Card Payment Sweden's Position on Payment Services Regulation Trilogue Negotiations

26 September 2025

Card Payment Sweden (CPS) is an industry association that promotes the use of cashless payments by card in Sweden and in the Nordics. CPS was established in 2017 by card acquirers and card issuers in the Swedish market. We aim to ensure that card payments are made securely, efficiently, and in a commercially viable way.

The significant use of cards has earned Sweden the reputation of having one of the world's most efficient payment markets. CPS strives to ensure that the regulatory framework in Sweden and the EU works effectively, facilitating fair competition among the different payment solutions.

Card Payment Sweden supports efforts to harmonise payment rules in the EU with the Payment Services Regulation (PSR). With the trilogues having begun in July, we have identified a number of points that require clarification during the discussions to ensure that the PSR is workable and fulfils its stated objectives of enhancing payment regulation in Europe and providing harmonised rules for the benefit of consumers and the competitiveness of payment actors.

Policy asks:

1. **Clarify the definition of payment accounts in relation to credit cards.**
2. **Explicitly exclude payments initiated by or through the payee (i.e. direct debits and card-based payments) from the scope of payment initiation services.**
3. **Avoid requiring two merchant names in the payment information, which would demand costly infrastructure updates without benefiting users.**
4. **Ensure fraud prevention measures are outcome-focused, particularly regarding spending limits and cooling-off periods.**
5. **Adopt harmonised rules on surcharging.**
6. **Avoid subjective criteria in the definition of authorisation.**
7. **Allow realistic investigation timeframes for cardholder fraud to ensure fair outcomes.**
8. **Adopt proportionate and balanced administrative fines.**
9. **Ensure the application of SCA and exemptions are always a decision left to the PSP of the payer.**
10. **Avoid dilution of what SCA means: SCA should consist of two factors of different categories. Behavioural and environmental elements are not inherence.**

1. Clarify the definition of payment accounts in relation to credit cards.

The issue

Previous European payments rules (PSD1 and PSD2) did not clarify whether credit card accounts qualify as payment accounts. Certain Member States, such as Sweden and Finland, treat them as payment accounts, while others do not – creating regulatory fragmentation across the European Union (EU).

The new definition of "payment account" in Article 3.15, in our view, clearly includes credit card accounts.[1] Indeed, credit cards support both outgoing and incoming transactions (e.g. consumer payments to merchants, refunds, gambling payouts, or card-to-card transfers). These functions are embedded in the card infrastructure and apply equally to debit and credit cards. As such, card payments fit the category of "daily payment transactions" referred to in Recital (20), without the need for further case-by-case consideration.

Nevertheless, Recital (20), does not provide sufficient clarity on the definition of payment accounts in relation to credit cards. Particularly with the Council's additions stating that *"in certain cases, such as that of credit card accounts […] a case-by-case analysis should be carried out to determine whether it possesses those characteristics"*, the text introduces even greater uncertainty. A single EU-wide interpretation is needed, as the Council text would leave credit card accounts undefined and market participants uncertain.

The impact

If credit card accounts are not defined as payment accounts, key PSR requirements and definitions would no longer apply to credit card payments. Since no other account substitutes as the payment account, such transactions would effectively occur without a payment account. This raises issues for areas such as merchant-initiated transactions (MITs)[2], transaction monitoring[3], agreement on consent[4] and potentially others.

> **Policy ask:**
>
> **To avoid confusion, we urge negotiators to maintain the Council provision on Recital (20) while explicitly clarifying that credit card accounts are payment accounts and that card-based payments are not eligible for payment initiation services (PIS). This ensures consistency, harmonisation, and legal certainty across all Member States.**

---

[1] Article 3.15: *"an account held by a payment service provider in the name of one or more payment service users which is used for the execution of one or more payment transactions and allows for sending and receiving funds to and from third parties"*

[2] Definition (17) "*mandate*" in Article 3 refers to "*debiting the payer's specified payment account*". For card MITs the mandate is for debiting a payment card (PAN) rather than an account (IBAN). Even though for debit cards a bank account is ultimately debited, the actual bank account is not known to the payee. For credit cards the card number (PAN) is the only reference, also used as reference for the payer to access his/her credit card account with the card issuer.

[3] Article 83.2 refers to payment account, both in the beginning and in 83.2(b). Without defining credit card accounts as payment accounts, transaction monitoring of credit card payments would be made impossible by PSR.

[4] Council's Recital (69b) refers to "*the payer has given its consent for the execution of the payment transaction in a manner agreed on between the payer and the account servicing payment service provider*". For a card payment such agreement must be made between the cardholder and the card issuer, which is the payer's PSP and also is the ASPSP if the credit card account is a payment account. If the credit card account is not a payment account, there is no account servicing payment service provider, and no such agreement on the manner of how consent is provided can be made.

As such, we recommend adopting Recital (20) with the following amendments : *"Any account that possesses those characteristics should be considered a payment account and should be accessed for the provision of payment initiation and account information services. <u>This also includes credit card accounts, although card-based payments being initiated by or through the payee are not eligible for payment initiation services.</u> In certain cases, ~~such as that of credit card accounts or~~ where the account is used only for the execution of one transaction, a case-by-case analysis should be carried out to determine whether it possesses those characteristics. [...]"*

2. Explicitly exclude payments initiated by or through the payee (i.e. direct debits and card-based payments) from the scope of payment initiation services.

The issue:
Payment initiation services (PIS) are defined by Recital (54) as services that allow a user to initiate a payment from their account, such as a credit transfer or direct debit, without using a traditional payment instrument like a card. The Council mandate further clarifies that PIS requires the payer's mandate to access their account, meaning the service is legally provided to the payer. At the same time, some PIS may also establish a relationship with the payee, reflecting that, in practice, providers can serve both the payer and, in certain cases, the payee.

For those outside the payments industry, this distinction can seem confusing. In practice, the merchant benefits most from a PIS because it guarantees they will receive the payment, similarly to a card transaction. So commercially, the merchant is the main customer, but the service provided to this customer is a payment guarantee service, not a payment initiation service. Legally, the actual payment initiation service is provided to the person making the payment (the payer), because they are the one authorising the transaction.

Why direct debits and card-based payments should not be considered in scope for payment initiation services.
PIS for direct debits are not relevant, as they are, by definition, initiated by the payee with the payer's prior consent. The purpose introducing payment initiation services in PSD2 was to let merchants accept credit transfers as payment on their websites or other points-of-interaction, even if the payment is processed later. Without PIS, merchants have no payment guarantee and may not want to deliver the goods or services. PIS provides this guarantee by allowing the payer to initiate the payment through the Payment Initiation Service Provider's (PISP) connection to the payer's bank (i.e. Account Servicing Payment Service Provider - ASPSP).

PIS should not apply to direct debits, as these are initiated by the payee with the payer's prior consent. The direct debit mandate gives the payee the right to initiate the payment. There is therefore no need for an additional guarantee that the payment will be executed. However, the payer of a direct debit has an unconditional right to a refund within 8 weeks (Article 62) without any guarantee for the payee that the payer will not exercise their right to do so.

Likewise, and in connection to the previous point on credit card accounts being payment accounts, PIS is equally inapplicable to card-based payments which are initiated by or through the payee[5]. Since the card payment is initiated on the merchant's point-of-sale (POS) terminal or website checkout, and not through the payer's PSP's online or mobile banking channels, the ASPSP has no interface for the cardholder to initiate the payment directly. Furthermore, as the payment guarantee is provided by the acquirer to the merchant, and indirectly by the issuer, there is no need for an additional service to provide this.

Policy ask:

The PSR should ensure that PIS applies only to credit transfers. This approach would preserve legal clarity as well as clarity for end-users. CPS therefore supports the Council position, removing "*direct debits*" in Article 36.4(a) and the subsequent changes in Recitals (54) and (59). Furthermore, Recitals (54), (59) and (20) must clarify that that card-based payments are not in scope of PIS either.

3. Avoid requiring two merchant names in the payment information, which would demand costly infrastructure updates without benefiting users.

The issue:
Article 25.1(a) of the PSR requires payment information to be provided, enabling the payer to identify the transaction and the payee. The Commission and Parliament's positions propose that this information include the payee's commercial trade name. However, the Council put forward a different wording stipulating that the legal name of the payee should also be provided.

The impact:
Currently, card payment infrastructure only supports the disclosure of one merchant name per transaction, which under international card scheme rules must be the merchant's commercial trade name. Responsibility for providing accurate information lies with the acquirer (the payee's PSP), while issuers can only transmit the information they have received. Most cardholders recognise their transactions, but merchant names could be clearer and more consistent. Holding acquirers accountable and strengthening scheme oversight would improve transparency, reduce confusion, and boost trust in card payments.

The merchant's name, along with other required information, helps the payer recognize the transaction on their statement as a payment they initiated or given their consent to. For this purpose, the name of the payee provided must be the commercial trade name of the merchant, not a legal name of a company group or similar. In case a cardholder does not recognize the payment and wants to dispute it as unauthorised, they must contact their card issuer, which reimburses the cardholder and initiates a chargeback of the original card payment towards the acquirer, which has all the information needed on the merchant. The legal name on a statement therefore does not contribute to resolving disputes. If a cardholder wants to contest a payment for

---

[5] Most card-based payments are initiated by the payer through the payee, i.e. by the cardholder by using his card at the POS or website of the merchant. MIT card payments are, like direct debits, initiated by the payee based on a previous mandate from the payer. Both are therefore pull payments and not eligible for PIS as the payer is not in direct contact with his PSP at the time of payment initiation.

other reasons after purchase, the buyer needs a full receipt or invoice showing what was purchased and the terms of the purchase.

Since the technical infrastructure does not currently support including two names in payment messages, requiring both names would demand costly changes for issuers, acquirers, merchants, and card schemes, with no benefits to consumers.

Policy ask:

CPS urges negotiators to reject the Council amendments to Article 25.1(a), which include the requirement to provide the payee's legal name where available, in addition to the commercial trade name.

4. Ensure fraud prevention measures are outcome-focused, particularly regarding spending limits and cooling-off periods.

The issue:
Articles 51.1(a), 51.1(b) and 51.1(c) of the Council general approach introduces rules on spending limits and cooling-off periods. Spending limits set maximum amounts that consumers can transfer or spend within a period, while cooling-off periods impose waiting times before new payment services or devices can be used. These measures aim to reduce fraud.

While such measures can absolutely be effective in combatting fraud, their use should not be detailed at this level in legislation. It must be up to the PSPs to apply them where appropriate, in combination with other fraud combatting measures. Different measures might prove more or less effective for different payment means and products, different customers and at different points in time.

CPS strongly believes that fraud prevention should focus on outcomes so as not to restrict the emergence of new tools. Fraud patterns, customer behaviour, and payment methods will evolve over the lifetime of the PSR. PSPs have the expertise to adapt their safeguards to specific risks, such as customer type, transaction size, and payment method.

The impact:
The Council's approach risks harming consumers. For example, if a commuter installs a new app to pay for public transport or parking but must wait several hours before using it, this creates unnecessary delays without reducing the risk of fraud. In addition, low-value, everyday payments such as instant app-based transfers have different risks from large invoice payments, and a one-size-fits-all rule is not appropriate.

Policy ask:

Spending limits and cooling-off periods should be set by PSPs, not mandated in the PSR. This flexibility is essential to ensure fraud prevention remains effective and proportionate and does not restrict user friendliness. We therefore recommend adopting the Commission's draft text on Article 51.1. Additionally, we advocate for the removal of the Articles 51.1(a), 51.1(b) and 51.1(c), leaving PSPs room to adapt their fraud prevention as appropriate for each case and as technologies evolve.

5. Adopt harmonised rules on surcharging.

The issue:
Surcharging means charging the customer an extra fee for using a specific payment method, such as a card. Under the Council mandate (Articles 28.3–28.6), surcharging would be banned for credit transfers and direct debits in all currencies, as well as for consumer cards with capped interchange fees in the Interchange Fee Regulation (IFR). However, commercial card payments would remain an exception, with each Member State free to decide whether to allow surcharges or not.

The impact:
This approach creates uneven rules across the EU/EEA. For example, some countries, such as Sweden, already ban all surcharging, including for commercial cards, while others still allow it. In this context, cardholders and merchants face different rules depending on where the payment takes place. A person travelling across the EU/EEA could pay no surcharge in one country but face additional fees in another. This undermines the goal of harmonisation, at the core of the PSR, and creates confusion for consumers and businesses.

Policy ask:

To achieve a single, consistent set of rules across the EU/EEA, negotiators should adopt the Parliament's proposal on Article 28.3. This would simplify the system, avoid unfair treatment of cardholders, and remove unnecessary complexity.

6. Avoid subjective criteria in the definition of authorisation.

The issue:
Decisions on whether a transaction is authorised or not should be based on objective criteria. However, the Parliament introduces subjective elements, including the payment service user's "*knowledge of all relevant facts*" (definition 34a, Article 3). Instead, authorisation should rely on the consent terms agreed between the payment service provider and the payment service user in the framework contract.

This point is not entirely clear in Articles 49.1, 49.5, and 49.6, but it is clarified by Council Recital (69b). However, this explanation risks leaving out credit card payments, if credit card accounts are not clearly defined as payment accounts, as it refers to "*a manner agreed on between the payer and the account servicing* *payment service provider"*. In such a case, the card issuer would not qualify as an account servicing payment service provider but only as a payment service provider.

The impact:
Basing payment authorisation solely on the payer's stated belief at the time of consent would significantly weaken safeguards against fraud. It would remove the obligation on users to exercise due care, leading to a sharp increase in fraudulent transactions. This would raise costs for financial institutions and consumers alike, while creating further opportunities for organised crime and terrorist financing.

> **Policy ask:**
>
> **CPS recommends keeping an objective approach to payment authorisation. We therefore call on <u>negotiators to reject the Parliament's proposed definition (34a) in Article 3 and adopt the Council's Recital (69b)</u> (where *"account servicing"* should be deleted in order for the provision to also include authorisation of payments without payment accounts). Furthermore, CPS supports the Council position to use the term *"consent"* as in PSD2, and not introduce the parallel term *"permission"* as proposed by the Commission and the Parliament.**

7. Allow realistic investigation timeframes for cardholder fraud to ensure fair outcomes.

The issue:
Article 56 sets investigation timeframes for cases where the payment service provider suspects that the payer (for a card payment: the cardholder) is the fraudster. The Commission proposal sets this at 10 business days, while the Parliament and Council amend it to 14 and 15 business days respectively. We believe even the longer period of 15 days is often too short to conduct a thorough and effective investigation. This is because assessing each case requires background material, including documents and communications between the payer and payee, which usually takes more time to obtain.

The impact:
Properly reviewing these cases requires gathering information from multiple parties, which cannot realistically be completed within such a limited timeframe. While Article 56 addresses some related issues, the proposed deadlines risk compromising the quality of investigations and may lead to unfair outcomes for genuine cardholders.

> **Policy ask:**
>
> **<u>By default, CPS supports the Council's longer 15-day limit,</u> but stresses that, in practice, it would be insufficient for most cases. CPS supports this timeframe only as the absolute minimum and urges policymakers to consider more flexible or extended deadlines in future provisions. This approach would better align with the experience of other European issuers and ensures a fair balance between speed and thoroughness in protecting consumers, whilst maintaining trust in the payment system.**

8. Adopt proportionate and balanced administrative fines.

The issue:
The European Commission, under Article 97(a) proposed that infringements under the PSR could lead to fines of up to 10% of annual turnover for legal persons and EUR 5 million for natural persons. The Council supports this approach. The Parliament mandates on the PSR proposes lower thresholds, 7.5% of turnover for legal persons, EUR 2.75 million for natural persons, and fines of up to twice the profits gained from a breach. These levels remain extremely high.

The impact:
Such penalties would particularly harm small and mid-sized payment service providers, discouraging innovation and limiting consumer choice. A fine of several million euros could easily force a growing PSP out of the market.

> **Policy ask:**
>
> **We call on negotiators to adopt the Parliament's lower levels in Article 97(a), but we continue to advocate for more proportionate sanctions.**

9. Ensure that the application of SCA and exemptions are always a decision left to the PSP of the payer.

The issue
Article 85 sets out the requirements for payment service providers (PSPs) to apply Strong Customer Authentication (SCA). Article 85.1 of the Parliament's draft text adds that the application of SCA is made "*on the basis of the risk assessment carried out under the transaction monitoring mechanism as set out in Article 83*".

While risk-based monitoring already plays an important role in card issuer authorisations, the Parliament's wording creates a risk of misinterpretation. It could be read as requiring all PSPs to apply risk-based SCA exemptions for all payment use cases, rather than leaving it to the payer's PSP to determine if and when such exemptions are appropriate. However, applying SCA should be for the PSP of the payer only – not anybody else, including schemes.

The impact
SCA is a powerful tool for fighting fraud. While it cannot fully prevent the growing social manipulation fraud threat, this does not justify weakening SCA requirements, which are already in effect. Exemptions should remain a temporary measure to balance security and convenience during the transition.

The ultimate goal is to make SCA so seamless that exemptions are no longer needed, ensuring all payer-initiated transactions are secured. In such a situation, end-users do not see SCA as an obstacle to make a payment, rather it makes them feel more secure in initiating the payment. CPS does not support the idea of exemptions being forced by law on payment solutions where it is not needed.

Policy ask:

CPS advocates for the Commission's proposal in Article 85.1 and Article 83.1(a), thus rejecting the Parliament's amendments. Furthermore, CPS advocates against the inclusion of Recital (107a) put forward by the Parliament.

Additionally, CPS calls for the following addition by the Council to Article 83.9(c) to be adopted in the PSR: *"Exemptions from the application of strong customer authentication shall not be mandatory. A payment service provider implementing an exemption always retains the right to decide that under the circumstances, strong customer authentication is necessary."*

10. Avoid dilution of what SCA means: SCA should consist of two factors of different categories. Behavioural and environmental elements are not inherence.

The issue

There are two significant changes proposed to SCA. First, to allow the SCA factors to be of the same category and, secondly, to allow environmental and behavioural characteristics to constitute the inherence factor. These changes would significantly weaken the safeguards SCA provides and could undermine its core purpose to protect consumers and businesses from unauthorised fraud.

Allowing both factors in two-factor SCA to come from the same category, as proposed by both the Commission and the Parliament (article 85.10), would weaken the robustness of SCA and create room for differing interpretations. The Parliament's mandate added that *"The independence of the elements shall at all times be fully preserved and the authentication procedure shall at all times ensure a high level of security."* However, it remains very unclear how this requirement would be applied in practice or what it would mean for enforcement.

Moreover, the Parliament has also added a new paragraph to Article 85.12, stating that the *inherence* element of SCA may include environmental and behavioural characteristics for example, the user's location, the time of the transaction, or the type of device being used.

Apart from leading to interpretation issues and weakened SCA protection against fraud, both of these proposals moves borderline between payer and PSP liability for fraudulent transactions, in the direction of the payer. I.e. payers would to a larger extent be held liable for unauthorised transactions, that today results from exemptions to SCA but with these proposals would be defined as transactions performed with SCA.

The impact:
Any weakening of SCA is directly at odds with its fundamental purpose to combat fraud. A major impact of moving the borderline for what is considered SCA and what is not, is moving the space for which the consumer is protected from standing the risk of paying for unauthorised payments.

Article 60.2 in PSR (article 74.2 in PSD2) states that the payer shall not bear any liability, when either of the payment service providers applies an allowed exemption from SCA. The actual use cases these proposals to dilute the definition of SCA in PSR is trying to address, where there are mitigating circumstances which reasonably should lower the need for SCA, either already are or should be covered by allowed exemptions from SCA. To allow such mitigating circumstances to instead be defined as SCA, would only result in the use case moving a use case which is allowed but defined as an exemption from SCA, to be defined as SCA and therefore introducing the possibility of holding the payer liable for the unauthorised transaction.

The idea of allowing behavioural and environmental elements as an inherence factor, is a perfect example of this: There is already an exemption, Transaction Risk Analysis – TRA (articles 18-20 in current RTS on SCA), which takes into consideration such environmental and behavioural characteristics for a decision on whether the individual purchase seems to fit with the payer's "normal" location, time, device, spending patterns etc. or making purchases, in which case the probability this is fraudulent is lower and SCA can be exempted. But this is not the same as saying the customer could unequivocally be identified. What happens then when the customer is actually doing a purchase that is not consistent with his previous behaviour when it comes to location, time, device and/or spending? As this cannot reasonably result in a full stop, failed SCA and transaction being declined, this situation would with all likelihood result in reverting to asking the payer to authenticate with a standard, true SCA method. Which is the same logic already applied for the TRA exemption. So this use of environmental and behavioural elements in a risk-based approach to application of SCA already exists today; the only actual difference with the Parliament proposal is that the payer comes into a worse liability position as compared with today.

To illustrate this with an example. If the physical card (but not the PIN nor any other authentication factor) is stolen from its owner (but not the PIN or any other authentication factor), and the fraudster uses this card to make purchases in the same locations and the same stores as the legitimate cardholder use to visit, the Parliament proposal would make it possible for the PSP to deem this as SCA: a possession factor (the card) used together with an inherence factor (location as environmental/behavioural element), and hold the cardholder liable for the purchases. In CPS's view, this is unreasonable.

Likewise, allowing both factors to be drawn from the same category undermines the principle of independence between factors. As mentioned above, there could certainly be use cases which resembles use of two factors from the same category, for which exemptions to SCA should be allowed instead of defining them as SCA, in order not to move the liability border away from the PSP and in direction of the payer. E.g. where the possession of some object might be a mitigating circumstance that for certain use cases relating to this object would lessen the need for actual SCA.

One such example is electrical vehicle charging, for which there is unfortunately no exemption today, although there is one for the close and many times dependent use case of parking. The possession of the car to be charged (provided the car is previously connected to the payment instrument being used for payment of the charging) should be such a mitigating circumstance that should allow for an exemption from SCA in the revised RTS on SCA.

Policy ask:

CPS supports the Council position on Article 85.10 and advocates for the rejection of the Parliament amendment on Article 85.12 (i.e. " ***The inherence element of strong customer authentication may include environmental and behavioural characteristics such as those related to the location of the payment service user, the time when the transaction occurs or the device being used."*)