THE MERCHANT RISK COUNCIL

EU PSD3/PSR REVIEW

MRC Advocacy Discussion Paper – Sep 2024

Peter Bayley
peter.bayley@merchantriskcouncil.org

1. Introduction

The European Commission has announced further legislative changes to the payments regulatory framework which will apply in Europe.

As is normal for European legislation, the EU Commission set out high level principles which are discussed and agreed with the EU Parliament. Detailed guidelines are then developed (typically via the EBA) which are finally approved, and the payments industry is then required to adopt the new framework within a set time period.

This paper seeks to extract the core implications from this new legislation which is of concern to MRC merchant members.

MRC Action:

The ask from MRC Members reading this document is:

1. To review the proposals and positions and confirm whether these meet your requirements
2. Highlight any other areas of concern which this paper has not picked up, so that these can be incorporated

Any feedback, issues or questions please contact: peter.bayley@merchantriskcouncil.org

2. PSD3 Context

The Payment Services Directive (PSD) is a European regulation designed to streamline and enhance payment services across the EU.

- PSD1 laid the groundwork for non-bank entities to enter the payments sector, increased transparency on fees, advanced the Single Euro Payments Area (SEPA) initiative, and set expectations for quick reimbursement after fraud.
- PSD2 built on this, introducing roles for non-bank payment initiation and information service providers, along with Strong Customer Authentication (SCA).
- PSD3 aims to further evolve the payments landscape.

3. PSD3 and Related Regulation

The European Commission's announcements lay out broad principles, with detailed provisions to follow from the EBA.

PSD3 will handle the authorization of payment and electronic money institutions, while a new Payment Service Regulation (PSR) will cover rules and controls for Payment Service Providers (PSPs).

The Financial Data Access (FIDA) proposal extends open banking regulations beyond PSD2, ensuring consistent implementation across the EU.

As with many things in life, for new regulation, the devil is very much in the detail and the published proposals are high level. The legislative process to finalize all these directives and regulations is well underway. EU policymakers involved in negotiating the final regulations have already made important modifications. It will be important to follow negotiations closely and the MRC will adapt positioning to reflect changes during the legislative process.

Whilst many changes are proposed some significant elements of the European Commission's proposal include:

1. **Consumer Protection**: Measures which seek to further protect consumers from fraud, especially when customers are tricked into authorized transfers by impersonators. (PSR Article 59)

2. **Credit Transfers**: Expanding payee name validation requirements, ensuring consumer refunds if discrepancies aren't flagged. (PSR Article 57)

3. **Data Sharing**: Provisions for sharing payment fraud data among payment services providers to enhance transparency and risk management. (PSR Article 83)

4. **Payment System Access**: Extending access for non-bank providers to EU payment systems, focusing on specific domestic schemes. (PSR Article 31)

5. **Open Banking and Data Sharing (FIDA)**: Extending data sharing to more financial players to foster innovation and competition. (FIDA Proposal 2)

6. **Refunds**: The regulation aims to align the treatment of card Merchant Initiated transactions (MITs) and direct debits (Article 62)

7. **Spending Limits**: PSD2 allowed a payer to set a spending limit for a card. This article now proposes that a default "low spending limit" must be applied (article 51)

8. **Strong Customer Authentication (SCA)**: Current SCA regulations deemed successful and likely unchanged, with clarifications on the use of elements from the same category. (PSR Article 85)

4. Potential Areas of concern

The remainder of this paper looks at potential areas of member concern, with each page setting out the high-level issue, an extract from the regulation (as far as is viable) and comments re impact and potential positioning.

5. Online platforms liable for fraud

In summary:
Article 59 creates requirements for electronic service providers to remove fraudulent or illegal content and imposes liability where this does not occur

Proposal text:

- 5...If the electronic communications service providers do not remove the fraudulent or illegal content, after being informed of its occurrence, they shall refund the payment service provider the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without any delay, reported the fraud to the police and notified its payment service provider.

- 5a. Electronic communications service providers shall have in place all necessary educational measures...when new forms of online scams emerge...

- 5b. ... Payment service providers, electronic communications service providers and digital platform service providers shall have in place fraud prevention and mitigation techniques to fight fraud in all its configurations, including non-authorised and authorised push payment fraud.

Implications:
This requirement would impose significant new responsibilities on merchants and marketplaces in the notoriously difficult area of content curation, with obligations to reimburse payment services providers for compensation provided to fraud victims in case of failure to remove the content.

This is likely to impact merchants who run and/or utilize marketplaces as claims of fraud / illegality would likely require a timely action. Timescales and process are currently unclear.

Proposed Merchant/MRC positioning:
Whilst the requirement to reduce the opportunities for fraud and fraudsters is always desirable, there is a need for standards and process around any control process to ensure a robust and sensible take down control.
As such, formalizing the provision of educational material and robust fraud prevention and mitigation controls (both already typically in place) is supported.

However, as the wording is currently stated, any claim that an item is fraudulent or illegal would

necessitate the item's removal from sale whilst the claim would appear to require no evidence from the informant. Given that a failure to take down the content could lead to substantial liability being imposed, merchants are strongly incentivized to remove any content on notification (regardless of merit).

This creates a huge incentive for false claims, as well as the possibility of malicious claims to disrupt a legitimate business.

It would be also equally challenging to allocate proportionate liability to the different actors involved. We'd further note that online platforms are already subject to legal regimes, such as the EU Digital Services Act, that impose obligations around the removal of harmful content, including those related to fraud and scams. In light of this, we believe a liability regime contemplated under article 59 would be unworkable and harmful to participants in the commercial ecosystem.

Merchants and service providers would ask that the control model is described in further detail, and explain proposed:

- minimum standards for substantiation and detail of claims that argue an item, content or advertisement is illegal / fraudulent and an established process for issuing claims
- timelines for validation and assessment on receipt of such a claim
- provisions which clarify how a claim should be allocated between parties
- processes for repudiating claims
- in what circumstances claim limit caps which would apply
- processes for the revocation/dispute mechanism in case there is a false claim.
- opportunities for an independent arbitration route, where a claim cannot be sensibly agreed (or similar)
- protections from false and mischievous claims

MRC would also request confirmation that this element only operates for situations where both buyer and seller are within the Europe Economic Area and for a model that is consistent across member states

The MRC and its members would be happy to assist in defining, assessing and testing any proposed model

6. Refunds

In summary:
The regulation aims to align the treatment of card Merchant Initiated transactions (MITs) and direct debits. This provision will give consumers the same "no questions asked" refund right for MITs as they have today for SEPA Direct Debits.

Proposal text:

- Article 62
  ...for authorised payment transactions which were initiated by a payee...the payer shall have an unconditional right to a refund within the time limits laid down in Article 63...

- Article 63
  The payer may request the refund ... of an authorised payment transaction initiated by or through a payee for a period of 8 weeks from the date on which the funds were debited. Within 10 business days of receiving a request for a refund, the payment service provider shall do either of the following:
  (a) refund the full amount of the payment transaction;
  (b) provide a justification for refusing the refund...The payment service provider's right under the first subparagraph of this paragraph to refuse the refund shall not apply in the case set

Implications:
In recent years merchants have increasingly recognized the problem that uncontrolled consumer protection can provide, with a huge growth in first party fraud which has created for some merchant sectors significant losses.

Card schemes have increasingly acknowledged this issue and increasingly enhanced services to balance first party fraud claims from customers and enforce relevant dispute/chargeback rights. Moreover, card payments are subject to interchange fees that compensate ecosystem participants for underwriting fraud risk; direct debit transactions do not involve such fees.

This change would invalidate many of these controls, open merchants with regular payments to a significant pre-payment risk and likely result in significant changes to the service offerings to consumers.

Proposed Merchant/MRC positioning:
MRC is firmly opposed to the extension of the direct debit liability model to card payments.

Our members have tested direct debit payments in Europe and have, to a large degree, found that the direct debit liability model is open to misuse and first party fraud.

Question: Do any MRC merchants have evidence to support this claim? The statement above is based on anecdotal comments

It should in particular be noted that:

- In the view of the MRC the level of risk in direct debits for ecommerce transactions is understated. Direct debits do not benefit from the monitoring and compliance regimes supported by card schemes, nor the robust consistent fraud and dispute reporting systems designed to identify and manage risk. This is not therefore a sensible model to replicate.

- Card schemes have well-established controls to determine when goods/services have or

have not been provided and guide liabilities accordingly. The proposed legislative approach unbalances this well established and performing model, to the detriment of merchants, creating a significant liability with no apparent balancing control.

- In recent years the card schemes have taken robust steps to better control the levels of first party fraud which remote payments can create. These actions have not been replicated within direct debits, and this legislation will undo the productive work undertaken.

- This legislation as stated would result in many merchants requiring a far more complex sign-up and validation process, combined with more pre-pay rather than pay-later models – reducing European consumers ability to easily access service-based ecommerce products

As such the MRC members strongly oppose this proposal, and would ask that it is reconsidered

7. Spending Limits

In summary:
PSD2 allowed a payer to set a spending limit for a card. This article now proposes that a default "low spending limit" must be applied. This would likely have a significant impact on decline levels and could allow consumers to game systems by changing value after an initial authorization has been received.

Proposal text:

- Article 51
  Where a specific payment instrument is used for the purposes of giving permission, the payer and the payer's payment service provider shall offer to the payment service user the possibility of setting fair and proportionate spending limits for payment transactions executed through that payment instrument.

  Payment service providers shall not unilaterally change the spending limits agreed with their payment service users. The spending limit shall, by default, be set at a low level and shall be specified in the contract between the payment service provider and the payer.

Implications:
It is unclear what risk this change manages. Blanket single value limits have caused significant decline issues in many markets and have mostly been replaced by statistically based detection models. The use of such a limit, may be useful in some circumstances but a generic 'low' value is likely to create friction and cost.

Proposed Merchant/MRC positioning:

Static spending limits are a legacy control which has been tested over many years and found to be problematic for consumers, banks and merchants.

The concept of allowing a consumer who wishes to set a card control, perhaps to aid budgetary spending or if there is concern that fraud may occur (say travelling overseas, or after a fraud experience) is understandable, and previous legislation provides for this.

However, requiring that PSPs must default this limit to a 'low level', can only increase decline levels with the attendant additional effort and cost between consumers, merchants and banks necessary to address these. There is no apparent additional benefit from fixed limits, and these undermine the investments in sophisticated detection systems which have long replaced these rudimentary controls.

Whilst 30 years ago banks did apply cardholder limits and there is some legacy for such limit deployment (e.g. ATM daily and monthly controls), most banks have found that machine learning and statistical models now allow far more effective fraud controls.

As this control limit is already in place for those consumers who wish to utilise them, it is therefore proposed that the requirement for a 'low level' limit be removed.

8. Technical Service Providers liable for SCA failure

In summary:
This creates a liability to a PSP whose technical failure results in the failure of an SCA process.

Proposal text:

- Article 58
  Technical service providers and operators of payment schemes that either provide services to the payee, or to the payment service provider of the payee or of the payer, shall be liable for any financial damage caused to the payee, to the payment service provider of the payee or of the payer for their failure, within the remit of their contractual relationship, to provide the services that are necessary to enable the application of strong customer authentication.

Implications:
Whilst this may open an opportunity for various parties in a payment transaction to claim against others for failure, it in practice could open up catastrophic claims for damages which would in practice create additional costs across the payment systems.

Proposed Merchant/MRC positioning:

In principle the concept of a liability for a party whose failure creates a high risk transaction has merit, but the wider consequences of such a position may not be fully appreciated.

The concern here, is that creating a liability for an entity during an outage for transactions which prevent SCA occurring will result instead of a controlled fallback situation, where increased risk is accepted by the party taking the risk decision, this will create a tendency towards either blanket approvals (because the liability now sits with the failing party) or blanket declines.

Blanket approvals will create a position exactly opposite to the probable intention of the legislation, and the latter will result in outages becoming severe, damaging payment system resilience and reliability.

It is proposed that a more detailed proposal be set out which seeks to address these potential extreme outcomes and shared with all payment stakeholders to assess any potential unintended impacts. A decision can then be taken in light of the implications of the proposed change.

9. Spoofing of customer PSP

In summary:
This creates a full PSP liability for any impersonation of their employees to undertake a fraud.

Proposal text:

- Article 59
  Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider using the name or e-mail address or telephone number of that payment service provider unlawfully and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without any delay, reported the fraud to the police and notified its payment service provider

Implications:
In practice some markets (e.g. UK) PSPs are required to support this form of liability model already and this may indicate a European desire to replicate this model more widely in Europe. However, if agreed as a principle it could be extended to other players in the payment system in future (including merchants).

Proposed Merchant/MRC positioning:

Whilst this provision does not directly create a risk to merchants, it may do so indirectly if a general payment liability exists for the transactions disputed (e.g. Directs Debits, card based telephone order transactions et al).

This creates a situation where an entity may incur a liability as a result of a third party manipulation of a consumer. This could occur, even if the consumer is warned of potential risks, discloses information which they are contractually forbidden to disclose and even if they are directly advised by their PSP not to not undertake the transaction proposed.

This creates the potential for a liability that a PSP cannot sensibly control or manage and the risk that genuine transactions may be stopped because the PSP determines that the transaction may be created due to manipulation. In terms of vulnerable customers (for example the elderly, disabled et al), this could make certain transactions difficult to complete resulting in considerable friction for such customers and potentially create a host of discrimination claims and concerns.

It is proposed that a robust model is developed and shared with the payments industry for review and assessment, before a decision is taken to enshrine this in law.

10. Data Sharing

In summary:
Requires merchant PSPs to provide data to issuers – but it is unclear quite how wide this data feed may be interpreted.

Proposal text:

- Article 83
  1. Payment service providers shall have transaction monitoring mechanisms in place that:

  (a) support the risk-based application of strong customer authentication...;
  (b) exempt the application of strong customer authentication based on the criteria under Article 85(11)...;
  (c) prevent, detect and, where possible, resolve potentially fraudulent payment transactions...

  2. ...Payees' payment service providers shall provide the data required for the purposes referred to in paragraph 1 to the payment service providers involved in the transaction.

Implications:
In practice merchant PSP's may be asked to provide a wide range of data relating to consumers, profiles, goods and services etc. which may be difficult and/or expensive to provide. Alternatively, this may relate to a few very specific fraud measures. This is currently a very open requirement that needs definition to allow opportunities and impacts to be assessed.

Proposed Merchant/MRC positioning:

Payment system rules already set out requirements in terms of data requirements to support transactions and risk management. There is a complex balance of costs/benefits intending to ensure that information that can be sensibly provided is, and that which cannot be produced, or cannot be produced prior to a payment instruction being completed, is not.

This proposal could be seen as a carte blanche for a PSP to demand a range of information, whether practical to provide or not.

It is requested that the requirement be clarified and that the balance between time available, information available and cost be set out to avoid requests of marginal risk benefit which could create significant impacts for merchants/payees.

11. Implementation Timeline

In summary:
Article 112 requires the acts recommendation to be fully deployed within 18 months of the regulation coming into force.

Proposal text:

- Article 2, 32, 82, 89, 91
  The EBA shall submit the Regulatory Technical Standards ... to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation].

- Articles 48, 84
  The EBA shall submit those draft regulatory technical standards to the Commission by [Please insert the date= 18 months after the date of entry into force of this Regulation].

- Article 112
  This Regulation shall apply from [OP please insert the date= 18 months after the date of entry into force of this Regulation].

Implications:
Without sight of the detail, this feels too restrictive. It would seem sensible for this to be considered in light of the ask and it is noted that previous PSD legislation carried heavy workloads

Proposed Merchant/MRC positioning:

MRC on behalf of the merchant community would request that the lessons from earlier significant legislation of this type (most notably PSD2) be considered. We would please request that 24 months be considered a reasonable time period for change to be implemented.