Four Years on from Open Banking:

Liability under PSD2

The revised Payment Services Directive (PSD2) came into force in January 2018 and introduced a regulatory framework for open banking. It established new regulated players in the market, which are called third party providers (TPPs).

Four years on, there still exists much uncertainty and confusion around how liability is divided between Financial Institutions and TPPs. In particular, there is one question that often emerges:

Who is liable if an unauthorised third party gains access to a customer's payment account?

With open banking API transactions surpassing 2 billion a month at the end of 2021, understanding how the ecosystem works and what regulations and fines a participant is potentially liable for is critical.

This white paper summarises the regulatory requirements for Account Servicing Payment Service Providers (ASPSPs) as laid out in PSD2 and the associated data protection laws. A holistic view of PSD2 makes it clear that an ASPSP is liable if an unregulated third party is granted access to a customer account.

PSD2 Overview

PSD2 was adopted to improve the existing rules of the first Payment Services Directive in 2007, responding to the emergence of new digital payment services. It requires ASPSPs to give a regulated TPP instant and reliable access to customer accounts. Three types of TPPs are identified:

- Account Information Service Provider (AISP)
- Payment Initiation Service Provider (PISP)
- Card Based Payment Instrument Issuer (CBPII)

According to the EBA Regulatory Technical Standards (RTS) on strong customer authentication and secure communication, the ASPSP should check the eIDAS certificate issued by a qualified trust service provider (QTSP) to identify the TPP. Specifically, the RTS claims eIDAS certificates should be used "for the purpose of identification" (Article 34(1)).

However, identification is only half the challenge. An eIDAS certificate cannot accurately determine the regulatory status of a TPP. Although the certificate does contain the authorisation number and authorised services of the TPP (in its Home Member State) at the time of issue, this information can quickly become invalid. An eIDAS certificate is only reissued every two years and there is no legal obligation for the National Competent Authority (NCA) or QTSP to keep it updated.

Konsentus estimated that in December 2021, 1.3% of all API transaction requests used an eIDAS certificate containing outdated information. Furthermore, the eIDAS certificate contains no information on passporting rights. In the last two years, passporting has driven the majority of growth across the EEA as existing TPPs have expanded into new markets and offered new

services (which are often different to those services offered in their Home Member State).

From September 2019 to September 2021, the average number of passported TPPs per country increased from 39 to 79. At the end of 2021, passported TPPs on average accounted for 89% of total TPPs in each country within the EEA.

As such, verification of the eIDAS certificate alone poses a huge risk for an ASPSP. But if things do go wrong, and an unauthorised third party is granted access to a customer account, and the customer subsequently reports fraud or the misuse of their data, what is the extent of the liability of the ASPSP?

Consumer Rights

The first thing to note is that PSD2 greatly enhances the rights of the consumer. Under PSD2, the consumer – or payment service user (PSU) – is granted reduced liability for non-authorised payments from €50 to €150. The 'preamble' clarifies that "*the user should be liable only for a very limited amount, unless the payment service user has acted fraudulently or with gross negligence*" (71).

The general approach of shielding the payment service user (PSU) from liability (except when the PSU is acting fraudulently) runs through PSD2. It means that an ASPSP must be careful to understand their additional liability. The 'preamble' also includes the following:

(73) *In order to ensure a high level of consumer protection, payers should always be entitled to address their claim to a refund to their account servicing payment service provider*, even where a payment initiation service provider is involved in the payment transaction.

In other words, even when a TPP is involved, a payer always has the right to address the refund to the ASPSP.

Unauthorised Payments

Looking at this in more detail, PSD2 makes it clear in several clauses that ASPSPs are fully liable for non-execution, defective or late execution of payments, even where a PISP is involved.

Article 89 explicitly states that the ASPSP (referred to simply as a payment service provider, or PSP) is liable for the correct execution of the transaction. This is supported by Article 52, in which "*Member States shall ensure…the liability of the payment service provider for the initiation or execution of payment transactions*".

The logic is that the ASPSP is in the best position to assess the risks of a transaction and should therefore be liable for it. The 'preamble' explains:

(85) *The payment service provider is in a position to assess the risks involved in the payment transaction. It is the payment service provider that provides the payments system, makes arrangements to recall misplaced or wrongly allocated funds and decides in most cases on the intermediaries involved in the execution of a payment transaction. In view of all of those considerations, it is appropriate, except under abnormal and unforeseeable circumstances, to impose liability on the payment service provider in respect of the execution of a payment transaction accepted from the user…*

Where a payment transaction is unauthorised, Article 73 requires the funds to be reimbursed by the ASPSP within one day unless there are reasonable grounds for suspecting user fraud. This is the same regardless of whether the payment transaction is initiated through a PISP.

As a recent discussion paper by the EBA on selected fraud data under PSD2 reiterates, "Article 73 of the PSD2… provides that liability for unauthorised transactions should lie primarily with the PSPs (unless the user has acted fraudulently)."

The ‘preamble’ summarises the position:

(71) *In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer.*

It is ambiguous in what sense “unauthorised” is being used, and this is never specified in PSD2, implying that ‘unauthorised’ is used generally. A payment transaction carried out by an unauthorised third party is an unauthorised transaction. It therefore follows that if an ASPSP fails to discover the correct regulatory status of a TPP and allows an unauthorised third party to initiate a payment, the ASPSP is liable at least for a full refund to the PSU.

ASPSP and the TPP: Who is Liable?

There are certain sections of PSD2 which suggest that a TPP may hold partial liability. Article 73 claims that the PISP can be liable for an unauthorised payment transaction and if so, must compensate the ASPSP at its request. Article 72 states “*the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated [by the PSU]*”.

However, nothing in the regulation explains how an ASPSP should go about contacting the PISP and requesting compensation. TPPs are regulated in their own right and are not required to have any legal agreement with the ASPSP in order to access an account. Nor are the PSUs legally required to check the legitimacy of a TPP. In the absence of any contract between the ASPSP and the TPP – and considering the ASPSP is the first port of call and must initially refund the customer – it seems that the ultimate liability and “*burden of proof should lie on the payer’s payment service provider*” (85).

In situations where the PISP itself is unauthorised, it is clear that the ASPSP holds the responsibility:

(74) *The allocation of liability between the payment service provider servicing the account and the payment initiation service provider involved in the transaction should compel them to take responsibility for the respective parts of the transaction that are under their control*.

The ASPSP is in control of which third parties it grants access to. Therefore, whenever an ASPSP allows a third party to access PSU account data or funds, it is liable for the subsequent transactions. Furthermore, if the TPP has been revoked and cannot be contacted, there is nothing the ASPSP can do. According to Nadja Van de Veer, Founder of PaymentCounsel, “If the PISP has then vanished, the bank takes the financial hit”.

Are eIDAS Certificates Enough?

So, to come full circle, does an ASPSP need to check more than the eIDAS certificate? In response to concerns raised by the market during the EBA industry working groups on APIs under PSD2, the EBA published the opinion that *“ASPSPs are not legally required to rely on any other means for the purpose of identification of TPPs”* (section 9).
However, as discussed, identification is only the first step in determining whether or not to grant a

TPP account access: its regulatory status (including authorised services) must also be ascertained. The ASPSP must perform due diligence and ensure that the TPP is legitimate to comply with PSD2. Article 37(1) confirms that there is a duty to "*prohibit natural or legal persons that are neither PSPs nor explicitly excluded from the scope of PSD2 from providing payment services"*.

Article 66 requires ASPSPs to ensure that the PISP is legitimate, and the payer has the right to access it, even when explicit consent has been given. Finally, Article 68 limits the use of the payment instrument and of the access to payment accounts, mandating that:

"An account servicing payment service provider may deny an account information service provider or a payment initiation service provider access to a payment account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that account information service provider or that payment initiation service provider, including the unauthorised or fraudulent initiation of a payment transaction."

In other words, an ASPSP can block an unauthorised or fraudulent TPP from gaining access to a payment account. This is not explained in further detail, but it suggests that at the very least the ASPSP should be verifying the authorisation status of the TPP. It could also be seen as an admission that more checks must be carried out in addition to consulting the eIDAS certificate.

Additional Checks

The way open banking has evolved has shown that the verification of TPPs is vital. TPPs are entering and exiting the market the whole time – in January 2022 alone there were 4 new and 4 withdrawn entities. In addition, TPPs make constant changes to the types of services provided and the countries in which these services are being passported. Therefore, real-time understanding of a TPPs regulatory status in its Home Member State (and Host Member State if the transaction is cross-border) is essential for an ASPSP to provide the appropriate duty of care to its customers as well as to comply with PSD2.

In another of its opinions, the EBA clarified:

"However, ASPSPs may choose to carry out additional checks of the authorisation/registration status of TPPs in the respective EBA and/or national registers, provided that, in doing so, ASPSPs do not create obstacles to the provision of payment initiation and/or account information services, as required in Article 32(3) of the RTS".

The question then becomes, how do you ascertain the regulatory status of a TPP while not adding any obstacles? How do you create a real-time process which sits seamlessly in the ASPSPs workflow?

Surrounding Regulations

In addition to PSD2, ASPSPs are subject to a range of data protection laws. Most pertinently, ASPSPs could be risking a Capital Requirements Directive or General Data Protection Regulation (GDPR) breach. According to Article 82 of GDPR, *"GDPR imposes certain legal duties on organisations to protect [customers'] data"*. If found liable, an ASPSP can face a fine of €20 million or 4% of annual global turnover – whichever is greater – as well as sizable reputational damage.

There are specific national banking regulations which require ASPSPs to perform all necessary steps to protect their customers. For example, in the Netherlands, the General Banking Conditions begin with:

"*The Bank shall exercise due care when providing services. In its provision of services, the Bank shall take the Customer's interests into account to the best of its ability."*

In the UK, the second and third principles of the Principles for Business in the FCA Handbook are:

2. *"A firm must conduct its business with due skill, care and diligence".*
3. *"A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."*

The risk of not checking the current regulatory status of a TPP has been well documented and can easily be foreseen. As a result, ASPSPs may be failing their duty of care and due diligence if they decide against checking. Considering the sensitivity of the data in question, not implementing additional measures could easily be construed as negligence.

The Bottom Line

Banks are institutions that fundamentally operate through trust. Beyond all the potential regulatory breaches and fines, banks stand to lose the trust of their consumers – and this is non-negotiable. Building secure trust frameworks is essential as the open banking ecosystem continues to grow and extends into open finance.

"Konsentus recognises the unenviable predicament that financial institutions face when balancing the 'access to accounts' rights of regulated TPPs under PSD2, with the robustness of necessary due diligence checks to minimise risk and maintain consumer trust.

As open banking transitions to open finance and the number of third parties participating in the ecosystem grows, this predicament will only become more complex and challenging to orchestrate. Konsentus Verify was designed to reduce this complexity and provides a platform for checking both the identity and authorised status for all participants in the open experience, without creating obstacles in the process or introducing friction in the customer experience."

Contact our specialists today at info@konsentus.com
to understand how we can enable success for your organisation.

Mike Woods
CEO, Konsentus

About us

Konsentus is a leading global open banking RegTech company fulfilling an essential role within the European open banking ecosystem and the adoption of open banking and open finance across the globe. We are a trusted and established service provider to over 500 clients across 32 international markets.

Our multi-award-winning Verify platform enables safe and secure data exchange, by providing Financial Institutions with real-time identity and regulatory checking services, ensuring that unauthorised or fraudulent third parties are never given access to end-user account data or funds.