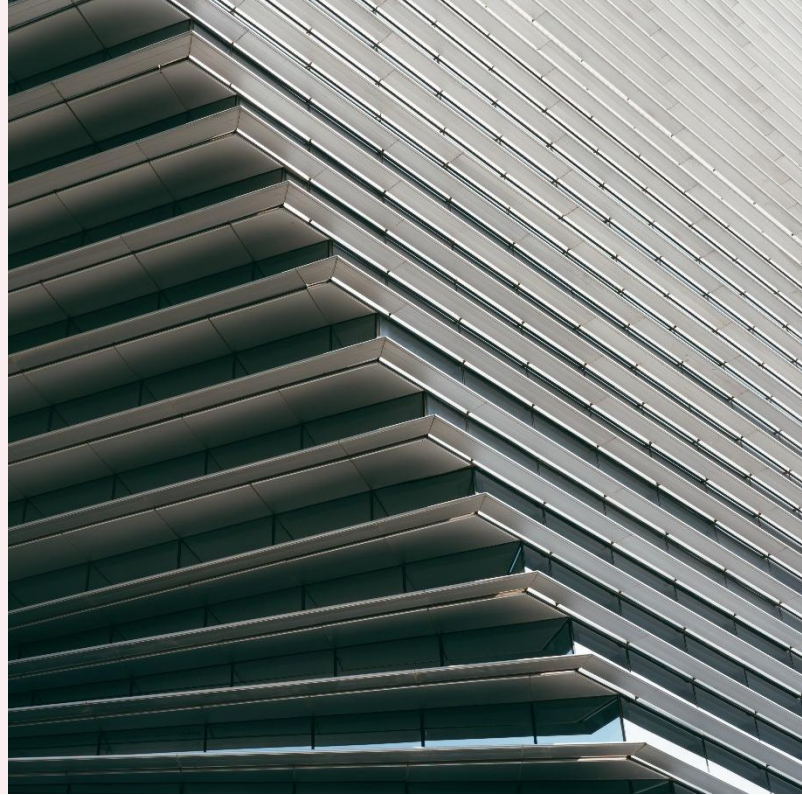


Legal bites on consumer protection in Spain (V)

Payment fraud: Tukowiecka, Spanish case law and the new liability landscape under the future PSR.

30 October 2026



The highly significant recent judgment of the Court of Justice of the European Union of 15 October 2026 (Case C-70/25, *Tukowiecka*) has made headlines that have raised concerns among financial institutions and other payment service providers: in the event of an unauthorised payment transaction, the provider must immediately refund the amount to its customer, even where it considers that the customer has acted with gross negligence.

However, the judgment goes further than this assertion and requires a more in-depth analysis, as the Court of Justice also states that, if the institution subsequently succeeds in proving such negligence, it can claim the corresponding loss from the customer.

For financial institutions, the significance of the judgment lies not so much in the extension of their liability as in the distinction between the obligation to pay an immediate refund and the definitive allocation of the loss. The issue is particularly relevant in Spain, where the European judgment intersects with national case law that had already been strengthening the user's position in court. Moreover, it comes at a time when the regulatory framework it interprets is in the process of being replaced by the forthcoming Payment Services Regulation (PSR).

The issue is no longer simply a matter of determining who is liable to the consumer, but of identifying when a refund should be made, who ultimately bears the loss, and what form any recovery takes with regard to other participants in the payments ecosystem. For banks, this requires a

review of the legal classification of cases of fraud, the process for assessing gross negligence, and the compilation of the case file from the outset.

Key points

- 1 Tukowiecka confirms that gross negligence on the part of the payer does not justify withholding the immediate refund of an unauthorised transaction under PSD2; only a suspicion of fraud can justify this.
- 2 Spanish case law (Supreme Court Judgment 571/2025) reinforces this line of reasoning: the provider's liability is quasi-absolute, and the burden of proof regarding fraud or gross negligence lies with the provider.
- 3 The correct legal classification of a payment – whether authorised or unauthorised – remains the first line of defence in any strategy to combat fraud.
- 4 The future PSR refines this framework: it allows for a provisional investigation into gross negligence and establishes a refund scheme for certain cases of impersonation in authorised transactions.
- 5 The future PSR also opens up avenues for recourse against other payment service providers, intermediaries and certain hosting providers linked to fraud.
- 6 The low average value of many fraudulent transactions poses a less obvious procedural risk: having the right to recover the loss but being unable to exercise that right effectively on a case-by-case basis.

Tukowiecka: immediate refunds and ultimate liability

The dispute stems from a clear-cut case of phishing. A customer of a Polish bank clicked on a fraudulent link, entered her login details on a page that imitated her bank's website, and a third party subsequently used those details to make a transfer of 3,000 zlotys, approximately 705 euros. After the fraud was reported, the bank refused to issue a refund, citing the customer's gross negligence in protecting her login details.

However, the question referred to the Court of Justice was not whether that conduct constituted gross negligence. Nor was the Court asked to define what constitutes gross negligence in the context of digital fraud. The question was more specific: whether such potential negligence could justify a refusal to provide an immediate refund.

The Court answered in the negative. Article 73(1) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, on payment services in the internal market, known as PSD2, requires the provider to refund the amount of an unauthorised transaction immediately and, in any event, by the end of the next business day. The exception provided for in PSD2 relates to the existence of reasonable grounds to suspect fraud committed by the payer, which must be reported in writing to the competent national authority (in Spain, the Banco de España). The fact that the institution considers there may have been gross negligence on the part of the payer does not constitute a further exception.

But that does not mean that such negligence is irrelevant. It operates on a different level: the definitive allocation of the loss. If the institution subsequently establishes that the payer breached their obligations deliberately or through gross negligence, it may seek to recover the losses to be borne by the payer or customer, through the legal remedies available under national law. The judgment preserves that possibility, but does not in itself constitute a standard procedural course of action: its specific application will depend on the national legal system and the procedural circumstances of each case.

The Spanish perspective: Tukowiecka following Supreme Court Ruling 571/2025

In Spain, articles 44 to 46 of Royal Decree-Law 19/2018 on payment services set out the key elements of the system established by PSD2: the burden of proof, the obligation to refund and the rules on the payer's liability. Supreme Court Judgment 571/2025 of 9 April constitutes a particularly significant precedent for assessing the impact of Tukowiecka.

The Supreme Court examined transactions carried out by a third party using the user's credentials and reached several important conclusions. In the event of an unauthorised transaction reported without undue delay, the provider must rectify it and refund the amount; where the user denies having authorised the transaction, it is for the provider to prove that it was authenticated, correctly recorded and accounted for. Merely recording the use of the payment instrument is not necessarily sufficient to prove either authorisation or fraud or gross negligence on the part of the payer. It is the provider's responsibility to provide evidence of the latter. The judgment also characterised the provider's liability in this area as "quasi-absolute".

There is, therefore, a clear convergence between the two decisions, although they operate on different levels. The Spanish judgment emphasises the rules governing the bringing of charges and the taking of evidence. Tukowiecka sets out more clearly a temporal consequence that the Spanish regulatory framework had already hinted at, but which Supreme Court Ruling 571/2025 did not need to elaborate on in those exact terms: any gross negligence does not permit the suspension of immediate refund under PSD2.

For Spanish banks, the difference is by no means insignificant. It is one thing to have a substantive defence against the definitive allocation of the loss.

But being able to use that defence to initially withhold the amount claimed is another matter entirely.

The first line of defence: determine whether the transaction was authorised

There is an issue that precedes gross negligence. Tukowiecka assumes that an unauthorised transaction has taken place: it is the fraudster who, having obtained the victim's login details, carries out the transfer.

Not all digital fraud follows that pattern. There is a legally significant difference between a third party who gains access to an account using stolen login details and a situation in which the customer enters the order, identifies the beneficiary and confirms the transfer, but does so because a third party has fraudulently induced them to do so.

For banks, the correct legal characterisation of the payment must form the first line of defence in any defence strategy.

Furthermore, the issue is far from being purely academic. Some court rulings are adopting a broad interpretation of Supreme Court Judgment 571/2025: the judgment of Murcia Court of First Instance No. 8 of 25 September 2025 (Oral Proceedings 1219/2024) broadens the scope of the Supreme Court's ruling and determines that the doctrine established in Supreme Court Judgment 571/2025 must apply not only to phishing or the theft of passwords, but also to cases where the customer orders the transfer under false pretences, since in both cases their true intention was not to part with the money. However, it is also worth noting that the court puts forward a second ground, independent of the first: even if the initial transfer to a bridge account opened in the claimant's own name at the same bank were to be considered authorised, the subsequent emptying of that account by the fraudster constitutes in itself an unauthorised transaction, for which the bank is liable in accordance with Articles 43 and 45 of Royal Decree-Law 19/2018.

Although this is a ruling with no case-law value, it should be treated with caution. Its broad interpretation of the doctrine set out in Supreme Court Judgment 571/2025, as applied to cases of direct deception of the payer, conflicts with the statutory definition of consent and with the distinction between an unauthorised transaction and an authorised one that has been fraudulently induced. The judgment does, in any case, reveal a trend in litigation towards a substantive reconstruction of the payer's intention and highlights one of the areas in which we can expect the most litigation: the extent to which the concept of lack of authorisation can be widened when, formally speaking, it is the payer who makes the payment.

A ruling on a system that Europe is already in the process of changing

There is one factor that makes the timing of the judgment in the Tukowiecka case particularly interesting. The Court of Justice concludes that PSD2 does not allow the introduction of an exception to the requirement for immediate

refunds on the grounds of gross negligence on the part of the payer. However, the forthcoming Payment Services Regulation (PSR) appears to be moving towards a more nuanced solution.

Article 57 of the most recent version of the text (after the Council established its position on 21 October 2026), retains the rule requiring the immediate refund of unauthorised transactions. However, it allows for a temporary exemption from this rule where the provider has objectively justified grounds for suspecting that the payer has breached, either intentionally or through gross negligence, any of the obligations set out in article 53, and notifies the payer of those grounds in writing. In such cases, according to article 57.2, the provider has 15 working days from the date the transaction is detected or reported to issue a refund or, following the relevant investigation, to provide a reasoned refusal and indicate the available channels for making a complaint. The text specifically requires that the provider report to the relevant national authority in cases where the provider concludes that the payer acted fraudulently.

Although the PSR has not yet been formally adopted, the contrast is clear. Tukowiecka does not state that allowing a preliminary investigation into gross negligence is conceptually incompatible with European law. What it concludes is that PSD2 does not contain this exception. The future PSR may end up introducing it explicitly.

If the current text remains unchanged, Tukowiecka will be a potentially significant ruling, albeit a transitional one, since it would bring a definitive end to a debate on interpretation under PSD2 just as the European legislature is designing a different approach for the future.

Authorised transactions that could also entitle customers to a refund

The future framework contains another innovation with potentially far-reaching consequences. Article 60.2 PSR establishes a specific regime for certain cases of impersonation fraud. Its scope is limited, as it requires: (1) the user to be a consumer; (2) a third party to impersonate the consumer's payment service provider using communication channels seemingly belonging to the provider; (3) this impersonation to give rise to subsequent fraudulent authorised transactions; and (4) the consumer to notify the provider of the fraud without undue delay and report it to the police. It does not provide general cover for any form of social engineering fraud or of impersonation.

This changes the traditional legal significance of the distinction between authorised and unauthorised payments. Although determining whether the transaction was authorised will remain a key issue, this may become the beginning, rather than the end, of the analysis.

In the future framework, providers will have to consider, in turn, which party initiated the transaction, whether authorisation was given, how that authorisation was obtained, what form of fraud was involved, what the parties' respective obligations were, and whether there are grounds to attribute the loss to the consumer or even another party. Pursuant to article

60.4, the protection given by article 60.2 does not apply if the consumer acted fraudulently or with gross negligence. Article 60.5 stipulates that the burden of proof lies with the provider, who must first invite the consumer to provide information on the sequence of events. Failure to respond is not in itself sufficient to conclude that there was fraud or gross negligence. The internal investigation thus becomes part of the evidence that may later be needed in legal proceedings.

In other words, correctly identifying the type of fraud involved is becoming increasingly important from a legal perspective. This makes it advisable for banks to move away from overly generic classifications like phishing, smishing and fraud. While they may be sufficient for day-to-day transactions, they are not precise enough to anticipate the legal consequences of the incident.

From bank–customer disputes to a wider chain of liability

Perhaps the most interesting thing about the future PSR is that it begins to challenge another traditional simplification, i.e. that lawsuits concerning fraud are necessarily confined to the customer and their bank.

Article 82.1 PSR establishes a right of recourse when the liability assumed by a provider under certain legal provisions can be attributed to a different payment service provider or an intermediary. Article 82.2 also provides for claims for compensation against certain hosting service providers, but does not make platforms generally liable. This compensation only has to be paid if the provider is not exempt from liability in relation to the illegally stored content under the conditions established in articles 6.1(a) and 6.1(b) of the Digital Services Act, and if the illegally stored content has led to unauthorised transactions as referred to in article 57 or the fraudulent authorised transactions specifically covered by article 60. Recital 127 clarifies that the PSR also does not turn this requirement into a general obligation for hosting providers to carry out active monitoring.

As a result, lawsuits may no longer simply be between customers and their banks, but also between the bank and another payment service provider, an intermediary or a liable third party.

This radically changes how the incident must be handled. The question will no longer be simply whether there are grounds for refusing the refund. Two further questions also need to be asked: if the bank has to provide a refund, who will ultimately bear the loss and what evidence should be kept in order to recover the loss later? These questions link together regulation, fraud management and litigation strategy.

The best defence begins before the case goes to court

Tukowiecka and Spanish precedents start from different perspectives but point to the same conclusion: evidence is increasingly important.

Spanish Supreme Court Judgment 571/2025 stipulates that the provider must prove that the payer acted fraudulently or with gross negligence. It is

not necessarily enough simply to show that the payment instrument was used. The future PSR also emphasises the importance of prevention and detection: article 87 requires transaction monitoring mechanisms that are designed, among other things, to prevent and detect potentially fraudulent transactions, and links this monitoring to the rules on payment execution and authentication. In terms of a legal defence, these mechanisms could either increase liability or be used as evidence of the controls put in place by the bank, depending on how well they are designed and function.

Banks should therefore move from simply handling claims towards genuine litigation readiness:

- Classifying the incident correctly in legal terms. A clear distinction should be made between transactions carried out by third parties, compromised passwords and other credentials, transactions carried out by the customer under false pretences, impersonation of the bank itself, and any fraud by the payer. These categories are not legally interchangeable.
- Distinction between authentication, authorisation and negligence. Supreme Court Judgment 571/2025 illustrates the risk of treating concepts as interchangeable when they serve different roles in the system of liability.
- Gathering the evidence from the very outset. The bank must be able to reconstruct the incident in enough detail to support its position in court, if necessary. It is not enough simply to store data. Sufficient evidence must be stored in relation to issues that are likely to be in dispute.
- Establishing a proper process for assessing gross negligence. After Tukowiecka, gross negligence should not be assumed automatically simply because certain credentials were used. Although it could subsequently form the basis of a claim against the customer, it must be analysed case by case and supported by admissible evidence.
- Preserving potential rights of recourse. If the future PSR retains the system set out in article 82, the case file for the incident should not be designed solely for the purposes of a potential dispute with the customer. It could also be used to establish and prove the liability of other parties involved.

The cost of making a claim: when the right to recover your loss is not enough

There is also an important procedural distinction between immediate refund and ultimate liability: when the amount is to be refunded, the bank cannot wait for the customer to bring a claim in order to address potential serious negligence. If it intends to recover the loss, it has to take the initiative and claim it.

However, we cannot overlook the fact that the proceedings leading to the ruling involved a transaction amounting to approximately 705 euros.

A bank having a solid legal claim against a customer does not necessarily mean that it is cost-effective to pursue the claim individually.

The ruling could, then, create an imbalance: the right to recovery may exist, yet the cost of enforcing it may considerably limit its practical value.

This is a strategic consideration, not a conclusion reached by the Court of Justice, but it might be just as important as the legal doctrine set out in the ruling.

For banks facing a large number of cases of fraud, the decision as to whether to pursue litigation should not be based only on the likelihood of success in a particular case. A broader, more strategic approach may be justified where the same type of fraud occurs repeatedly or on a large scale, there is strong evidence, or action could also be taken against other parties. Individual lawsuits are therefore no longer necessarily the correct way to approach the matter.

From liability to risk architecture

The main mistake in interpreting Tukowiecka would be to simply conclude that the ruling obliges banks to pay first. Its significance is more interesting.

Under PSD2, the ruling definitively distinguishes between three questions: whether the transaction was authorised; whether the refund must be made immediately; and who should ultimately bear the loss. Spanish precedent adds a fourth question: who must prove the facts that allow the ordinary liability rule to be set aside. The future PSR may well add a fifth question: whether there is another participant in the payment process to whom the loss could ultimately be passed on.

The resulting picture of how fraud risk is distributed is considerably more complex than Tukowiecka might suggest when read in isolation.

The trend in European regulation does not appear to be simply a matter of shifting liability from the customer to the bank. It is moving towards something more sophisticated: a framework for distributing fraud risk among the various participants in the payment process, accompanied by obligations relating to prevention, evidence and, where necessary, recovery.

For banks, this development also requires a change in perspective. The defence no longer begins when the claim is filed. It does not even necessarily begin when the customer makes a claim.

It starts earlier, with how prevention and monitoring mechanisms are set up, how each type of fraud is classified in legal terms, what evidence is generated and retained, how any conclusion of gross negligence is documented, and how rights of recourse against those who may ultimately have to bear the loss are preserved.

Tukowiecka's true legacy may not be deciding who loses in a phishing case, but rather demonstrating that, in the new landscape of digital fraud, the obligation to provide a refund, legal liability and the question of who ultimately bears the loss are three distinct matters.



María Guinot

Partner, Disputes, Madrid

Email : maria.guinot@cliffordchance.com

Mobile: +34 656 288 015

This publication does not necessarily cover every important topic or address every aspect of the topics it deals with. It is not intended to provide legal or other advice.

cliffordchance.com

Clifford Chance, 110 Paseo de la Castellana, 28046
Madrid, Spain

© Clifford Chance 2026

Clifford Chance, S.L.P.



Jaime Almenar

Partner, Public Law, Madrid

Email : jaime.almenar@cliffordchance.com

Mobile: +34 680 602 966

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels
• Bucharest** • Casablanca • Delhi • Dubai • Düsseldorf
• Frankfurt • Hong Kong • Houston • Istanbul • London
• Luxembourg • Madrid • Milan • Munich • Newcastle •
New York • Paris • Perth • Prague** • Riyadh* • Rome •
São Paulo • Shanghai • Singapore • Sydney • Tokyo •
Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture established by
Clifford Chance LLP.



Laura del Campo

Senior Associate, Disputes, Madrid

Email: laura.delcampo@cliffordchance.com

Mobile: +34 657 417 662

**Clifford Chance has entered into partnership
agreements with Clifford Chance Prague Association
SRO in Prague and Clifford Chance Badea SPRL in
Bucharest.



Laura García-Valdecasas

Associate, Disputes, Madrid

Email : laura.garciavaldecasa@cliffordchance.com

Mobile: +34 649 145 586