

Maximum Harmonization and General Domestic Law

(Roma Tre University, 14th April 2023)

Maria Cecilia Paglietti

Roma Tre University

mariacecilia.paglietti@uniroma3.it

Do the rules governing the allocation of legal responsibility
in the event of unauthorized payment transactions need
regulatory changes ?
(Arts. 69-77 PSD2)

Two constant needs and objectives: consumer
protection and consistency in application

Consumer protection

because of the continuing market developments, we assist to the emergence of:

- new payment methods (digitalization, mobilization)
- new security risks for electronic payments
- new political trend: differentiating between groups of users: corporate, microenterprises, consumers (and among them vulnerable/non vulnerable consumers: the latter of which refers particularly to the elderly in the payment law field)

Consistency in application and enforcement: risks of

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar extending downwards from its right end.


- forum shopping
- regulatory uncertainty (the latter being the biggest obstacle faced during the implementation of PSD2)
- altering the level playing field
- making the competitive scenario more uncertain

The high level of consumer protection and consistency in application can be ensured by resorting interpretative instruments

By working on two levels:

- 1) A proper reconstruction of the relationship between special supranational rules and general domestic private law;
- 2) An open texture nature of PSD2 (co-presence of general clauses and specific rules)

A proper reconstruction of the relationship between special supranational rules and general domestic private law



- The regulatory framework for the allocation of losses in cases of unauthorized payment:
- legislative level rules (Level 1: the directive and the relevant national transposing legislation)
- regulatory acts (Level 2, those of the regulatory agencies)
- pre-existing general internal rules on inter-subjective relations

Basic rule: financial institutions bear payment losses unless they are caused by consumer gross negligence or fraud

- C-337/20 states that the matter is regulated exhaustively by the Directive, rejecting the continued application of domestic regulatory additions of general private law
- guarantees a high degree of harmonisation
- avoids divergent application between jurisdictions and the localism of the enforcement

An open texture nature of PSD2 (co-presence of general clauses and specific rules).

- Detailed rules: strong customer authentication (Art. 4, n. 30; Art. 97);
- General clauses: the users conduct:
 - the "reasonable steps" that the users should take to keep safe their payment instruments (art. 69(1)a) and personal security credentials (Art. 69(2)),
 - users' gross negligence as an exemption from the strict liability imposed on institutions (Art. 74, § 1(2)).

Pros and Cons of the use of open-textured rules

- **PROS:**
 - makes it possible to regulate a large number of cases,
 - gives the legal framework flexibility,
 - allows the prevention of obsolescence (and of the need for continuous regulatory updates),
 - allows the setting of different levels of protection and liability based on the user's particular degree of vulnerability (as relating to, for example, elderly people).
- **CONS:**
 - broadens the margins of discretion of the judge and therefore of arbitrary choices
 - consequences on the jurisdictional (or quasi-jurisdictional) review.

Definition of gross negligence is decisive: If the customer is grossly negligent, the financial loss is shifted from the financial institution

Recital 72 PSD2:

- gross negligence is “conduct exhibiting a significant degree of carelessness” (like, for example, “keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties”)
- assessing gross negligence on the part of the payment service user, account should be taken of all of the circumstances

The concept doesn't really differ among MS, the level of diligence demanded does

- if we look at the concept of gross negligent, it does not really differ from Member States, as it is commonly intended to be “a higher standard than the standard of negligence, so “more than just carelessness” (FOS, DRN6368356; FOS, DRN135977; Cour de cassation 1st July 2020, 18-21487; Cass. civ., 19 November 2001, n. 14456; ABF, Dec. N. 540/2023
- inconsistencies might be found when it comes to assess what level of diligence demanded from the consumer: in France in most of cases concluding that the victim was not liable (Cass. 1re civ., 28 mars 2008, n° 07-10.186); in Scandinavian Countries in most of cases concluding that the victim was liable (Norwegian Supreme Court case, 19 March 2004, Rt. 2004 s. 499)
- But this was almost in the past

Nowadays differences in assessment seem to be reduced and we can find large areas of convergence in assessing the user conduct among different legal systems

Card present frauds:

common example of gross negligence:

- keeping the credentials beside the payment instrument
- keeping a payment card in a place which is accessible to third persons
- typing the credential knowing of being watched
- the short span of time between the thief of the card and the execution of the unauthorized payment transaction(s)

Card not present frauds (vishing, smishing, phishing, spoofing, SIM swap fraud cases) there are even more areas of convergence and shared principles:

- 1) every reasonable user knows by now (or at least should know) that the secret code of a payment instrument must not be communicated to any other person
- 2) every reasonable user should behave, when dealing with payment instruments, with a minimum self-responsibility and be aware of the risk of cyber-attacks
- 3) Falling for a fake email or text message or phone call disclosing security credentials and one time password is not considered, ex se, a conduct grossly negligent
- 4) Court's/Ombudspersons' assessment differs depending on the level of sophistication of the fraud

Examples that exclude gross negligence:

- **sophisticated frauds:** gross negligence cannot be attributed to the customer due to the insidiousness of the means of attack. **non-recognizability** (such as, for example, in phishing cases, receipt of an e-mail bearing a perfectly reproduced logo of the intermediary) excludes gross negligence

General clauses and consumer vulnerability



Use of general clauses allows Courts/Ombudspersons:

- to set of different levels of protection and liability based on the user's degree of vulnerability and having regard for payment service users' different levels of financial and IT education (as bearing, for example, on elderly people).
- The extent of the gross negligence, i.e. the level of diligence requested, can be graduated in virtue of the vulnerability of the consumer, especially the age

A possible conclusion

A thick yellow horizontal bar spans the width of the slide, with a vertical yellow bar extending downwards from its right end.

Instead of a changing in the legal framework, L1 legislation may remain as it is (for the reasons above mentioned) and L2 legislation may clarify the concept of gross negligence explicitly mention examples of behavior that constitute gross negligence.

And...

Thank you