LIABILITY UNDER PSD2

Additional remarks on issues in PSD2's liability regime

5. Juli 2022

Effective protection against fraud is key for making payments work for consumers. Liability is the counterpart to security and needs to ensure thatconsumers and their funds are safe from economic harm, even in the case of unauthorised transactions. However, vzbv has identified issues in PSD2 that put consumers at risk and have to be addressed in order to ensure safe payment services and digital banking for consumers. This paper aims to elaborate vzbv's position in broader length than is possible in the targeted consultation's questionnaire.

1. Liability regime and incentives

In theory, PSD2 has created a balanced liability system for unauthorised payments. On the one hand, there is strict liability for PSPs incentivizing them to implement high-quality security measures that protect their customers from unauthorised payments. On the other hand, there is fault-based liability for the PSUs as they can take measures to avoid unauthorised payments as well. Since PSUs – especially consumers – are risk averse and already have a strong incentive to protect their bank accounts against unauthorised payments, their liability should be kept to a minimum in order to not discourage them from using modern payment solutions. PSD2 sought to reach that by holding PSU responsible for gross negligence only – as soon as the amount exceeds 50 €. PSUs should feel safe using modern payment solutions as long as they act with due care. PSUs refraining from using modern payment solutions for the fear of liability and loss of funds would harm the whole payments market and is therefore undesirable for both – PSPs and PSUs.

2. Actual situation of consumers

Unfortunately, vzbv's observations are that the liability regime is not always acting out as intended. German consumers complain about having to bear the costs for unauthorised transactions even though they took reasonable care. Banks generously interpret gross negligence in their terms and conditions, circumvent the burden of proof laid down in Art. 72 PSD2 and push liability to PSUs.

This matter also applies to other jurisdictions than Germany, as the ufc-que choisir's current complaint against 12 institutions shows, which is based on more than 4.300 reports of consumers.[1]

[1] Ufc-que choisir: Refus de remboursement des fraudes bancaires, 2022, https://www.quechoisir.org/action-ufc-que-choisir-refus-de-remboursement-des-fraudes-bancaires-l-ufc-que-choisir-depose-plainte-contre-12-banques-n101896/, 01.07.2022

Therefore, vzbv comes to a different conclusion than the EBA's opinion that states, "that the liability regime has worked well"[2]. From a consumer perspective, action is necessary.

3. Gross Negligence

The discussion revolves around the question of what constitutes gross negligence. PSUs need legal certainty because it defines what standard of care they have to stick to in order to avoid liability. An unclear standard of care can only entail excessive or too little care – and therefore never result in the optimal standard of care that would promise the most efficient outcome. An example for excessive care is the wide distribution of RFID-blocking cards, wallets and cases that protect against RFID-skimming. There are little to no reported cases of RFID-skimming, yet consumers seem to feel that this is an actual danger for which they are liable. Money being used to prevent a hazard that does not exist is exactly the reason to avoid excessive care as it is inefficient.

When defining a new standard of care it is vital that this standard is not supposed to demand too much of PSUs as in that case they will refrain from taking part in the modern payments market as their (not necessarily monetary) costs will exceed their gain from those transactions. However, not participating in modern payments and banking (like not using payment cards or online banking) would exclude consumers from significant parts of the economy and is in practice not a real option.

a) Inconsistent Case Law

German case law has not established a uniform interpretation of gross negligence. On the one hand, there are legal decisions stating that it is not negligent of the PSU to refrain from reporting malfunction of the phone used for SMS-TAN to the PSP[3] or passing on the PIN to the spouse and registering their smartphone to a TAN-App[4]. On the other hand, there are decisions taking the view that becoming the victim of phishing via phone call[5] or a banking Trojan[6] falls under gross negligence as well as waiving a receipt for a payment disruption[7]. These examples stand for the contradictory case law in Germany, leading to legal uncertainty on the behaviour expected from consumers to avoid liability. They show that leaving the definitions of gross negligence to judges is impractical in the payment sector. The payment process is complex and as there is no fault-based liability for PSPs, judges only search for fault on side of the PSU and forget to investigate the security measures of the PSP. It is much easier to spot mistakes made by a single human being as the PSU, than to evaluate if the PSP's complex payment process might have been the reason for the PSU's error. PSUs have the possibility and also a responsibility to provide backend security measures suitable to prevent

---

[2] EBA: Opinion on EBA's Response to the call for advice on the review of PSD2, 2022, p. 66, no. 281, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf, 01.07.2022.

[3] LG Kiel, Urteil vom 22.06.2018, 12 O 562/17.

[4] LG Nürnberg-Fürth, Urteil vom 17.07.2020, 6 O 5935/19.

[5] LG Köln, Urteil vom 10.09.2019, 21 O 116/19.

[6] OLG Oldenburg, Urteil vom 21.08.2018, 8 U 163/17.

[7] AG Frankfurt am Main, Urteil vom 06.08.2019, 30 C 4153/18.

phishing and social engineering. Regulation needs to be more detailed on the term of gross negligence. Gross negligence can only exist when the PSU's behaviour is violating those basic security rules that are absolute common sense. More is not to be expected and would be an excessive demand, keeping PSUs in an unsafe position and hinder their access to modern payments and banking.

b) Terms & Conditions of PSPs

PSPs take advantage of this uncertainty by defining obligations for the PSU using payment instruments in their terms and conditions. These obligations are often unrealistic, for example the obligation not to leave a payment card in the car (even when it is locked)[8] or that the same mobile device is not to be used for receiving TAN and online-payments via credit / debit card[9]. These examples illustrate that regulation is necessary to prevent PSPs from imposing disproportionately high behavioural standards upon PSUs in terms and conditions.

4. Burden of Proof

In Germany, it is settled case-law to use prima facie evidence when it comes to an unauthorised card payment.[10] This means that in the event of an unauthorised payment, authorized via PIN, after the loss or theft of a card, courts will assume that the PIN had been noted down on the card. The PSU can invalidate that conclusion by explaining circumstances that increase the likelihood that the card thief could have received notice of the PIN in some other way (e.g. by stating that someone has watched him entering the PIN). This seems to contradict Art. 72 of PSD2, which states: "Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Art. 69". The wording however is not fully clear, as there is no further elaboration on when the record of the use of the payment instrument is sufficient to prove the aforementioned things. The provision needs to state clearly that there is no room for prima facie evidence against the PSU in the case of an unauthorised payment.

5. Circumvention of Immediate Refund Requirement

Art. 73 I PSD2 contains an obligation for the PSP to refund the amount of the unauthorised payment transaction immediately. The only exception is in the event of reasonable grounds for suspecting fraud.

PSPs are obliged to refund first. They are supposed to get the amount back after gross negligence, fraud or other reasons for PSU's liability have been ruled by court. This provision is in practice circumvented by PSPs.

---

[8] DKB, Bedingungen für die Visa-Karte, 2021, https://dok.dkb.de/pdhttps://dok.dkb.de/pdf/kk_visa_mc.pdff/kk_visa_mc.pdf, 04.07.2022, Nr. 8.1.

[9] DKB, Bedingungen für Onlinebanking, 2022, https://dok.dkb.de/pdf/b_pin_tan.pdf, 04.07.2022, Nr. 8.1.

[10] See OLG Frankfurt am Main, Urteil vom 30.09.2021, 6 U 68/20 against which vzbv unsuccessfully lodged appeal to the BGH; BGH, Beschluss vom 19.05.2022, I ZR 153/21.

They set off their alleged claims against the PSU with the PSP's claim for refund and in doing so bypass the immediate refund requirement.[11] The result for PSUs is that they have to take legal action in order to get their refund, whenever the PSP reckons not to be liable. An immediate refund would be preferable for consumers as they are risk averse and therefore often shy away from taking legal action. Moreover, their financial solvency is in danger if the amount of the unauthorised transaction is high enough.[12] Besides, (at least in Germany) the place of jurisdiction would change if the PSP was the one taking legal action in favour of the PSU – as the legal place of jurisdiction is the defendant's domicile.

This setoff could be prevented by an exclusion of setoff for these cases. However, vzbv wants to emphasize that this is under no circumstances to be realized without clarifying what constitutes gross negligence. Currently PSUs are often liable even when they had no opportunity to prevent the unauthorised transaction from taking place. Regarding costs to be borne by the losing party – as it is the tenet in Germany – the danger of consumers having to bear both, the legal costs and the liability for the unauthorised transaction is an undesirable outcome.

[11] This legal possibility is taken for granted, see: LG Köln, Urteil vom 10.09.2019 – 21 O 116/19.

[12] See OLG Bremen, Beschluss vom 19.05.2021 – 1 W 4/21: The plaintiff has been granted legal aid after having lost more than 16.000 € through unauthorised transactions.