not block the TPP, by retaining static credential access to TPPs who have supplied their identity and confirmed their regulatory position, it might be a relatively smooth transition of the customer access through the RTS date and on until an adjusted or dedicated interface was supplied. When the customer is required to transition to an adjusted or a dedicated interface, they will have to re-onboard using a new Consent, Authentication and Authorisation Flow. There are material challenges to this, as large scale migration of an installed base of customers (where the customer has to participate) will take time.

For example, if an ASPSP is given an exemption, some time in August or September 2019, from adjusted Interface, when does the AIS provider transition its customer base to the new method of access? In the EU, there are many millions of customers using the services of TPPs. Some TPPs and TSPs have over a million connected accounts. The RTS does not contemplate the time requirements for customer transition. When an exemption is

granted, ASPSPs seem to be able to refuse other methods of access, outside API outages. The ASPSP could also implement SCA at any point blocking AIS access before 14th September. Even if the TPP gets to maintain its current access right up until the 14th September deadline, using the online PSU interfaces access method, there is no possibility of the TPP transitioning an extensive customer base to a new technology where the customer would have to effectively Consent to being a customer all over again (whilst potentially having a materially diminished service due to the scope issues). It was not the intention of PSD2 and the RTS timetable to disconnect AIS providers from their customers by failing to create a reasonable transition period to any new technology connections, it is simply an oversight.

The other transition time issue for TPPs is that there are potentially hundreds, or even thousands, of ASPSPs they need to integrate with to maintain existing customer services, and these ASPSPs might all provide a completely different integration challenge. This could not take place in a few weeks.

The TPPs should be given 12 months from the date of the exemption being granted to seek to move customers to a new API or Consent and Authentication process, during which time the ASPSP should not be allowed to implement new SCA, and where the TPP can continue to use their existing method of access. Furthermore, ASPSP dedicated interfaces should not be exempted unless they support all of the recommendations of API Evaluation Group. This will enable the market to not only move customers, but buy some time for the scope issues and inverse incentive issues to be addressed. As has now been well proven in the UK market, it will take time for the ASPSPs to mature and stabilise their APIs, whilst also resolving the issues of building the functionality to remove obstacles.

Summary of Remaining Functional Issues of PSD2 and RTS

Information requirements for PISPs via APIs

For PIS, the API should upon first SCA by the PSU provide TPPs with the same user data, that would be available on the PSUI. This typically includes the following: (a) account number or IBAN (in clear form, not aliased and not tokenized); (b) account type, (c) balance, (d) funds available (can be greater or lower than balance), (e) currency, (f) account name (product name), (g) the payer's name, (h) address plus date and place of birth, or if applicable personal/social security number.

For PIS, the API should also provide the execution-related information necessary for the provision of PIS. This has to include, at least, either the confirmation of the payment in a real-time environment, or in a batch environment, the "available balance", consisting of

(i) the account balance, (ii) any overdraft limit, and (iii) any pending/scheduled transactions, and (iv) one month of account history.

This information is in most cases already provided through the customer-facing interface and should therefore also be available through a dedicated API.

Why is that information needed?

Fraud mitigation considerations

In order to effectively mitigate the risk of fraudulent use of PIS, a PISP needs to, also when accessing an API, obtain from the ASPSP information on the identity of the payer. As an example, a payer has available funds and initiates a payment following which the TPP notifies the merchant. Post initiation, but before the payment is executed, the payer goes to an ATM and consciously withdraws all funds on the account, meaning the initiated payment will not be executed. Fraudsters can do this systematically, account by account and in multiple different banks, with fraud costs as a result. If the TPP knows the identify of the payer, it can prior to initiation for a new payment made by a PSU who has previously been associated with fraudulent behavior take mitigating measures such as delaying the confirmation of funds to the merchant. Without information on the identity of the payer such fraudsters cannot be "flagged" and anti-fraud measures cannot be properly deployed. As such, obtaining the identity of the payer is necessary for the provision of the PIS.

Payer relation purposes

From time to time a payer may contact the PISP to inquire e.g. about the status of the payment or if the individual indeed has made a payment with the PISP. In such scenarios it makes "tracking down" payments easier if the PISP gets information about the identity of the payer via the API, as this is information that the payer knows by heart.

Non-execution risk mitigation

The execution-related information is required for the PISPs to allow them analysing the likelihood of the transaction being de facto carried out and providing confirmation to merchant on settled funds and whether the payment has been executed, cleared and settled. Without any additional information PISPs cannot provide the merchant with a reliable real-time payment confirmation and acceptable rate of payment failures. **This would mean that PIS could not be used for e-commerce anymore**, where all merchants expect a real-time confirmation.

Data access

It should also be noted that PSD2, in the definition of sensitive payment data, explicitly states that the name and account number of the payer do not constitute sensitive payment data, to our understanding exactly to clarify that the PISP can access such data. It therefore needs to be ensured that data elements pertaining to the identity of the payer are not withheld by the ASPSP in the API.

Information requirements for AISPs via APIs

For AIS, the API should provide AISPs with the information necessary to provide AIS. This should be the same information related to payment accounts that has been made available by the ASPSP to the PSU or has been used to market a banking service to the PSU when logging into online banking or any other PSUI provided by the ASPSP, i.e. user data. Such as banking or budgeting apps or mobile web directly, including inter alia all account balances and historical statements, with the same historical depth, dates, label and details for transactions, fees exchange rate (if multi-currency) etc.

APIs shall provide, for each payment account, at minimum: (a) account number or IBAN (in clear form, not aliased and not tokenized); (b) account type, (c) balance, (d) funds available (can be greater or lower than balance), (e) currency, (f) account name (product name), (g) account opening date, (h) a list of account co-owners, specifically: whether the specific account owner is an organisation (company, association, etc.) or a physical person and whether that bank account is a joint account, (i) full name, (j) full address, (k) government ID number, (l) tax ID, (m) phone number, (n) email, (o) any further transaction details available in files that can be requested and downloaded through PSUIs even if they need to be downloaded to become visible, such as direct debit batches and the result of each debit.

APIs shall provide, for each transaction, at minimum: transaction date, booking date, amount, balance (after transaction), currency, IBAN of the second party to the transaction (for all incoming and outcoming transfers), second party to the transaction (for all transactions having the second party, including card payments), subject (title, description), type of transaction as defined by bank (card payment, incoming transfer, bank fees, interests, etc.), MCC code (for card payments), information of the beneficiary if available.

It would also be desirable that credit card and similar accounts shall be visible in the API. Transactions processed on a credit card should be visible on the API at least as early as they are visible on the ASPSP direct access, which may be up to 30 days before the transaction value date. Non payment accounts access should also be considered, including transaction history for products such as mortgages, credit cards, investment products, allowing controller-to- controller data sharing in accordance with the right to data portability under GDPR.

Moreover, it would be advantageous for the AIS services if the API could also provide access to the list of trusted beneficiaries with details (including at least full IBAN and label); allow adding or removing a trusted beneficiary and allow for the creation of recurring payments such as the one ASPSP offer today via the customer-facing interfaces.

Why is that information needed?

Service continuity

As with the payment initiation services, also for account information services, the Commission and the EBA stated that the APIs would need to offer at least the same availability and performance as the customer interface and

must not create obstacles for TPPs. To prevent discrimination and to maintain the same user experience and convenience that the existing AIS provide, the same information needs to be provided as through the PSUI.

Data portability of users

Effective controller-to-controller data sharing in accordance with the right to data portability under GDPR Article 20(2) gives consumers the right to share their data with other providers for the use of their services (e.g. AIS). The Article 29 Working Party ("WP29") calls for cooperation between industry stakeholders and trade associations to deliver the requirements of the right to data portability (WP29 Guidelines on the right to data portability).

Non-redirection requirements for PISPs and AISPs via APIs

In the context of PIS and AIS, the term "redirection" (or sometimes "redirect") refers to a process where the PSU starts to interact with the customer interface provided by the TPP, but is then forced to interact with an interface provided by the ASPSP (or another party), typically for authentication purposes. OAuth2 is an example of such redirection process.

Analysing the first testing facilities provided for the API access by banks as of 14 March 2019, we found that basically all banks across Europe intend to enforce redirection as their method for PSU authentication/authorisation purposes. In our view, this is creating level-playing-field issues between TPPs and banks, creating a competitive disadvantage for TPPs when offering their services based on APIs.

RTS Article 32(3) explicitly states that obstacles to the provision of PIS and AIS may include, among others, redirection. As such, ASPSPs should ensure that the API enable any credentials that are transmitted by the PSU to the ASPSP (e.g. token generator one-time codes) to be transmitted by the TPP and that the PSU does not need to interact with an ASPSP-provided landing page in order to use Mobile Bank-ID.

Redirection may not be an obstacle per se for all TPPs, but for those who have offered a fully automated, one-screen-one-click flow to 100% of their customer base, this would be an insurmountable obstacle and severe detriment of their service, leading to a significant loss of customers and business. There is no reason or rationale for imposing on these PSUs a new and less convenient flow which would unnecessarily remove choice for the merchant and consumers.

In countries with existing bank-owned or bank-integrated payment execution services, e.g. Netherlands, Germany, Austria, Poland, and many more, which are offering a payment guarantee and are all based on redirection, it would be a complete show-stopper for PIS being forced to use redirection as well. Not being able to offer payment guarantees until Instant Payments become the norm, they must be enabled to differentiate at least on the user experience level.

The main means through which bank-independent fintech's compete and innovate is through the user journey which needs to be convenient and easy-to-use. As a result of a better customer journey, in many European countries bank-independent services based on the embedded authentication method are the most widely used. Millions of European consumers and thousands of European merchants are used to such user journeys.

Furthermore, it is crucial for all TPPs to remain in control of the user experience to be able to offer products adapted for new channels and devices, e.g. voice-enabled services, payments at Point-of-Sale terminals or payments at a wrist watch or in other technological environments which are not compatible with the redirect method.

For all the above reasons, the embedded authentication method must be supported by ASPSPs. Whilst redirection can be an optional authentication approach, it is very clear that it cannot be made mandatory. An API that offers solely a redirect-based user journey will be considered a strong obstacle by all existing PIS providers having used direct access up to now and whose PSUs have therefore enjoyed the most frictionless payment flow possible. In the interest of innovation and user experience as well as PSD2 and RTS compliance, TPPs must not be blocked from the possibility to adapt their customer interfaces to new contexts and devices, i.e. must not be required to use redirection.

Summary of Remaining Technical Issues of PSD2 and RTS

PSD2 and RTS set out to be deliberately technology neutral. In most instances this is a reasonable position. Law should not set the pace of technological advance. That is not the same as requiring standards to be developed by the market.

eIDAS

The one technology that the PSD2 / RTS unfortunately does not remain silent on is the use of eIDAS certificates by which TPPs identify themselves to ASPSPs. These certificates do not appear to be designed for modern best practise and the use of cloud architecture which is prevalent in the TPP community. The availability of capable eIDAS technology is not available in the market yet, and with now only a few months to go until it becomes a requirement, TPPs across the EU are still trying to figure out how they will comply. This is a material unresolved market risk. It needs further time to enable this to be resolved.

Testing Environments

Whilst there is a requirement for ASPSPs to provide test facilities for TPPs, the examples provided to date do not bear a close resemblance to production environments. The broader issue is that the real testing is going to be conducted in the production environment and this requires careful market orchestration to enable TPPs to work closely with ASPSPs.

Contingency Arrangements

RTS Article 33, Paragraph 4 explains the conditions and expectations on the ASPSP in providing Contingency method of access, when their dedicated (API) access fails.

'As part of a contingency mechanism, payment service providers referred to in Article 30(1) shall be allowed to make use of the interfaces made available to the payment service users for the authentication and communication with their account servicing payment service provider, until the dedicated interface is restored to the level of availability and performance provided for in Article 32.'

Whilst TPPs are hopeful that the risks are somewhat mitigated by real rigour in the exemption process, there is a strong degree of scepticism in the TPP community as to whether the Contingency Access Method is realistic. The wholesale transition of the customers of TPPs to a new Consent, Authentication and Authorisation flow cannot be reversed so easily. TPPs **can not maintain** direct access ("screen scraping") agents for ASPSPs which they are not allowed to use, that can reasonably be expected to function in a crisis. Customers can not be induced at the 'touch of a button' to re-enter credentials for the AIS use case. The SCA measures imposed by RTS would also impede day 2 access (as described above). It is more likely that the TPP **would remain non-functional** whilst the ASPSP fixes their API channel. In addition to the technical and customer security issues, there would be material customer communication, confidence and engagement challenges. Regulatory supervision of the ASPSP's Dedicated Interface is a material component, as the current planning for 'Contingency' is unrealistic.

Summary

In his letter of 18th February 2019, European Commission Vice President Valdis Dombrovskis lays out his encouragement for the various strands of the EU payments ecosystem to work together to reduce friction and solve some of the challenges which are in front of it. In particular, in the accompanying Annex, the VP of the European Commission welcomes the focus on a smooth transition to APIs, whilst recognising some of the challenges in respect of scope and current regulation. We welcome this encouragement to work together to analyse and solve the problems. VP Dombrovskis suggests there is a chance of further legislation to deal with some of the issues if they are not adequately addressed by the market. Whilst this is also welcome, the severe issues unintentionally created as a side effect of the RTS cannot wait for new legislation. It is most urgent that regulators **impose an order now** that explains that where there are conflicting market demands, the needs of the customers are prioritised, with other requirements flexibly imposed to support long term best practise.

At this stage, we can see that the key issue is that the timelines of the RTS are certainly not compatible with a good outcome. If the SCA elements of RTS go forward according to the mandated timeline and if the functional and technical issues around current APIs are not resolved, there will be material disruption to existing customer services and be hugely damaging to the PSUs and to the businesses of TPPs.

To avoid this disruption, current TPP access practices need to co-exist with high quality and resilient APIs for at least 1 year past the RTS date to 14th September 2020. Or perhaps better solution would be 1 year past the date from which an ASPSP becomes compliant with requirements requested by their NCA. This will give ASPSPs additional time to mature their API delivery, remove obstacles and for regulatory incentives to provide access to

non-payment data to be brought forward. The easiest way for this to be managed is for new SCA to be applied by ASPSPs only when they have delivered their resilient, responsive and functionally rich API that meet the full range of API Evaluation Group recommendations and allowed a period for TPPs to migrate their customer base. ASPSPs who are also regulated for services which are not payments, should be compelled to make available their other protected resources - such as savings accounts, loans, mortgages and investments - before bringing forward SCA. This appears to both align incentives and keep ASPSPs focussed on moving forward the API agenda, rather than giving up.

This proposal for a structured delay to SCA implementation, tied to other factors and not independent of other factors would be needed even if every ASPSP in the market delivered the APIs perfectly to the current RTS timeline and if non-payment account types were ignored. The RTS timetable simply forgot to allow a transition period to move customers from the previous technology to the new one. SCA would impede the previous technology and therefore this needs to now be planned in. By planning the delay, we can align incentives and encourage ASPSPs who are trying to implement an API to persist in their endeavours, remove obstacles and solve some of the broader ecosystem issues outlined in this paper.

Practical Proposal to Reduce Risk

1. NCAs to ask ASPSPs to report on intentions in respect of Dedicated v Adjusted Interface, and to indicate whether they have non-payment customer data held as protected resources in their digital channels
2. Coordinated by the EBA, NCAs to remove the cliff edge for customers and TPPs by announcing a delay in the requirements for new SCA to be implemented on the grounds of reducing customer detriment.
3. Markets to work with their NCAs to develop incentives and plans to widen scope, whilst also providing a period of customer transition, which could reasonably be measured for each ASPSP individually on the basis of being compelled to implement new SCA 12 months after they have provided a fully functioning API access to all of their protected resources in a manner which their NCA finds acceptable.
4. The ASPSP would be prohibited from using new SCA to block TPP access during the transition.
5. AISP should be able to manage every 90 Days SCA for payments and non accounts instead of ASPSP.
6. In order to be exempted, all APIs to include the full range of missing functionalities as identified by the API Evaluation Group to enable ASPSPs providing dedicated interfaces without obstacles for the TPPs' continuation of PSU services without degradation in both functionality and quality.
7. Until APIs include all API EG functionalities, TPPs allowed to continue accessing all customer-facing online interfaces and identify themselves based on HTTP Header