ACCIE
Association of Credit Card Issuers Europe

Position on the review of the Payment Services Directive

The Association of Credit Card Issuers Europe (ACCIE) represents the specialised European credit card issuing industry in the European and national legislative processes. ACCIE's mission is to ensure that cardholders across Europe gain optimal benefit from the credit card payment instruments offered by its members.

ACCIE welcomes the review of the PSD2 as the payment market has undergone significant changes since the introduction of the Directive in 2015. The PSD2 introduced the ground-breaking framework of Open Banking and helpful instruments such as Strong Customer Authentication (SCA) and Application Programming Interfaces (APIs) which effectively increased competition and the amount of customer data accessible by industry players, along with safer payment methods for consumers. However, the PSD2 is no longer a good fit for the payments market which has undergone significant shifts, notably with the arrival of new players and the acceleration of digitisation in response to the Covid-19 crisis. ACCIE believes the review of the PSD2 should be both ambitious and proportionate, and therefore calls on the European Commission to take into account the new players in the payments market, reduce compliance costs without undermining the effectiveness of the Directive, and tackle the remaining issues on SCA and new fraud patterns. In annexe to this position paper, ACCIE members have provided examples of business use-cases covered by PSD2 where issues remain.

Future-proofing the Directive

In the fast-paced payments environment, European legislation should particularly take into account the future entrance to the market of innovative solutions. In the context of PSD2, this means first paying attention to its cohesion with other EU legislation, and second, striking the right balance between legislation and market-driven innovation.

Certain tensions exist between PSD2 obligations and data restrictions under the General Data Protection Regulation (GDPR). Indeed, when a consumer grants access to details in a payment account, access to details of other parties involved in the transactions on that account is also granted, which is not permitted under the GDPR. ACCIE calls for clarity on where liability lies in such cases, as issuers are usually mandated to provide consumer data during a transaction with a third party. Furthermore, the advertising of payment services and standardisation of contractual information for credit cards are already regulated under the Consumer Credit Directive. It is essential that, if such aspects are to be regulated under PSD3, credit cards should be exempted.

New market entrants such as FinTechs and BigTechs are underregulated as compared to traditional payment market players. In addition, traditional market players must often invest in updating their IT and legacy systems to comply with new regulations not applicable to newcomers, which they will benefit from (e.g. through APIs), therefore creating unfair competition that jeopardises innovation from traditional players. ACCIE calls for the same requirements to be set on all recently emerged newcomers – as well as those emerging in the coming years – and a balance should be found between regulation and market-driven innovation.

Finally, ACCIE is in favour of granting specific investigatory powers to National Competent Authorities to detect breaches of rules, enhancing the harmonisation of the Directive, while respecting the specificities of national markets. This would ensure a safer and more secure payment system for consumers and businesses.

ACCIE represents the European credit card issuers to policy-makers in Europe. The members of ACCIE provide services to over 21 million cardholders in 12 EU Member States.

For more information, please contact the ACCIE Secretariat via contact@accie.eu

Costs of compliance

The introduction of SCA has provided additional layers of security for consumers and payment service providers for mitigating cyberattack risks and issues. However, issuers have faced an increased burden and resource investment in supporting integration requests and technical issues from third parties using issuers' APIs. This has resulted in higher costs in terms of development and maintenance that are not always proportional to returns. Furthermore, fraud reporting has proven burdensome, especially since new fraud patterns appeared. ACCIE would like to point out that APIs can potentially be a weak point in terms of security (e.g. DDoS attacks[1]) if not properly managed. ACCIE calls for the review of the PSD2 to focus on reducing compliance costs without undermining the effectiveness of the Directive and also to include the management of disputes.

Strong Customer Authentication

ACCIE welcomed the introduction of SCA, but issues remain when setting limits. Due to the additional friction at checkout and the consequent volume loss for issuers, merchants and acquirers, the benefits related to SCA did not match or cover the costs of its implementation. For example, current regulation on SCA does not reflect the complexity of the travel ecosystem where credit cards are predominant. Furthermore, ACCIE notes that little to no enforcement measures are being taken in cases where merchants are not compliant. In addition, the current exemptions result in only a minority of transactions actually using SCA, furthermore, the technical realities of SCA implementation (i.e. via the Merchant Initiated Transaction Dummy Trace ID) allow circumvention and result in only a fraction of transactions properly using it. Thus, ACCIE believes that the application of SCA should be better implemented and monitored to ensure a level playing field among payment methods.

For contactless payments, payment service users should be able to set their own limit and the allowed limit should be higher than €150, following countries such as Switzerland where the thresholds for contactless payments were pushed further without any rise in fraud.

Information transparency and data sharing

Following the successful introduction of Open Banking, ACCIE sees great potential in data sharing and calls for access to and use of payment accounts data to be extended to other accounts within the banking sector. This would create an opportunity for issuers to access other financial data (e.g. other loans, income, etc.), necessary for fulfilling legislative requirements such as the Creditworthiness Agreement and Anti-Money Laundering measures. However, if access to such data is opened up to lesser-regulated market players, concerns would be raised over the security of such data. Because, if not adequately managed, automated processing risks leaving payment service providers unaware of why certain customer applications are approved/denied and can lead to the loss of direct contact with the end consumer. Lessons can be drawn from the situation in the United States, when credit data became more broadly available, customers began to be assessed on this information and were viewed as a credit rating rather than holistically, leading certain players to artificially maintain a credit rating in order to get access to services which can be discriminatory. ACCIE believes that data sharing should be balanced with the need to maintain a human customer relationship.

[1] Distributed denial-of-service

Annexe: use cases on PSD2

Several use-cases brought up by ACCIE members are echoing the European Banking Authority's response to the Call for advice on the review of the PSD2 that was published on 23 June 2022.

Strong Customer Authentication: high decline rates

1. Acquirers are not sending valid trace IDs

When it comes to the handling of (initial) recurring or Merchant Initiated Transaction (MIT) authorisations, many acquirers are still not ready with the relevant SCA setup in the authorisation message. Moreover, trace IDs are not correctly applied, and issuers face cases where dummy trace IDs or no trace IDs at all in MIT authorizations are used. This leads to issuers rejecting authorisation requests as not in compliance with the RTS. This further results in an increased number of declines and, eventually, growing customer dissatisfaction. As just one example, an ACCIE member noted approximately 2000 authorisation requests declined per day in May 2022 (including soft declines) due to the wrong settings in the authorisation message. In February 2022, Mastercard also highlighted the same issue in its publication "EMV 3DS & PSD2 SCA: Optimization opportunities".

2. Business case: Substitute in a purchase order

Regarding online shopping (mainly groceries), when a merchant makes substitutes to the original order (e.g. a substitute product if the original item is not available) that are higher in price, this results in soft declines due to an amount deviation in authentication and authorization. These transactions are frequently classified as MIT, and, as interaction with the user is limited to none, the authentication process cannot be performed if the transaction is soft declined due to amount deviation.
Furthermore, issuers observe a difference in rules across different regulatory authorities. E.g. FCA UK allows 20% amount deviation between Authentication and Authorization whereas (at least some) other regulators in the EU do not allow any amount deviation. The EBA recently proposed that the revision of the PSD2 provides clarity on this use-case[2].

3. Merchant sending LVP SCA exemption instead of MIT

For payment transactions of amounts below €30, many merchants/acquirers send transactions using the Low-value payment (LVP) indicator, even if they could classify for MIT exemption. This is because the LVP exemption has different counters set up, such as that the maximum number of transactions should not exceed 5, and the cumulative amount must not breach the €100 threshold. Once these counters are reached, the transaction is soft declined. This can easily be avoided if an MIT exemption was sent wherever applicable, or if an acceptable threshold of an increased amount between authentication and authorisation were included in PSD2.

- **ACCIE calls for improvement on SCA, to cluster different market entities, different products, and business cases and then fine-tune SCA guidelines accordingly**

Commented [A1]: [background info]

278. Second, the provision of Article 75 of PSD2 does not address cases where the final amount of the transaction may not be known in advance and where funds are not blocked. This is particularly relevant from the perspective of the application of SCA for these transactions. Relatedly, the EBA has clarified in Q&A 5133 that 'for card-based payment transactions where the exact transaction amount is not known in advance, if the final amount is higher than the amount the payer was made aware of and agreed to when initiating the transaction, the payer's PSP shall apply SCA to the final amount of the transaction or decline the transaction. If the final amount is equal to or lower than the amount agreed, the transaction can be executed and there is no need to re-apply SCA, as the authentication code would still be valid in accordance with Article 5(3)(a) of the Delegated Regulation. This applies also to card-based payment transactions where the exact amount is not known in advance and funds are not blocked by the payer's PSP in accordance with Article 75(1) of PSD2.

279. In relation to the above, the EBA proposes that the Directive clarifies these two aspects in the Directive.

[2] Article 278-9, *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, EBA/Op/2022/06.

Strong Customer Authentication: new fraud patterns

The introduction of PSD2 forced fraudsters to change their modus operandi. Fraud losses due to account takeover or manipulation of the payer have increased as the customer is now the "weakest point" since technical security barriers have improved. Indeed, the EBA Discussion Paper on Payment Fraud Data under PSD2[3] noted that "[as] reported by issuers, the theft of card details is the most common event and represents 75 % of the value of the fraudulent SCA payments […] the authentication with SCA may not be effective in preventing such type of fraud."

As such, SCA sometimes presents customers with complicated requirements for payments, which are not always effective against the most common type of fraud reported by issuers. ACCIE believes that, as recommended by the EBA[4], more effective ways to tackle such fraud would be greater consumer empowerment, such as a notification to warn them that the PSP is not checking for IBAN and payee name match, and educational and awareness programs aimed towards consumers.

- **ACCIE calls for improvement in fraud education aimed toward consumers and for liability to fall out of the scope of consumer protection engagement in case of social engineering fraud targeted at the consumer**

The cost of data sharing

With Open Banking, safe access to data via APIs is granted free of charge to third-party service providers, which reverses all the investment costs and risks to issuers. Thus, data sharing through Open Banking and Open Finance is most valuable for consumers and third-party service providers but fails to be an attractive feature for issuers, who must also bear the costs of collection, consolidation and management of the data itself.

ACCIE believes, in line with the recent EBA proposal[5], that appropriate compensation for the cost of data sharing should be considered. ACCIE also supports the idea that the setting of an appropriate level should be market-driven.

To give an example, if a fee structure were to be introduced, the connection could be priced with a one-time fee for setup and an annual fee to contribute to the maintenance and operation on the issuer's side. Whereas regarding the data, information, and functionality accessed, it would be fair for both parties (issuers and third parties) to introduce fees based on actual usage (e.g., data volume, connection time, number of calls to the APIs). Finally, regarding the quantification of fees, one could think of a flexible price defined by each issuer, although with a reasonable, regulated maximum cap, to be defined in collaboration with European issuers.

- **ACCIE calls for a level playing field through the allowance of compensation for the development and maintenance of the API infrastructure, and the related use of data, information, and functionality through them**

Commented [A2]: [background information]

40: "Regarding remote card payments reported by issuers, the theft of card details is the most common event and represent 75 % of the value of the fraudulent SCA payments and 60 % of the value of the fraudulent non-SCA payments in H2 2020. This can be explained by fraud arising from social engineering such as phishing. In these instances, the **authentication with SCA may not be effective in preventing such type of fraud."**

341: The EBA has observed that the security requirements in PSD2 have had the desired effect since in **almost** all instances the share of fraudulent payment transactions in the total payment volume and value of transactions is significantly lower for transactions that are authenticated with SCA than those that are not.

Commented [A3]: [background information]

270: EBA recommended that a notification is sent to the customer to warn them that the PSP is NOT checking whether the IBAN and payee name match (therefore putting burden on customer).

298: (but not for inclusion here) with Instant Payments the EBA suggests informing PSUs that they are irrevocable etc, due to fraudsters targeting IPs

351: while there may not be a specific solution that could easily address the risk of social engineering fraud, the EBA proposes Introducing specific requirements in the Directive on educational and awareness programs for applicable risks, These programs could be addressed towards PSUs and focus on specific key messages rather than provision of comprehensive and detailed information. Some programs could also be addressed towards employees of PSPs

Commented [A4]: [Question]
Would that add a burden to the issuers to make this notification happen?

Commented [A5]: [Background information]

417: The costs for market participants to implement a new Open finance framework should also be carefully considered, as the cost of investing in the relevant infrastructure to share data could be very high. In particular, the cost impact on smaller entities should be carefully considered as these may more likely experience the need to recoup the cost from their customers and thus lose competitive advantage.

418: In this respect, in order to provide more incentives for financial institutions to develop high quality APIs as a foundation for Open Finance, the EBA proposes that the EC explores the possibility of leaving it to market to decide on the appropriate compensation for the use of these APIs by third parties.

[3] Article 40, *Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry*, EBA/DP/2022/01.
[4] Articles 270 and 351, *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, EBA/Op/2022/06.
[5] Articles 417-418, *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, EBA/Op/2022/06.