Trilogues on the Digital Euro Regulation

Mastercard's position

Executive summary

- Position the digital euro as a complement to Europe's payments ecosystem, preserving consumer choice and private-sector innovation.
- Establish sustainable compensation and clear, independent governance for the ECB's different roles.
- Reuse existing acceptance infrastructure and standards wherever possible, minimising duplication and preserving scope for innovation.
- Ensure proportionate, workable privacy, fraud, AML/CFT and implementation rules.

1. Sustainable compensation and commercial flexibility

- **Begin with a transitional market-based model lasting at least five years; ten years would be optimal.** Domestic and international consumer cards should be the practical benchmark. Fees should leave merchants and payment providers no worse off than with comparable methods, guiding the overall level rather than imposing a transaction-by-transaction cap.
- **Use the transitional period to build evidence for a permanent model.** A permanent methodology should follow reliable cost and volume data, an independent impact assessment and market consultation. The Commission should establish it with appropriate ECB technical input.
- **Design the permanent methodology to sustain a diverse, competitive market.** It should allow issuers, acquirers and other intermediaries to recover efficiently incurred set-up, connectivity, operating, fraud, compliance and capital costs, with a reasonable margin. Merchant service charges and inter-PSP fees should be assessed separately. The methodology should reflect differences in scale, services, operating models and market conditions rather than rely on a uniform fee level.
- **Preserve commercial flexibility.** Value-added services should remain outside regulated basic-service fees and be separately priceable. Commercial digital euro use should remain outside the basic-services regime.

2. Interoperability, distribution and innovation

- **Build on proven payment infrastructure wherever possible.** The digital euro should work with existing acceptance terminals, established standards and widely used EMVCo specifications wherever they meet policy, security and operational objectives.
- **Minimise unnecessary duplication.** New infrastructure or standards should be introduced only where existing solutions cannot meet clearly identified requirements, reducing cost and complexity and supporting merchant readiness.
- **Keep the framework open to different user interfaces.** Legislation should set outcomes and interoperability requirements rather than prescribe or exclude interfaces, allowing banks and payment providers to develop appropriate solutions.

- **Maintain open and competitive distribution.** Banks, payment companies and technology providers should connect on fair, reasonable and non-discriminatory terms. PSPs should remain responsible for customer-facing and secure, user-consented value-added services.

3. Clear separation of the ECB's roles

- **Require enforceable functional separation in legislation.** The ECB's monetary, supervisory and oversight functions should be separated from its roles as scheme owner, standard setter, infrastructure coordinator and procuring counterparty.
- **Provide independent governance and accountability.** Separate decision-making, staffing and information barriers, supported by transparent procedures and external scrutiny, should prevent conflicts of interest and preferential treatment.
- **Ensure structured market involvement.** PSPs, schemes, merchants and technology providers should have ongoing input into the rulebook, technical standards, pilots, procurement and change management.

4. GDPR alignment, privacy, fraud and AML/CFT

- **Apply the GDPR consistently to the digital euro.** The Regulation should not create an additional privacy regime and should confirm that all lawful grounds under Article 6(1) GDPR apply equally to digital euro services.
- **Provide legal certainty for necessary data processing and sharing.** Personal data should be processable and shareable, in accordance with the GDPR, for contract performance, fraud prevention, cybersecurity, compliance and user-consented value-added services. The roles and lawful bases of PSPs, the ECB and support functions should be clear.
- **Protect privacy without weakening security and fraud prevention.** Privacy-by-design and data minimisation should remain compatible with authentication, fraud monitoring, cybersecurity, sanctions screening and other legal obligations. Central-bank access to identifiable transaction data should be strictly limited.
- **Make offline AML/CFT obligations proportionate and workable.** The final text should clearly allocate responsibilities among the ECB, EBA, AMLA and PSPs and avoid gaps in financial-crime controls or unequal rules for public and private payment solutions.

***