Visa response to EU targeted consultation on PSD2 Review

Visa welcomes the opportunity to provide feedback to the European Commission Consultation on the PSD2 review.

Our mission is to connect the world through the most innovative, reliable and secure payment network. For us, making the global payment ecosystem safer for retailers and consumers reducing fraud levels is a key priority.

Visa fully supports the overall objectives of the PSD2 and we would like to share our views on this matter to ensure that the legislative framework paves the way to have a modern, digital and well-functioning payments market, where European consumers and businesses have a choice of easy, fast and safe payment methods, suitable to their different needs.

General comments on the PSD2 objectives: What has been achieved and where we would need to make some changes.

- In the recent years we have seen a revolution in digital payments which was accelerated by the Covid crisis. There is an increased demand for contactless, online, digital, frictionless and speedier payments. Consumer expending habits are also changing and new services such as BNPL and crypto currencies are increasing in the market. Thus, we believe that PSD2 will benefit from some changes to cater for all these changes.

- The revised Payment Services Directive (PSD2) has been a major step forward for the payments industry and it brought many benefits such as:

    - It increased competition in the payments market and enabled the emergence of new business models based on the sharing of payment account data such as payment initiation services (PIS) and account information services (AIS) providing the legislative and regulatory foundation for Open Banking. Although these new entrants are facing some challenges.

    - It improved the general level of the security of payment transactions through the implementation of strong customer authentication (SCA).

    - It stimulated innovation in the area of customer authentication allowing the industry to introduce innovative tools to detect and prevent fraud. We have seen great developments around EMV 3DS, which creates a standardized, harmonized and secure authentication solution for all stakeholders. This includes improving the risk decision with more data, new payment methods, new channels for payments and a better user experience. Another area where we see increased innovation is around behavioural biometrics which works passively in the background of a user web or mobile session to monitor thousands of parameters, such as the way a person holds the phone or how they scroll, thereby minimizing friction in the user experience.

- However, there are still some barriers due to very prescriptive regulatory requirements that have a negative impact on the way the market innovates and adjusts to the new and fast changing circumstances. We would therefore suggest **moving to a more outcome-based approach**.

- While the PSD2 was initially designed to be technological neutral, we believe that this objective may not be fully achieved. New EU regulatory measures should not undermine payment service providers' ability to

design best solutions to ensure a safe and secure payments ecosystem and at the same time, allowing them to constantly evolve to stay ahead of the very rapid changes that the payments market is experiencing.

Scope of the PSD2

- We do not believe there is a need for payment processors, and operators of payment systems and schemes to be added into the scope of the PSD. These activities are markedly different from end-user services currently captured under the scope of the PSD2, and do not fit neatly into the PSD2 framework as it exists today.

- It is important to also stress that a robust and globally agreed basis for the supervision and oversight of these activities already exists today outside of the PSD2 framework, known as the Principles of Financial Market Infrastructure ("PFMIs") which are internationally agreed standards published by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) in April 2012. They are a part of a set of standards that the international community considers essential to strengthening and preserving financial stability. For example, Visa Europe Limited (VEL) is incorporated in the United Kingdom and supervised by the Bank of England against the PFMIs. VEL, being located outside the euro area, is also overseen by the European Central Bank as per the Eurosystem oversight policy framework as part of a cooperative arrangement with its main supervisor, the Bank of England, against the Oversight Framework for Card Payment Schemes – Standards (2008).

- In our view, it is important that no treatment of these activities under PSD2 results in duplication with the well-functioning supervisory and oversight processes already in place to avoid inefficiency, additional complexity, and potentially undermine the smooth functioning of payment systems operating across the EU. Any decision on whether to expand the PSD2 activities in scope should also be looked at with proportionality in mind and take place with consultation of both the ECB, national central bank overseers and affected industry participants – the decision to introduce additional and potentially duplication requirements must be proportionate to the risk posed given the existing European supervisory and oversight frameworks already in place.

- As an alternative to capturing these services under the scope of PSD2, we recommend ensuring that the European Banking Authority, ENISA and Joint Overseers under the Digital Operational Resilience Act (DORA) are informed as observers to the oversight activities undertaken by the European Central Bank and oversight colleges (which include national central banks) currently in place for payment processors, and operators of schemes and systems operating across the EU. The European Commission and ECB should also explore further integrating existing mechanisms like the Euro Cyber Resilience Board's CIISI-EU voluntary cyber threat intelligence sharing initiative into existing regulatory framework structures, before introducing new frameworks which may duplicate these activities.

- Visa supports maintaining the Limited Network Exclusion (LNE) under article 3 (k) of the PSD2 but notes the different interpretations among Member States as to what constitute a limited range of goods and services.

Strong Customer Authentication (SCA) requirements

- One of the main areas that we believe would need to be reviewed is with regard to the **implementation of SCA requirements** which is also holding innovation back in some ways.

- While we fully support the ultimate objective of detecting and preventing fraud to ensure a safe and secure payment ecosystem, we believe the SCA framework fails to achieve the right balance between security and convenience creating unnecessary friction which is translated into different abandonment rates across different regions.

- European regulators should enable the full use of innovative fraud prevention and authentication tools to allow payment service providers to stay ahead of fraudsters while improving customers' experience by encouraging them to select the best combination of authentication methods and technologies.

- The current interpretation of SCA negatively impacts the ability of PSPs to deliver their services to those users that do not have access to digital devices and other vulnerable customers. In order to avoid this, we would reiterate the importance of focusing on overall security objectives instead of prescribing specific acceptable authentication methods.

- Please find below a list of recommendations for the European Commission to take into account when reviewing the PSD2:

    - **Expand the concept of behavioural biometrics as inherence factor** for remote payments: It has been proven that behavioural analytics solutions, such as 3DS profiling, are vastly superior in terms of fraud prevention compared to static knowledge factors.

    - **Flexibility on the use of SCA factors**: PSPs should be free to develop solutions that satisfy the independence obligation without having to have two factors from different prescribed categories, which are arbitrary and limit the development of effective two factor solutions. The focus should be on the independence of those factors and that that the breach of one does not compromise the reliability of the others.

    - **Raise contactless limits:** Due to Visa data showing consistent low fraud, we recommend a review of the current regulatory thresholds setting the maximum per transaction (from 50 to 100 EUR) and cumulative limits (to 250 EUR or 5 consecutive taps) before strong customer authentication (SCA) must be applied for contactless transactions, giving industry the flexibility to set higher limits in their respective markets if they choose.

    - **Extending the current SCA exemption for unmanned parking terminals**: to include unmanned electric vehicle charging stations and charity donation stations.

    - **Fraud calculation for TRA exemption**: Further clarity is needed on the calculation of fraud rates applicable to TRA. PSP should only include in the fraud calculation the fraudulent transactions for which it is solely liable.

- **Application of the Low Value Exemption**: We would welcome some clarification stating that one counter could be used in authorisation and another one in authentication for the payment instrument rather than requiring issuers to synchronise counters of both routs so the two do not have to be synchronised but may count independently of each other.

- **Deferred authorisation**: We have seen issues with the cases where transactions are performed when no connection is available to authenticate and authorize and are therefore processed later. We believe that an exemption should be created for these cases.

- We ask for clarifications on MIT and MoTo. We believe that the regulation should focus on the type of transactions rather than the instrument used when setting up SCA requirements. When setting up a mandate for the payer to initiate a transaction or a series of transactions, the setting up of such a mandate is subject to SCA. This principle also applies for MoTo transactions. Card payments and bank transfers are both 'electronic' when used via the internet or other digital systems; and are not electronic when payment details are delivered via non-electronic channels such as MoTo even if the details captured that way are then sent onwards electronically for processing. The review should maintain that all payments can be MoTo, subject to the key characteristic that a non-digital channel is used by the consumer.

- Regarding MIT, due to its nature, we think that extending SCA to MITs is not practically possible and it would have a negative impact on a range of business models and leading to significant inconvenience and friction to consumers. We would support confirmation on the Level 1 text that payee-initiated transactions are exempted from SCA requirements and SCA would only be required for setting up the mandate. We also believe that further clarity may be beneficial to ensure the correct use of MITs and avoid that those transactions, which are in reality Customer Initiated Transactions (CIT), are incorrectly treated as MITs. It is important to stress that a transaction can only be an MIT if the cardholder is not available at the point of interaction, whether is physical or online, to (I) initiate; or (II) authenticate the transaction.

- We also point out the complexities of the travel sector. With no exemptions in place for this sector, the industry shared with regulators an interim solution which enables them to use, for the short term, the MoTo flag. If we are to put an end to the usage of this interim solution, which would be preferable, there is a need to discuss with regulators what other acceptable solution could be put in place for indirect travel bookings.

- Regarding delegated authentication, we have seen different interpretation across the EU as to whether it constitute outsourcing and therefore subject to the EBA outsourcing guidelines. We would welcome clarifications form the regulators to define the line as to when delegated authentication could be consider as use of a third-party technology for SCA and when it becomes outsourcing.

Open banking and open finance

- As Visa, we believe that the future of payments and retail financial services at large is open. There is a clear, global shift towards open banking, open finance and open data. However, it is still early days for open banking in Europe with limited uptake of open banking account information services.

- While open banking has been lauded as a success there is still tremendous potential to be unlocked. Open Finance builds upon the foundations of Open Banking with the potential to address the challenges and shortcoming of the existing framework, allowing for the full use of the benefits of enhanced data sharing in the financial ser as long as they are safe and don't expose customers to any data privacy, financial, or cyber risk.

- Open Finance will unleash the development of numerous new businesses and services increasing the complexity of the current Open Banking ecosystem, making it increasingly necessary to address the challenges to ensure data security and data privacy while managing new permissions and levels of access. Data controls are one way to address that complexity. The development of APIs and premium APIs can play a crucial rule to help people connect their accounts across thousands of financial services providers and to have full control over the financial data and the ability to choose to share it with their personal digital finance tools.

- Financial firms must be given not only the legal clarity necessary to develop new businesses and services but also both clear strategic and commercial benefit and have confidence of a stable and secure legal and regulatory environment around data sharing, to invest and develop new products.

Transparency Conditions and information requirements

- Information disclosure requirements to end-users of currency conversion and payment services are an important tool for increasing competition, consumer-centric choice and consumer protection. In addition to the information disclosure rights themselves, consumers need to receive the information in a meaningful way. Disclosure and transparency of information in payments must be looked at holistically and not purely through the lens of the PSD2 obligations.

- Any decision to update to the PSD2 information requirements should take into account the industry improvements, and efforts, already being made across the payment ecosystem. They should also ensure that the current flexibility and good practices which are continuing to develop, and which allow for tailored disclosure to meet the specific needs of specific consumers.

- Transparency should be looked at from the perspective of the end-user. Different requirements or methods of displaying transparency should generally be avoided where they could provide confusion – such as a European consumer being shown different mark-ups or disclosures when using the same or different payment instruments and methods to do the same activity. It is also important to balance accuracy and legibility in information disclosure requirements to end-users – this is particularly important when promoting comparative transparency such as under the Cross Border Payments Regulation (noting the use of non-commercial ECB euro reference rates as a benchmark against which commercial costs and charges are marked-up against).

Liability provisions

- Further clarity would be welcome defining that when the PSP of the payee triggers an SCA exemption and the transaction is carried out without an SCA, they will be liable towards the payer's PSP for the financial damage caused. If the exemption has been triggered by the issuers, they should bare the liability. It is also

important to differentiate the cases where the merchant (or PSP of the payee) request friction less (but an acquirer exemption is not requested) in these cases, liability rest with the issuers. We are of the view that a Merchant is only liable when he asks for a true acquirer exemption. When he just asks for frictionless without acquirer exemption, the liability rest with the issuer.

Open access to payment systems

- We support the Commission's intention to amend the Settlement Finality Directive the SFD to allow payment institutions and e-money institutions to be direct participants in SFD designated systems. the European Commission should expand the benefits of SFD protection to as many participants operating across the EU internal market as possible in order to provide greater legal certainty over when settlement finality is agreed, increases efficiency and reduces risk.

- Having a set of designation criteria harmonised across the EU would be helpful, and potentially encourage central banks to recognise third country designed settlement systems more easily if they have been designated for similar protection under similar regimes in their respective countries.