Copenhagen 2 December 2022

Finansdepartementet
Fi.remissvar@regeringskansliet.se
Fi.fma.b@regeringskansliet.se

Your reference: Fi2022/02529
Our reference: Visa Europe

Fi2022/02529 Memorandum on Increased Resilience in the Payments System – Visa Europe opinion

About Visa

Visa is a network and world leader in digital payments, working to remove barriers and connect more people to the global economy. The company facilitates digital payments across more than 200 countries and territories among a global set of consumers, merchants, financial institutions, businesses, strategic partners and government entities through innovative technologies.

Visa appreciates the opportunity to submit comments to the memorandum on increased resilience in the payments system, Fi2022/02529.

Executive Summary

Visa shares the Ministry's interest in promoting a sound and resilient payments ecosystem. However, it must be clear who is targeted by the legislation and when. Visa understands that the intended scope of the proposal is limited to clearing operations in Sweden. Therefore, companies which offer payment processing to the Swedish market but have their clearing operations outside Sweden would not be subject to the license requirement. *However*, we are concerned that this is **not sufficiently clear** in the proposed text. Especially in the preparatory text, section 6.1 and in the legal text Chapter 2, §1. The focus of the preparatory text indicates that the proposal is limited to account-to-account payments, however this is **also not explicit** in the legal text. Clarity on these points is important to provide certainty and avoid overlapping regulation and unnecessary cost.

We recommend amendments to the text to clarify that international payment networks are not in scope of the license requirement. For example, changes should be made in relevant parts of the preparatory and legal text including chapter 1 and chapter 2 §1 explicitly by adding "in Sweden":

"2 kap. Tillstånd

Tillståndsplikt

1 § För att bedriva clearingverksamhet *i Sverige* krävs tillstånd av Finansinspektionen."

This would recognize the comprehensive regulatory arrangements already in place for payment systems in Europe and would also support the rules of free movement in the Treaty on the Functioning of the European Union (TFEU).

Discussion

The text on who would **be subject to** a license requirement and who would **be viable to** apply for a license is unclear and could cause confusion. A foreign company with clearing operations outside Sweden is viable to apply, but not subject to require a license. The viability to apply might be interpreted as including a requirement to apply which would create a situation of duplicative oversight of international payment networks. This can lead to regulatory inefficiency, economic distortions, and an uneven playing field across the payments ecosystem. Fragmentation of regulation can also increase operational and resilience risk due to differing standards and regimes across regions, and the creation of potential single points of failure.

To support strong and stable payment systems, it is important that oversight is proportional to the risk posed by individual players in the payments ecosystem. Oversight frameworks also operate most effectively and efficiently when they recognize the oversight requirements already in place for international payment networks that meet best-practices and compliance standards under other competent authorities.

Visa is already subject to multiple layers of robust regulatory and supervisory arrangements in Europe (including by the European Central Bank (ECB) and the Bank of England) and the United States. The current oversight framework that the ECB has in place (i.e. PISA) imposes demonstrably comprehensive obligations on the operators of important payments systems in the European Union (EU), which takes into consideration the need to ensure financial stability across the EU. PISA (and the CPMI-IOSCO Principles for financial market infrastructures (PFMIs) on which PISA is based) cover all aspects of the organizational set-up and operation of important payment systems. This includes the legal basis, governance, liquidity and credit risk, operational risk, access and participation criteria, and disclosure. Operational risks are just one of the risks identified in PISA, which ensures exceptionally comprehensive supervision.

All retail payment systems operating in Europe are therefore subject to a central bank oversight policy, which incorporates the PFMIs. For example, Visa in Europe is currently assessed against the PFMI principles twice already. We are assessed against the PFMI principles by the Bank of England, as a recognised payment system. This assessment includes ongoing reviews as well as a periodic self-assessment that Visa needs to submit on an annual basis. Furthermore, the ECB and a panel of Central Banks from the EU also assess Visa against the PFMI principles through PISA. Under this regime, Visa is subject to ongoing oversight as to Visa's compliance, consistent with PFMI principles, which covers the analysis of the legal basis under all jurisdictions where Visa operates in Europe; the information (including financial information) that is made available to the actors in the Visa system; the appropriateness of the degree of security, operational reliability and business continuity; the effectiveness, accountability and transparency of the governance arrangements; and the management and containment of risks in relation to the clearing and settlement process. A Memorandum of Understanding to minimise duplicative oversight is in place between the Bank of England and the ECB in relation to these arrangements.

All aspects of proper governance and risk management relating to payment processing (clearing and settlement) envisaged in the proposals are covered comprehensively in the PFMIs and existing regulatory arrangements. The proper functioning of our retail payment system is our primary objective and, accordingly, continuity and resilience are matters which Visa takes extremely seriously.

Related discussions are ongoing in the context of the Digital Operational Resilience Act, which support the position that the existing regulatory framework for payment systems is sufficient and individual member states should not depart from this with local regimes. We strongly recommend that national regulators align with pan-European regulatory approaches; having to comply with multiple, disparate local regimes is highly costly and difficult to manage, and fragmentation of regulation can also lead to increased risk and inefficiency for regulators.

Conclusion

We recommend amendments to the text to clarify that international payment networks are not in scope. This would recognize the comprehensive regulatory arrangements already in place for payment systems in Europe and would also support the rules of free movement in the Treaty on the Functioning of the European Union (TFEU). The clarification should include an explanatory text in the preparatory work.

Additional information on Visa's approach to security and resilience

Worldwide, Visa has invested $9bn in fraud prevention and cyber security in the past five years alone. Visa employs more than one thousand dedicated specialists protecting Visa's network from malware, zero-day attacks and insider threats, and more than 900 dedicated cybersecurity professionals additionally operating around the clock to detect, prevent and respond to threats. In addition, Visa has adopted the Three Lines of Defense (3LoD) model to proactively identify and mitigate risks across the organization. We help to prevent an estimated $25bn in global fraud every year and incidents of fraud occur in less than 0.1% of transactions- among the lowest of all payment forms. We have invested in state-of-the-art fraud prevention tools which enable us to identify and prevent attacks such as ATM cash outs, either by alerting industry to threats or directly blocking fraudulent transactions in real time. Our world-class artificial intelligence and machine learning capabilities are designed to identify the most sophisticated threats.

Visa leverages extensive and resilient cross-border infrastructure to help ensure the network remains available with uptime of >99.999%. VisaNet operates via three geographically diverse global locations, which have been carefully selected because they provide high levels of resilience and a minimal attack surface for bad actors. European client sites connect to the three VisaNet data centres with two connection paths per data centre that are geographically separated and supplied by two independent network providers. In our annual tests of failure scenarios, we ensure the system can withstand the simultaneous loss of the European data centre plus one of the two other data centres used for contingency payment processing, proving the service can be maintained throughout any 'severe but plausible' failure. Visa also has extensive protocols to recover and learn from incidents, including detailed response and recovery plans and processes for all operations.

We also take a full end-to-end approach to risk in our payment network. This means we mitigate risks across all stakeholders in transactions processed by VisaNet, to help ensure consumers and merchants can make payments without disruption even if another player in the value chain suffers an outage or cyberattack. For example, in the event of disruption at an issuer, Visa can and regularly does 'stand in' and approve or decline transactions on the issuers' behalf. In the highly unlikely event that all three of Visa's data centres were to fail, we also have a system in place whereby acquirers can similarly 'stand in' for Visa.

Contact: Emily Rayment, Director – Government Engagement, Nordics & Baltics