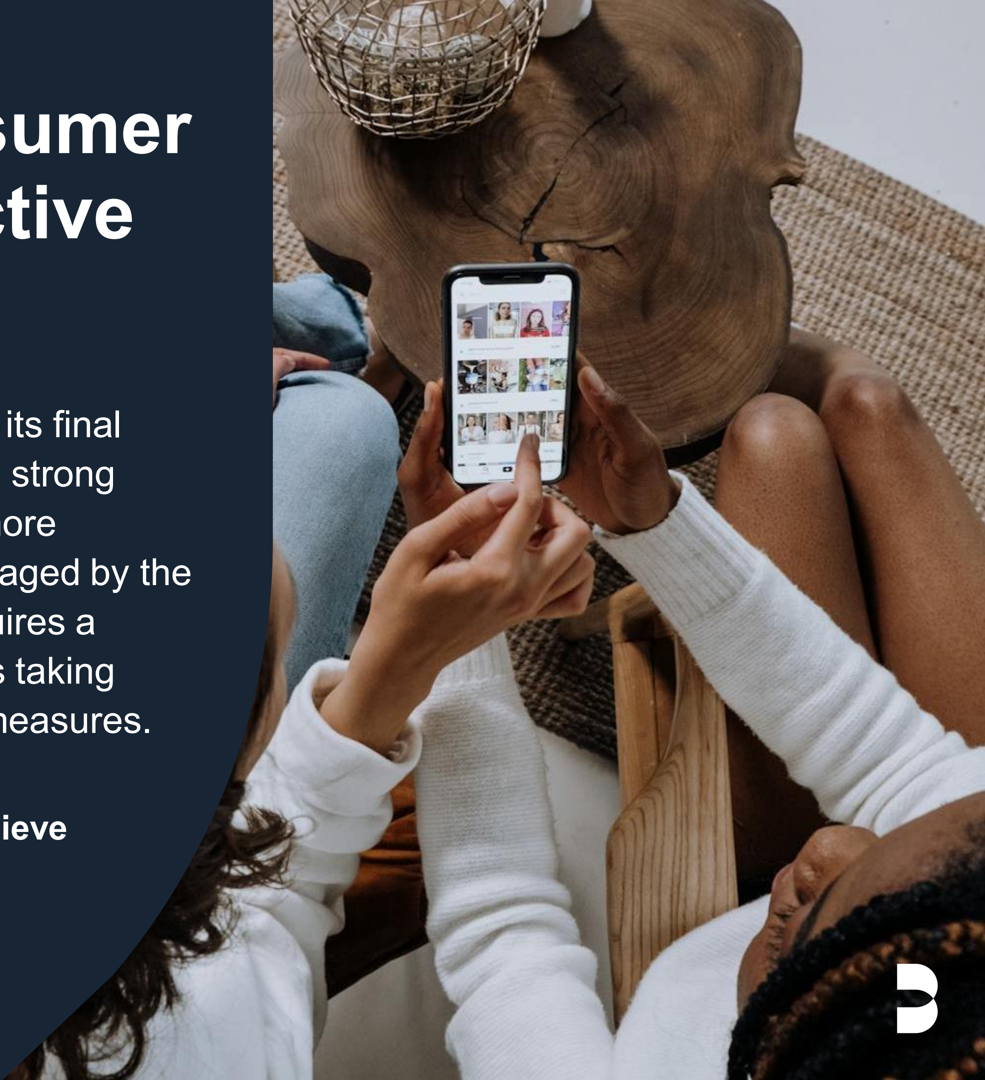
Towards enhanced consumer protection through effective fraud prevention.

The Payment Services Regulation (PSR) has entered its final stage with the start of the trialogues. The PSR holds strong potential to enhance consumer protection through more effective fraud prevention measures. We are encouraged by the growing consensus that combating online fraud requires a holistic approach, with both public and private actors taking responsibility and implementing targeted, effective measures.

In this document, we offer four elements that we believe could further enhance the PSR in its final phase.



1. Fraud prevention

Transaction monitoring (art. 83)

Banks are committed to protecting consumers by preventing fraud through monitoring real-time transactions. Banks provide a critical last line of defence, intervening before funds can reach the hands of scammers.

- We **support** the Parliament's proposal for a principle-based approach to fraud monitoring. Setting minimum requirements instead of imposing limitations, allows banks to adapt to evolving criminal tactics, including the use of AI. This leads to more effective fraud prevention and better consumer protection. The rule-based approach from the Council and the Commission may unintentionally limit the effectiveness of fraud monitoring. This approach risks undermining effective measures already in place, and limits room to respond to new types of fraud, ultimately resulting in reduced consumer protection.

- The Council's proposal for Article 83(2) rigidly splits transaction monitoring between payer and payee. This limits banks to use data for detection from only one side. The most successful fraud monitoring systems take a holistic view. To achieve this, the (transaction) behaviour of the payer and the payee must be assessed in relation. The payer PSP should be able to use the data for fraud monitoring shared by the payee PSP. For example, specific characteristics of the payee, such as account age and type, are crucial indicators to assess fraud risk. Fragmenting this view risks missing fraud and wrongly blocking legitimate transactions, ultimately harming consumers.

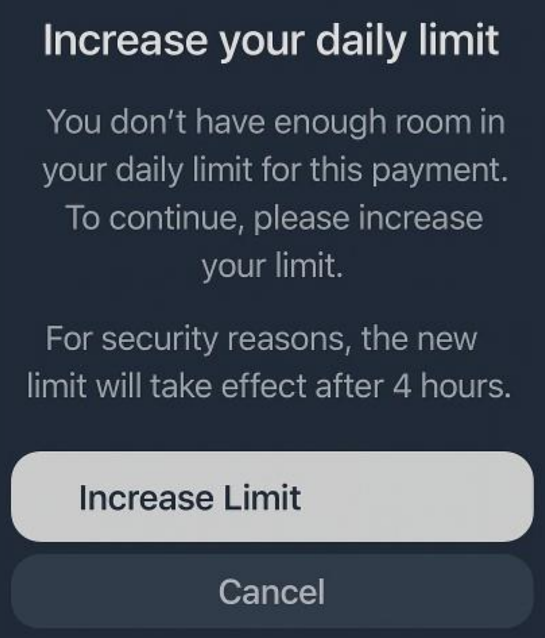
- We note that the current principle-based approach is already common and proven effective, and fully compliant with GDPR.

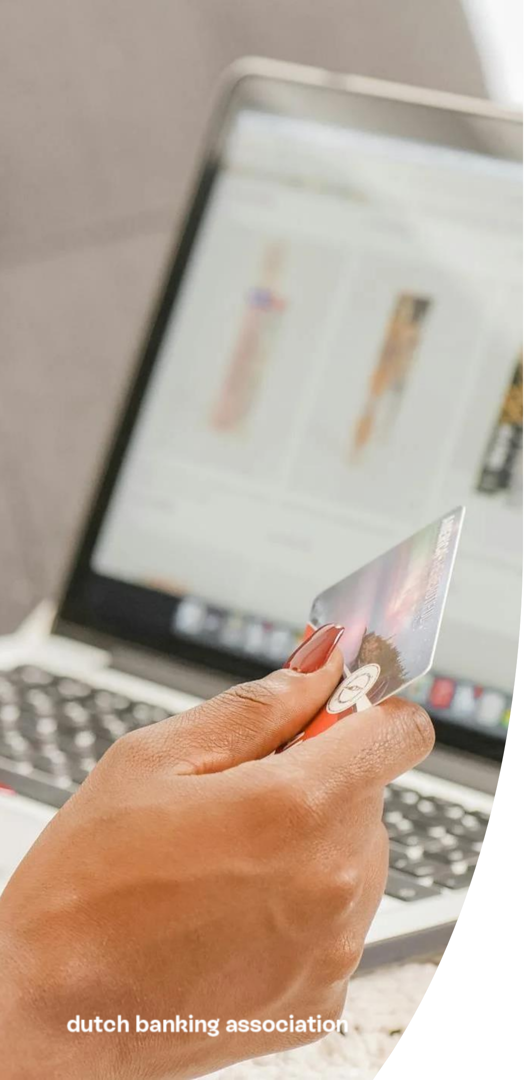
2. Fraud prevention
Cooling off period & limits (art. 51)

- We **support** the European Council’s proposal to introduce a cooling-off period (art. 51(1a)) as an effective safeguard against bank employee impersonation scams to protect all consumers. Vulnerable consumers often don’t use fraud prevention tools, banks must be able to activate this measure on their behalf. Opt-outs should not be allowed, as a one-time safeguard leaves users exposed in future transactions.

- We **support** adopting the Council’s Article 51(6). While the IPR promotes consumer autonomy by allowing immediate limit changes, it unintentionally excludes the cooling-off period and increases fraud risk. To ensure consistency and consumer protection, the PSR should take precedence over the IPR in case of conflict.

- We **support** maintaining alignment with the European Commission’s proposal regarding limit structures, (art. 51(1)). The Council’s proposal to require consumers to set multiple types of limits introduces unnecessary complexity and confusion for users, which ultimately undermines effective fraud prevention. Instead, banks should have the flexibility to design appropriate limit structures based on their own risk assessments.





3. Liability

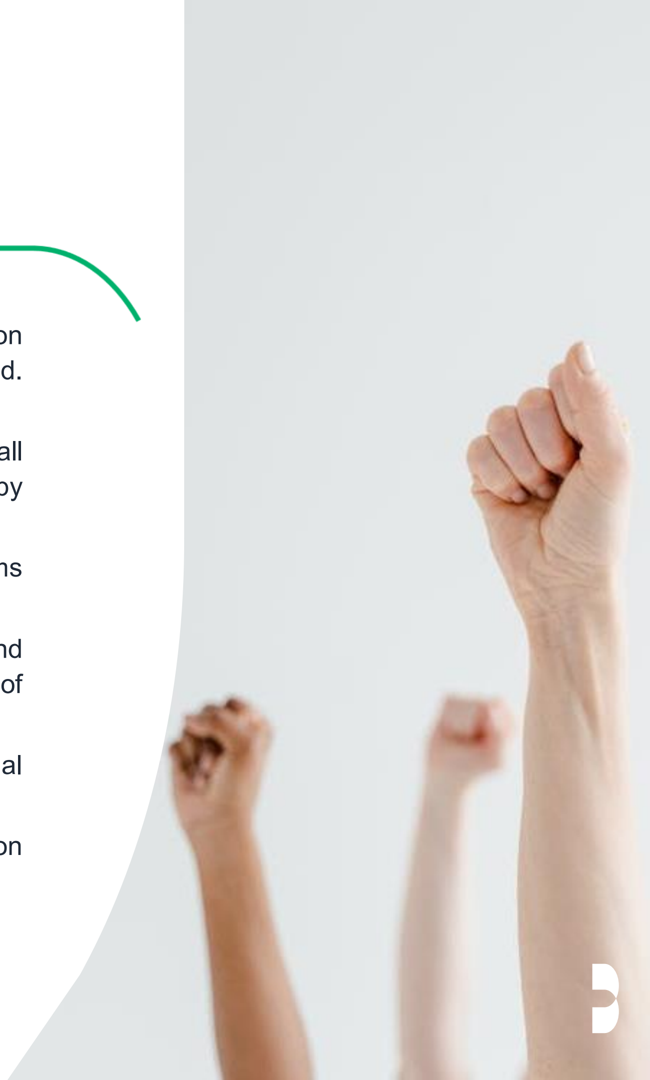
Impersonation scams (art. 59) & authorisation (art.3)

- (Art. 59) We **support** the proposals put forward by the Commission and the Council with regards to the compensation framework. We are committed to reimbursing bank employee impersonation scams, recognizing the impact these scams have on consumer trust and integrity of the banking sector. However, proposals that go beyond this specific type of fraud are, in our view, disproportionate and risk encouraging criminal abuse, moral hazard, and potentially higher costs for all customers.
- (Art. 3) We **strongly support** keeping an **objective** definition for authorisation, rejecting the Parliament's proposed art. 3(34a). Introducing subjective factors such as 'the payer's intent', or 'the payer's full knowledge of all relevant facts' would undermine legal certainty, make payments reversible, and expose banks to liability without a verifiable basis for customer consent. We believe this shift does not serve the objectives of the PSR.

4. Shared responsibilities

The role of online platforms & ECSPs (art. 59)

- It is essential that all actors within the fraud ecosystem, including all electronic communication service providers (ECSPs), implement both individual and coordinated measures to combat fraud. After all, it takes a network to defeat a network.
- It is, therefore, important that the PSR ensures both individual and collective responsibilities of all relevant actors in the fraud ecosystem, and avoids unintentionally creating a legal imbalance by assigning disproportionate responsibility and liability to a single party within the fraud chain.
- We **strongly support** the European Parliament's recognition of the role played by online platforms and ECSPs, as reflected in the proposed obligations:
  - ECSPs would be required to reimburse banks for bank employee impersonation scams and unauthorised payments if they fail to remove fraudulent or illegal content after being informed of its occurrence.
  - ECSPs are expected to take an active role in fraud prevention by implementing educational initiatives that better inform and protect their customers.
  - Banks, ECSPs, and digital platform service providers should establish robust fraud prevention and mitigation techniques to combat all forms of fraud.



dutch banking association

Gustav Mahlerplein 29-35
1082 MS Amsterdam
The Netherlands

www.nvb.nl