EBA consultation on the draft Guidelines on the sound management of third-party risk

Mastercard Consultation Response

October 7, 2025

Executive Summary

Mastercard welcomes the EBA's proposed revision of its Guidelines on outsourcing arrangements of February 25, 2019 (the "**Guidelines on Outsourcing**") and the public consultation launched on July 8, 2025 on its draft Guidelines on the sound management of third-party risk (the "**Guidelines on Third-Party Risk**"), which will replace and update the Guidelines on Outsourcing.

In its consultation document, the EBA proposes to expressly include '*authentication & authorisation*' in its non-exhaustive list of functions that could be provided by a third-party service provider and that will therefore be subject to the Guidelines on Third-Party Risk (Annex I to the draft Guidelines). This would require payment service providers ("**PSP**"), such as banks, payment institutions and e-money institutions, to enter into an arrangement subject to the requirements of the Guidelines every time they rely on a third party for the authentication and/or authorisation of transactions, including card transactions. This would negatively affect the deployment of innovative and secure authentication and authorisation solutions, and ultimately take the European card payment industry backwards.

Mastercard therefore welcomes the opportunity to provide the following views and recommendations to the EBA on the treatment of third-party provision of authentication and authorisation services:

- **Authentication and authorisation should be excluded from the scope of the Guidelines.** In the payments ecosystem, there already exists a broad range of authentication and authorisation solutions which do not constitute outsourcing—for example, authentication services provided by card schemes and wallet providers, and authorisation solutions provided by schemes. Treating these solutions as outsourcing would significantly restrict PSPs' ability to make use of them. This is because card issuers would need to conclude dozens, if not hundreds, of outsourcing agreements with all possible providers of authentication and authorisation solutions. Such an interpretation would also undermine the roll-out of the EU Digital Identity Wallet ("**EUDIW**") introduced by Regulation (EU) 2024/1183 (the "**eIDAS2 Regulation**"). In order for the EUDIW to be used for the authentication of payments, PSPs would be required to enter into outsourcing agreements with each EUDIW provider, creating unnecessary friction and regulatory burden and potentially delaying consumer adoption of this strategic EU initiative.
- **Any decision on the inclusion of authentication and authorisation within the Guidelines should be postponed until the adoption of the Payment Services Regulation (PSR) and the Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and outsourcing.** Whether the delegation of SCA for card transactions qualifies as outsourcing is a debated issue and still under discussion in the context of the PSD2 revision. We therefore believe it would be more appropriate to defer any decision on the inclusion of authentication and authorisation within the Guidelines on Third-Party Risk until the adoption of the upcoming PSR (replacing the PSD2) and the RTS on SCA delegation and outsourcing to be developed under this new regulatory framework. This is important to guarantee clear, stable and harmonized rules across Europe, and allow the EC to have its say on this important issue.
- **Clarifications would be needed if authentication and authorisation remain in scope of the Guidelines.** Should authentication and authorisation remain within the scope of the Guidelines on Third-Party Risk, the EBA should clarify that:
    - **Delegation of authentication and authorisation does not constitute 'critical or important outsourcing'**, as these activities do not meet the relevant conditions set out in the Guidelines.

- **Multilateral or scalable agreements for the delegation of authentication to third-party providers should be permitted**, as they are essential to foster innovative and secure authentication solutions.
- **Only models whereby the payer's PSP does not retain control over authentication / authorisation should qualify as outsourcing subject to the Guidelines**. Conversely, models where the PSP remains in control of these functions should fall outside the scope.
- **Authentication and authorisation services provided by card schemes should be expressly excluded** from the scope of the Guidelines under the exclusion for 'global network infrastructures' set out in point 32(b) of the draft Guidelines.

For any questions and comments, please reach out to Mr. Boris Martinovic at boris.martinovic@mastercard.com.

1. Authentication and authorisation should be excluded from the scope of the Guidelines

Authentication today is highly fragmented, with PSPs relying on a wide range of solutions that are already embedded in the payments ecosystem and that do not constitute outsourcing. These include card scheme protocols (such as EMV 3DS), global wallet providers (e.g., Apple Pay, Google Pay, Samsung Pay), local wallet providers, biometric authentication services, device-based authenticators, and telecom-based solutions (e.g., SIM-based). With the forthcoming roll-out of the EUDIW under the eIDAS2 Regulation, PSPs will also be expected to accept authentication through multiple EUDIW providers across Member States. Authorisation is less fragmented but is similarly often supported by scheme-level infrastructure and third-party solutions that can differ from market to market.

If the EBA were to classify all of these activities as "outsourcing," then each PSP—whether a bank, payment institution, or e-money institution—would be obliged to conclude a full outsourcing arrangement with every third-party provider it interacts with. This would not mean a handful of contracts, but potentially dozens for smaller PSPs and hundreds for large issuers operating across the EU. Such arrangements would have to meet all the requirements of the Guidelines, including due diligence, risk assessments, ongoing monitoring, reporting obligations, exit strategies, and audit rights. **The resulting administrative and compliance burden would be disproportionate, impractical, and ultimately unworkable at scale**.

By way of illustration, a large EU bank could:

- Issue cards in more than 10 jurisdictions;
- Support multiple wallets (Apple Pay, Google Pay, Samsung Pay, and local wallets);
- Work with several biometric and device-based authentication providers;
- Accept authentication from multiple national EUDIW providers once deployed.

Each of these relationships would, under the proposed interpretation, require a full outsourcing agreement, creating significant legal and operational complexity. **This would not only strain PSPs' resources but also discourage them from adopting innovative solutions**.

Moreover, such an interpretation would directly undermine the EU's strategic policy objectives. In particular, **it would hamper the roll-out of the EUDIW under the eIDAS2 Regulation**. For the EUDIW to be usable for payment authentication, PSPs would need to contract with every EUDIW provider as an outsourcing counterparty—an approach that would create unnecessary friction, regulatory burden, and delays in consumer adoption of this key EU initiative.

In sum, extending the outsourcing framework to authentication and authorisation would create a compliance regime that is **disproportionate and misaligned with broader EU digital policy objectives.**

Last, this approach is **duplicative of existing regulatory requirements**, and goes against the simplification objectives of the European Union because:

- Authentication and authorisation of payments are already comprehensively regulated under PSD2 and the RTS on SCA & Secure communication and will be regulated in the upcoming PSR and subsequent RTS.

- PSPs must already meet prescriptive requirements for authentication factors, independence, dynamic linking, and security.
- National competent authorities already monitor compliance, and PSPs are directly liable if authentication or authorisation is deficient or not properly performed.
- Card schemes (e.g., Mastercard, Visa) and wallet providers (e.g., Apple Pay, Google Pay) already impose strict technical, operational, and compliance requirements on issuers and acquirers to ensure security and resilience. These frameworks often go beyond what is in EU law, with regular audits and certification requirements.

2. Any decision on the inclusion of authentication and authorisation should be postponed until PSR and RTS approval

Whether the delegation of authentication qualifies as outsourcing has been a much-debated issue in recent years. While the EBA has aimed to provide some guidance with non-binding Q&As provided through its online Q&A tool (e.g., EBA Q&As 2018_4047, 2019_4651, 2019_4937, 2020_5643 and 2021_6141), the EBA itself recognized this is a very complex issue, which requires further clarification and harmonization in the context of the PSD2 revision.

The EBA Opinion on the PSD2 review of June 2022 to this end, without taking a clear position on this much-debated issue, proposes that the regulation replacing and updating the PSD2 "*clarifies and articulates further the requirements on who is responsible and liable for the application of SCA and the related requirements on delegation of SCA. This should ensure protection of customers, legal certainty, and transparency of the related requirements*" (point 308).

In June 2023, the European Commission (the "**EC**") published its proposal for a PSR, which will replace and update the rules set out in the PSD2. The EC proposed that SCA delegation by PSPs to third parties (e.g., wallet providers, merchants and technical service providers) would be outsourcing and therefore subject to the Guidelines on Outsourcing. To this end, Article 87 of the PSR provided that "*A payer payment service provider shall enter into an outsourcing agreement with its technical service provider in case that technical service provider is providing and verifying the elements of strong customer authentication. A payer's payment service provider shall, under such agreement, retain full liability for any failure to apply strong customer authentication and have the right to audit and control security provisions*".

The PSR also mandates the EC to adopt RTS (to be developed by the EBA) that specify the requirements applicable to the outsourcing agreements for SCA delegation (Article 89(1)(d) of the EU PSR).

The upcoming RTS will also have to take into account the ongoing technological developments in the authentication space. This includes the EUDIW introduced by the eIDAS2 Regulation, which PSPs will need to accept for SCA purposes for online use cases as of December 2027 (Article 5f of eIDAS2 Regulation). To this end, Article 89(3) of the PSR provides that "*the EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments, and the provisions of Chapter II of Regulation (EU) 2022/2554, and the European Digital Identity Wallets implemented under Regulation (EU) No 910/2014.*" (emphasis added).

While the Council supports the approach set out by the EC in its proposal for the PSR, **the Parliament has instead proposed to delete Article 87 EU, which qualifies SCA delegation as 'outsourcing'**, and leave it to the EBA to regulate this controversial issue through the RTS.

The PSR is expected to be adopted shortly (possibly by the end of 2025), after which the EBA will have 12 months to prepare its RTS. Once adopted (probably in 2027), those RTS will constitute the definitive regulatory framework for the outsourcing of authentication-related activities (including in relation to the use of the EUDIW).

Hence, in our view, any debate on whether authentication should fall within the scope of outsourcing requirements in the context of the revision of the Guidelines on Outsourcing would be premature. The forthcoming PSR and RTS will likely explicitly address this matter and establish a fully harmonized regulatory framework just a few months after the adoption of the EBA Guidelines (which is planned for Q3 2026, as outlined in the recent EBA 2026 Work Programme).

Any attempt to anticipate the regulatory treatment of authentication within the Guidelines on Third-Party Risk (Level 3, which is also subject to the comply-or-explain principle) risks creating fragmentation, overlaps, or inconsistencies with the forthcoming PSR (Level 1) and RTS (Level 2).

The EBA should also wait for the adoption of the RTS to allow the EC to intervene on this issue. This is because, while the RTS on SCA delegation and outsourcing under the PSR will be developed by the EBA, the EC can amend them and has the final say on their adoption. Depriving the EC of this possibility would be contrary to the PSR, which mandates the EC and the EBA to regulate together this very important issue through RTS.

For these reasons, we consider it more appropriate to defer any detailed discussion on the inclusion of authentication and authorisation within outsourcing requirements until the adoption of the PSR and RTS. This is important to guarantee clear, stable and harmonized rules across Europe on this crucial issue.

3. Delegation of authentication and authorisation is never 'critical' outsourcing

If the EBA were to decide to include authentication and authorisation within the activities subject to the Guidelines on Third-Party Risk, we believe that it should recognize that 'authentication and authorisation' are never 'critical or important functions' under the Guidelines and therefore expressly exclude the application of the stricter requirements for third party provision of critical or important functions.

The draft Guidelines on Third-Party Risk define critical or important functions as follows:

> "*a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.*"

While the Guidelines on Third-Party Risk leave discretion to financial entities (including PSPs) to decide whether a specific activity qualifies as 'critical or important' function, it provides the following guidance:

> "*Considering the risk assessment foreseen under Section 11.2, financial entities should always consider a function as critical or important in the following situations, where its disruption, discontinuity, defect or failure in its performance would materially impair:*

a. their continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law;

b. their financial performance;

c. the soundness or continuity of their services and activities.

When relying on a TPSP for operational tasks of internal control functions, financial entities should always consider such tasks as critical or important functions, unless the assessment establishes that a failure to provide the tasks or the inappropriate provision of the tasks would not have an adverse impact on the effectiveness of the internal control functions.

When financial entities intend to use TPSPs for the provision of functions of banking activities or payment services or issuance of ARTs as defined in Article 3(1), point (6), of Regulation (EU) 2023/1114 to an extent that would require authorisation by a competent authority, they should automatically consider such function as critical or important, as referred to in Section 12.1.

In the case of financial entities that are subject to Directive 2014/59/EU, particular attention should be given to the assessment of the criticality or importance of functions if the third-party arrangement concerns functions related to critical functions and core business lines as defined in Article 2(1), point (35) and 2(1), point (36) of Directive 2014/59/EU and using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778. Functions that are necessary to perform activities of core business lines or critical functions should be considered as critical or important functions for the purpose of these Guidelines, unless the financial entity's assessment establishes that a failure to provide the function or the inappropriate provision of such function would not have an adverse impact on the operational continuity of the core business line or critical function" (points 33-36).

We believe that authentication and authorisation do <u>not</u> meet the above-mentioned conditions to qualify as a critical or important functions for the following reasons:

- Failure to provide delegated authentication / authorisation would not 'materially impair' the compliance of the payer's PSP (i.e., in the card environment, the issuer) with the PSD2 requirements under the draft Guideline 4, point 33(a). This is because:
    - In the case of authentication, if a third party (for example, a wallet provider) to which authentication was delegated fails to authenticate the user, the issuer can still apply its own authentication, its own exemptions from SCA requirements (e.g., for low-value and low-risk transactions, or for transactions at white-listed trusted beneficiaries), or decline the transaction, hence remaining fully compliant with the regulation.
    - In the case of authorisation, if a third party to which authorisation was delegated (for example, a provider of services to authorize transactions on behalf of the issuer) fails to authorize a transaction, the issuer can typically rely on fallback authorization systems. The issuer can also ensure that transactions are declined if there is a material risk of fraud (e.g., by configuring the parameters of third-party authorisation systems), hence remaining compliant with the regulation.
- Failure to provide delegated authentication / authorisation would not 'materially impair' the issuer's 'financial performance' under the draft Guideline 4, point 33(b) or 'the soundness or continuity of their services and activities' under the draft Guideline 4, point 33(c). If a wallet provider to which authentication was delegated fails to authenticate the user, or if a service

provider that authorizes card transactions on behalf of the issuer fails to authorize transactions, this has in fact a very limited impact on the issuer's overall financial performance or on the continuity of the issuer's activities. This is unlikely to have a critical effect on the ability of an issuer to provide its payment services, even if it can add some inconvenience to users.

- Delegation of authentication and authorisation does not relate to 'operational tasks of internal control functions' under the draft Guideline 4, point 34.
- Delegation of authentication and authorisation does not relate to 'functions of banking activities or payment services to an extent that would require authorisation by a competent authority' under the draft Guideline 4, point 35. This is because only the authentication / authorisation of the card payment is delegated, and not the provision of the card payment itself, which is the activity that requires an authorisation as PSP under the PSD2 and the upcoming PSR and PSD3. The provision of payment services, including card issuing and acquiring of card transactions, and the execution of card transactions is indeed already included in the list of activities of Annex I to the Guidelines on Third-Party Risk that are subject to the requirements set out in therein.
- Finally, failure to provide the authentication / authorisation function would not have "*an adverse impact on the* [issuer's] *operational continuity of the core business line or critical function*" under EBA Guideline 4, point 36. This is because if a third party to which authentication or authorization was delegated fails to provide their services, the issuer can generally continue to provide card payments (as well as other payment services or banking services).

4. Multilateral or scalable agreements for SCA delegation are needed

The EBA has recognized that delegation of SCA to technical service providers "*may have positive effect on the introduction of new authentication solutions facilitating the development of new business models for payment services, as well as customer convenience. This could allow for seamless, efficient and integrated SCA solutions*" (EBA Opinion of June 2022, point 309).

If each issuer were to be required to enter into bilateral outsourcing agreements for every authentication solution with each and every third party, these positive effects would not materialize. This is because SCA delegation would become very burdensome and costly.

This could bring significant disruption not only to e-commerce but also to contactless payments in Europe. We understand that only very large third parties providing authentication solutions would have the capacity and capabilities to conclude thousands of outsourcing agreements with each and every issuer. Smaller players would not have the possibility to do so. This problem would be clearly exacerbated if the stricter requirements for third party provision of critical or important services under the EBA Guidelines were to apply.

This would take the European payment industry backwards, in the exact opposite direction of where the EBA would like to arrive in terms of "*facilitating the development of new business models for payment services, as well as customer convenience"* and enabling "*seamless, efficient and integrated SCA solutions"*.

For this reason, if the EBA were to decide to include authentication and authorisation within the activities subject to the Guidelines on Third-Party Risk, it should clearly and explicitly allow for multilateral or

scalable outsourcing agreements for SCA delegation, so that an issuer can easily delegate SCA to multiple entities. A central entity, such as a card scheme, could be in the best position to evaluate and validate the security of each authentication solution and conclude multilateral or scalable outsourcing agreements. This would significantly facilitate the deployment of new and innovative authentication solutions and would ultimately result in better and cheaper evaluations and increased security.

5. When the issuer remains in control of authentication and authorisation there is no outsourcing

The EBA requested the EC to clarify in the context of the PSD2 revision whether the use of "*third-party technology would require an outsourcing agreement or not and whether some conditions need to be applied in case the EC arrives at the view that an outsourcing agreement is not needed*" (point 314 of the EBA Opinion on the PSD2 review of June 2022, emphasis added).

The EBA therefore recognizes that there can be authentication solutions, relying on third-party technology, that do not require an outsourcing agreement.

In this regard, the EBA seems to be of the view that a model whereby the issuer remains in control of authentication should not be qualified as SCA delegation, nor outsourcing (see EBA Opinion on the PSD2 review of June 2022, point 313).

If the EBA were to decide to include authentication and authorisation within the activities subject to the Guidelines on Third-Party Risk, it should expressly clarify that all models whereby the issuer remains in control of such activities should fall outside the scope of the Guidelines.

As regards authentication, this is the case, for example, when the issuer:

1. Has its own app and authenticates the payer by relying on 'off-the-shelf' technology that is readily available on the consumer device (e.g., a fingerprint reader on a smartphone). In this case, the issuer is in fact authenticating the payer and is using such technology to support its own SCA (this case where the issuer uses its own app is reflected at point 313 of the EBA Opinion);

or

2. Relies on a third party for operating or triggering the authentication of the payer but remains in control of authentication. This is the case where the issuer:
    a. Validates/verifies an authentication factor transmitted by a third party (e.g., the issuer validates device possession by using the device public key to validate the signature generated by the consumer device on each transaction);
    b. Validates/verifies the results of SCA carried out using an 'off-the-shelf' technology (e.g., fingerprint reader) that is readily available on the consumer device. When issuers rely on 'off-the-shelf' technology readily available on consumer devices, such technology is provided 'as is' and for free by the device manufacturer and without a contract. There is no SCA delegation nor any entity to which SCA is delegated;
    c. Is technically able to revert to its own SCA and decline the transaction if there is a material risk of fraud.

We believe the same principles should apply to authorisation: where the issuer retains full control over the decision to authorise or decline a transaction, the use of third-party services should not qualify as

outsourcing. When third parties provide technical support in the authorisation process, if the issuer has control over the authorization rules and parameters of these third-party services, for example to decline transactions in case of a material risk of fraud, there is no delegation of the authorisation function, and therefore the requirements under the Guidelines on Third-Party Risk should not apply.

Finally, we believe that services provided by card schemes to ensure the security and business continuity of their scheme, including authentication and authorisation services, are not outsourcing and are therefore out of scope of the Guidelines on Third-Party Risk. This is because card scheme services are excluded from the application of the EBA Guidelines on Third-Party Risk under the exclusion for 'global network infrastructures':

> "*As a general principle, the following functions are excluded from the scope of these Guidelines:* […] *b. global network infrastructures (e.g. Visa, MasterCard);*" (point 32(b) of the draft Guidelines on Third-Party Risk).

We believe that this exclusion should expressly cover authentication and authorisation solutions provided by card schemes for greater legal certainty.

* * *