



AGE Platform Europe feedback on Digital financial inclusion (item 3), Fraud prevention and detection (item 4) and High level product description (item 5) presented at the 8th ERPB technical meeting on 12/05/2023

Item 3: Digital financial inclusion

AGE Platform Europe (AGE) warmly welcomes the attention paid to digital financial inclusion in the context of the digital euro project and fully support the proposed approach.

- **Completeness:**

The proposal seems rather complete at this stage of the discussions.

We appreciate particularly the clear definition of what digital financial inclusion means and why it is essential to take action to foster access to and usage of the digital euro for the 40% of EU adult population who currently do not use internet for banking services for various reasons.

The list of citizens groups at risk of digital financial exclusion is also quite comprehensive and describes the main categories of citizens who are at risk of financial digital exclusion.

We welcome the reference to the need for the digital euro to comply with the European Accessibility Act (EAA). The EAA is indeed a binding EU legislation for both EU institutions and national actors. It aims to improve the functioning of the internal market for accessible products and services by removing barriers created by divergent legislation. Hence the need for the digital euro to draw the lesson from the current barriers preventing access to and usage of many digital retail payments solutions available across the euro area, and to adopt a pan-European approach as this is the only way to deliver a harmonised UX including in cross-border situations.

Ensuring that the digital euro will be inclusive by design will avoid a fragmentation of inclusion solutions across member states and supervised intermediaries, and will ultimately benefit both the demand and supply sides by delivering more effective and cheaper interoperable inclusion solutions.

We also welcome the proposal that a public or private dedicated licenced entity should be mandated by each member state to provide access to inclusive digital euro services to those at risk of digital financial exclusion, free of charge for eligible individuals. Yet restricting



access to free of charge basic services to eligible individuals contradicts the first principle of the proposed compensation model outlined on slide 29 of the high level product description which is: **Free basic use by private individuals**. We would like to recommend to stick to the initial principle of free basic use by private individuals – perhaps up to a reasonable limit in terms of volume of transactions per month, rather than limit access to ‘eligible’ individuals belonging to the groups of consumers at risk of digital financial inclusion. Such restriction would require a clear definition of who is eligible which might be difficult to implement, and may exclude individuals who do not strictly meet the definition of ‘eligible’ individuals.

Finally, we would like to recommend to add fraud prevention/management in the list of tools foreseen to enhance digital financial inclusion (slide 6). For ex. in the first column, the app should include an easy process to report suspected fraud to the supervised intermediary and it should be possible to easily block one’s physical card in case of loss or theft. In the 4th column ‘Advocacy’, targeted educational campaigns should include campaigns on what consumers can do to avoid fraud and report loss/theft of their D€ device or fraudulent transactions as well as how to seek redress.

- Synergies

In our views there are obvious synergies between the digital euro inclusion measures and initiatives/measures taken in the framework of the [EU Digital Inclusion Strategy](#) and its recently adopted initiative on [Digital rights and principles: a digital transformation for EU citizens](#). Synergies could notably be built with the following EU activities implemented in the framework of the EU Digital Inclusion Strategy on:

- accessible ICT: making ICT more accessible for all and fostering the development of accessible technologies
- assistive technologies: supporting the development of ICT that assists people with disabilities in the digital world

- Trade-offs

We welcome the public approach proposed by the Eurosystem to ensure that every eligible individual will have access to a digital euro account and basic services free-of-charge. We do not feel however that this inclusion objective should rely on a single dedicated licenced entity per country as national specificities and population’s needs vary a lot between member states and may require to licence more than one entity to cover all groups with inclusion needs. For ex. a public bank and national post offices offering basic bank services and access to cash could be dedicated licenced entities to ensure the broadest geographical coverage possible.

We would like also to stress that inclusion measures should not become the sole responsibility of those public or private dedicated licenced entities. Accessibility and

usability of all digital euro services should be fostered by the pan European inclusive design of the digital euro and supported by all supervised intermediaries, bearing in mind that the European Accessibility Act will apply to all PSPs, not only to the foreseen dedicated licenced entities.

Item 4: Fraud prevention and detection

AGE shares the view that a solid prevention and detection mechanism needs to be developed to ensure a safe and secure digital euro. This is an essential element to guarantee a sustainable digital euro in the longer term.

We agree with all key activities proposed on slide 7. We would like however to highlight the importance of fraud reporting by PSPs. Obviously not all consumers complaints will prove to be fraud cases, but reporting as required by PSD2 is not optimal today ([EBA/DP/2022/01](#)). The digital euro should seek to improve fraud prevention/detection and be able to quickly accommodate emerging risks.

- ECB functional analysis and proposed role for a central fraud support service (CSS)

We agree with the ECB analysis of how fraud can best be tackled in the framework of the digital euro and we are happy to see on slide 9 that end users (individuals and businesses) are listed among actors with key roles involved in fraud management. Yet the role of end users is missing on slide 10. Consumers can play a key role by reporting suspicion of fraud and help prevent fraud by reporting loss or theft of their D€ device (card, smartphone or tablet).

We agree with the proposal to set up a CSS and feel that option 3 is by far the best option to complement supervised intermediaries fraud prevention and detection measures. All stakeholders - including the supervised intermediaries - will benefit from the CSS real-time monitoring and risk-scoring of transactions and the role it will be able to play in real-time fraud detection. Option 3 should thus be deployed as soon as possible and ideally for the initial launch of the digital euro. Otherwise the risk is high that poor UX with fraud management will hamper take off of the digital euro and deter new end users to adopt the digital euro who may think that option 3 is a mere fix-up of an ill-designed digital euro.

- Potential opportunity for PSPs to combine (specific) digital € fraud case information, with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP

At this stage this proposal seems to make sense but action will be needed to ensure that supervised intermediaries get quickly acquainted with the digital euro specific fraud reporting process. More generally fraud reporting on all retail payment means needs to improve to enable comparable data between means of payments and countries.


- AGE suggestions to complement the fraud prevention approach

Citizens at risk of digital financial exclusion are known to be at a higher risk of fraudulent transactions and manipulation by fraudsters. Fraud prevention and detection measures need therefore to be developed to adequately protect all digital euro users including the identified vulnerable groups of consumers. This can be achieved through regular and easy-to-understand communication about fraud risks and how to avoid them, and easy tools for consumers to report fraud and block their D€ account/digital euro card.

Item 5: High level product description

AGE welcomes the high level product description and congratulates the team who has been able to integrate a long list of written feedback and oral comments from the technical sessions. Points still to be discussed are also well identified.

Below are a few minor comments/suggestions concerning a few slides:

- Slide 20: The last bullet point reads: “Funding *and defunding* should be possible from accounts held at **PSP other than the digital euro servicing PSP**”. We would like to recommend to specify that this bullet point concerns both funding and defunding as the bullet points above. (We fear that readers may interpret the icon  as a warning that this bullet point only concerns funding while the above bullet points concern both funding and defunding)
- Slides 37 – 41 on Digital financial inclusion: As said earlier we are very pleased with the attention paid to digital financial inclusion issues and only have a few minor suggestions to make (see on page 1 above our feedback on item 3).



AGE work is co-funded by the **Citizens, Equality, Rights and Values Programme** of the European Union. The contents of this document are the sole responsibility of AGE Platform Europe and cannot be taken to reflect the views of the European Commission. Transparency Register ID: 16549972091-86

BEUC response to ERPB written procedure on digital euro following ERPB technical session of 12th May 2023

1. Financial inclusion considerations of a digital euro

1.1 Completeness: which other aspects would need to be considered to make the digital euro as inclusive as possible?

BEUC highly appreciates ECB reflections on financial inclusion and the broadening of the concept of inclusiveness beyond access to a bank account.

As regards the different measures proposed:

Form factors: BEUC supports a public digital euro app which is fully compliant with the EU Accessibility Act. In addition, the provision of a physical digital euro payment card will be very important. It will provide a payment instrument which is independent from possessing and being able to use a smartphone or other digital devices. The physical payment card should be fully functional for all use cases as regards payments and (de)funding. Following the discussions on the digital euro rulebook, it is important that the card could also be used as an authentication element for online payments (e.g. e-commerce). It would allow consumers to use the card in combination with chipTAN and therefore provide a secure but smartphone independent authentication method.

Eligibility criteria to access payment cards: BEUC regrets that the provision of physical cards free of charge is subject to (yet to be defined) eligibility criteria. Due to its social dimension, this could lead to fragmentation across member states with regards to who gets access under which conditions. This would jeopardize the objective of creating one digital euro for the single currency area. Beyond the bureaucratic hurdles which eligibility criteria will produce for vulnerable consumers, not having access to a payment card free of charge will reduce the attractiveness of the digital euro for a large part of the population. According to the ECB SPACE study¹, in 2022, card payments represented next to cash the dominant payment means (34% at the point of sale, 51% online). Conversely, the share of mobile apps represented overall 3% of all payments in 2022. We expect that these payment behaviors will not change dramatically in the near future and hence the digital euro should be adapted to these consumer preferences.

Onboarding and portability: BEUC welcomes that in-person onboarding will be required for all PSPs. For consumers using only cash-like transactions such as offline transactions and lower-value online transactions, lighter onboarding requirements should be considered (as supported by the ECB in advocacy actions for the legislative proposal). Current de-risking practices by PSPs (to combat money laundering) lead to denied onboarding and offboarding of certain consumer

¹ https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.spacereport202212~783ffdf46e.en.html

groups e.g. homeless people without permanent address or refugees/asylum seekers but also residents from other EU Member States.² Lighter onboarding requirements than currently for cash-like transactions similarly to Article 12 of the 2015/849/EU (Anti-Money-Laundering Directive) should be considered. This would contribute also to increased privacy.

Functionalities: BEUC supports the proposal to offer basic services of a digital euro account free of charge. Basic services should include all services which are required to render a digital euro account fully functional. In our view, the basic services should therefore correspond to the basic features of a basic payment account which include the provision of a payment card usable for online and offline transactions.³ BEUC supports the possibility to (de)fund digital euros with cash without the need for a smartphone. This possibility should be widely available and free of charge.

BEUC supports the provision of “customizable account settings” for budgeting and automatic functions. According to a study by BEUC’s member vzbv in 2022, budget management is named as the most important reason to use cash by 35% of consumers.⁴ This is in line with the findings of the recent ECB study on digital wallets⁵ where the focus group of underbanked consumers highlights the importance of a top-up functionality similar to prepaid cards. The same focus group expressed the fear that the waterfall functionality makes budget management more difficult (e.g. risk to overrun linked bank account). It is therefore important that the digital euro allows for the top-up functionality and a digital euro is fully functional without the waterfall functionality (automatic top-up via the commercial bank account). In addition, the study shows that many “underbanked” consumers are afraid of making mistakes/fear fraud when using online banking. Hence, customizable account settings should include the possibility to set transaction limits which are difficult to overrule.

BEUC supports the offline functionality both for financial inclusion and privacy reasons as already expressed in previous rounds of comments.

Public approach: BEUC supports the addition of dedicated onboarding channels via public entities which would provide necessary supports to those at risk of financial & digital exclusion.

BEUC welcomes the availability of human interaction to guide consumers throughout all steps of the digital euro (incl. dedicated customer services) via public entities. It needs to be further defined what is meant by availability. Consumers should receive a satisfactory service in terms of geographical availability, opening hours etc. as well as quality requirements such as services adapted to the needs of different vulnerable groups.

² Commission report on the Payment Account Directive: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0249> and EBA Guidelines on to challenge unwarranted de-risking and safeguard access to financial services to vulnerable customers: <https://www.eba.europa.eu/eba-issues-guidelines-challenge-unwarranted-de-risking-and-safeguard-access-financial-services>

³ Payment Account Directive (2014/92/EU), Article 17, point d ii).

⁴ https://www.vzbv.de/sites/default/files/2021-12/2021-12-03_Chartbericht%20Bargeld_3.0.pdf

⁵ https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230424_1_annex~93abdb80da.en.pdf

As flagged above, consumers should not be prevented to use public intermediaries by setting up eligibility criteria. Such criteria will be a significant administrative hurdle for vulnerable consumers and risk excluding consumers from accessing the public service as different grades of financial literacy might not be well-reflected. As adequately reflected in slide 3, there are 40% of adults in the EU who do not use internet for banking services. In addition, there are different grades of usage, many consumers use a payment card to pay online but do not use online banking. Similarly, some consumers use a smartphone for basic messaging services, but this does not mean that they are able or feel at ease to use a smartphone for online banking.

1.2 Synergies: which opportunities for synergies do you see for the digital euro inclusion measures and other initiatives addressing digital financial inclusion?

Synergies with access and acceptance of cash: Cash remains the preferred payment method for many consumers. It is thus important to keep an efficient cash infrastructure alive to respect consumers' preferences. This requires a dense network of ATMs and bank branches as well as the obligation for merchants, public services and essential services such as healthcare and public transport to accept cash. At the same time, our society becomes increasingly digital where many goods and services, including public services are offered online. Consumers who cannot pay digitally nowadays cannot access these goods and services.

From a consumer perspective, we see the following synergies:

- Reinforce the existing cash infrastructure by setting up a public digital payment method which is accessible via a broad network of ATMs and bank branches, including public intermediaries. This will improve both the access to cash and digital euros.
- Replicate the characteristics of cash when designing a digital euro to ensure that consumers who use mainly cash gain access to a digital way to pay.
- Ensure that there is a public payment method, both for offline and online payments which guarantees that consumers do not have to rely solely on private providers to pay for goods and services.
- A well-defined obligation to accept both cash and digital euros everywhere (legal tender).

Synergies with the access to a basic payment account: Everyone should have access to a payment account. From a consumer perspective, this could also be a digital euro account. Given the ECB plans to provide basic services free of charge and setting up public entities to offer such accounts to vulnerable consumers, the digital euro could further contribute to achieve the objective of financial inclusion. For example, in some countries, basic payment accounts are still far more expensive than normal bank accounts⁶ and many banking services which rely on cash or paper-based transactions are way more expensive than equivalent digital services.⁷ If these services are offered free of charge, the digital euro will contribute also economically to financial inclusion.

⁶ <https://www.test.de/Basiskonten-im-Test-4936098-0/>

⁷ https://www.arbeiterkammer.at/beratung/konsument/Geld/Konto/AK-Bankenmonitoring_2023.pdf

1.3 Trade-offs: which challenges do you see in implementing the suggested measures, if any?

Financial and digital inclusion should be considered as a genuine public interest which should be considered more important than possible considerations on competition with offers from private intermediaries.

2. Fraud and risk management

2.1 Does ERPB share the view from the functional analysis, with a role for a central fraud support service (CSS)?

BEUC supports the ECB in pursuing a central fraud support service (option 3). Consumers are increasingly exposed to online fraud⁸ and to ensure consumer protection, the digital euro should ensure the highest level of fraud prevention mechanisms. It remains important that next to a central fraud support service which looks on fraud cases across different PSPs, individual PSPs have their individual fraud prevention management in place and remain liable for unauthorised payments.

In addition, a high number of fraud cases identified with a particular PSP has a reputational impact on the digital euro as a whole and the trust consumers will place in the digital euro as a payment method. To ensure a high level of trust and consumer protection, where the ECB identifies a high number of fraud cases, enforcement measures should be taken towards the responsible PSP to ensure that fraud prevention measures are improved and that there are adequate incentives for all PSPs to set up strong fraud prevention measures.

A proportionate approach should be taken with transaction monitoring for offline transactions ensuring full privacy and increased fraud management for online transactions/higher transaction values.

2.2 What is ERPB view on potential opportunity for PSPs to combine (specific) digital € fraud case information, with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP?

No reply given that this question is targeted to PSPs.

2.3 Would ERPB have any suggestions to complement the fraud prevention approach?

Following the introduction of an IBAN name check for instant payments via the SEPA regulation, it should be ensured that such a name check is also implemented for the digital euro. Similar fraud checks should also be available for other ways of digital euro payments initiated by the payer (e.g. alias). In addition, when launching the digital euro, there needs to be clear communication about the project and the difference between a central bank digital currency and crypto assets. When searching for example for eKrona on different internet browsers, there are a lot of offers for crypto assets called also eKrona. The ECB should integrate clear

⁸ https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-027_A_payment_fraud_epidemic.pdf

communication lines when launching the project to avoid that fraudulent crypto asset providers can take advantage of the launch of the digital euro.

3. Digital euro holistic design review

The digital euro should become an attractive payment instrument for consumers which replicates the characteristics of cash to ensure privacy and financial inclusion and which enables a truly European payments landscape. In addition, the digital euro should be developed as a public project in the interest of consumers. A digital euro should offer a public digital payment method. At the same time, consumers willing to pay with cash should be able to continue doing so meaning that a digital euro should not compromise access and acceptance of cash.

ECB design proposal	BEUC position
<i>Access and acceptance</i>	
Availability for everyone	Access to a digital euro should be as easy as for cash. Similarly to the objective of a basic payment account, all consumers should have access to digital euro account. To ensure higher privacy, lighter eligibility criteria than currently applying for bank accounts should be introduced for consumers using only offline transactions and lower-value online transactions.
Basic services free of charge	All services which are needed to render a digital euro account fully functional should be offered free of charge. The list of services should correspond to the basic features of a basic payment account and should be regularly updated with a view towards new features that will eventually be considered "basic". (De)funding in cash should be offered free of charge.
Right to human interaction	BEUC welcomes the availability of human interaction to guide consumers throughout all steps of the digital euro (incl. dedicated customer services) via public entities. In addition, Member states should have the option to endow consumer organisations and other relevant industry-independent NGOs with the task that already possess the infrastructure and know-how in supporting consumers in payments provided that they receive sufficient funding to fulfil this task. It needs to be further defined what is meant by availability. Consumers should receive a satisfactory service in terms of geographical availability, opening hours etc. as well as quality requirements such as services adapted to the needs of different vulnerable groups.
General acceptance (legal tender)	Next to cash, digital euros should be accepted by all merchants but also by public administrations and other services (e.g. doctors and hospitals, public transport, electric car charging stations). Should exceptions be introduced during the roll-out of the digital euro, they should be limited in scope and time.

Wide use cases (P2P, Point of sale, E-Commerce, Government payments)	BEUC welcomes the possibility to use digital euros in a wide range of use cases. However, there are still limitations in terms of payment instruments. For instance, consumers should be able to use a card in e-commerce as this is the most common payment method currently used online.
Prioritise euro area for first release	BEUC agrees to focus on the euro area for the first release of the digital euro.
<i>Cash-like features</i>	
High level of privacy	<p>BEUC supports a bearer instrument for offline use, in addition higher levels of privacy should also be attained for lower-value online transactions.</p> <p>Consumers must be in full control of their data and should not be penalised for not sharing data e.g. with their intermediary. BEUC thus welcomes that the availability and usability of basic services shall not be diminished when a user is not sharing data. BEUC agrees that the Eurosystem should minimise any use of data to essential tasks (e.g. settlement, fraud management).</p> <p>The degree of privacy that the digital euro will deliver, will likely be one of the key parameters against which Europeans will judge the new payment means.</p> <p>The digital euro needs to provide a higher level of privacy compared to existing digital payment needs. This has been a core promise of the whole project and repeated in many speeches time and time again. The Eurozone and the single market would highly benefit from a safe digital means of payment that impedes on practices of corporate surveillance.</p> <p>The digital euro needs an ambitious approach, including likely a dedicated enforcement regime.</p>
Facilitate budget management	<p>BEUC supports the objective to introduce tools to facilitate budget management given that for many consumers, this is a key reason to use cash. It needs to be clarified how the digital euro can facilitate budget management and it should be ensured that a digital euro account can be used conveniently without the waterfall functionality which renders budget management more difficult. Thus, holding limits should be set at a reasonable level allowing for an independent use of the digital euro account.</p> <p>Individuals should be able to set limits that cannot be easily altered for the sake of fraud prevention and a sense of control.</p>
Programmable money	Digital euros should be equivalent to physical euros (cash and banknotes), hence not limited to

	certain types of purposes (vouchers). Like the traditional euro, digital euro needs to be designed as money.
<i>Role of the Eurosystem</i>	
Central bank liability	Similarly to cash, digital euros should have central bank liability.
Immediately settled by the Eurosystem	Like cash and instant payments, digital euros should be immediately settled, facilitating also budget management. Given that digital euros will have central bank liability, the Eurosystem should take care of the settlement.
Standalone digital euro app	BEUC welcomes the development of a standalone digital euro app as a contribution to financial inclusion and allowing consumers to use digital euros separately from their commercial bank account.
Dispute resolution and fraud management	The digital euro should fulfil high standards of dispute resolution and fraud management. BEUC welcomes the ambitious approach taken in favor of a centralized fraud management system but regrets that the approach towards dispute resolution is currently less ambitious (e.g. exclusion of commercial disputes).
<i>Distribution and compensation model</i>	
Distribution by private and public intermediaries	<p>There is a risk that private intermediaries will make the digital euro unattractive for consumers given that it stands in competition with their private digital payment methods. BEUC has a preference for public intermediaries. BEUC welcomes in this regard the addition of public intermediaries. Such public intermediaries should be accessible to all consumers.</p> <p>There seem to be no specific requirements for PSPs to handle the digital euro. If Big Tech companies have a competitive advantage in providing digital payments (which they seem to have), the digital euro might not only not deliver on the objective of strategic autonomy but further undermine it.</p> <p>If private intermediaries are selected to distribute the digital euro, clear legal obligations should be attached to this task in terms of privacy and financial inclusion (e.g. availability of ATMs, bank branches, right to human advice).</p>
Compensation model for private intermediaries	As for any other public good (for instance: physical cash), the objective should not be to generate huge economic returns but to compensate PSPs for the costs when distributing the digital euro. When PSPs are not interested in distributing the digital euro under these conditions, an end-to-end solution which

	<p>public/non-for-profit intermediaries should be explored instead.</p> <p>The interchange cap of 0.2 percent could serve as a guideline, if any leeway for additional fees is effectively ruled out.</p> <p>Economic incentives should be paired with legal obligations to maintain a well-functioning infrastructure (ATMs/bank branches) in place.</p>
Easy portability/switching	<p>It should be easy to compare different intermediaries (e.g. public vs. private) and to switch between them.</p>
Financial stability	<p>BEUC can agree to targeted measures to ensure financial stability such as holding limits, deposit outflow limits, tiered remuneration and a limit of one wallet per citizen. However, the functionality and attractiveness of digital euro accounts for consumers should not be compromised by these measures (e.g. by a very low holding limit).</p>



Brussels, 15 June 2023

Digital euro

EACB feedback to ECB

Financial inclusion considerations

Fraud and risk management

Holistic design review

The **European Association of Co-operative Banks** (EACB) is the voice of the cooperative banks in Europe. It represents, promotes and defends the common interests of its 26 member institutions and of cooperative banks in general. Cooperative banks form decentralised networks which are subject to banking as well as cooperative legislation. Democracy, transparency and proximity are the three key characteristics of the cooperative banks' business model. With 2,700 locally operating banks and 40,000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 227 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 89 million members and 720,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

The voice of 2.700 local and retail banks, 89 million members, 227 million customers in Europe

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels

Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19

www.eacb.coop • e-mail : secretariat@eacb.coop



The EACB welcomes the opportunity to provide input to the ECB following 8th ERPB technical session on digital euro held on 12 May 2023. The consultation covers the following aspects of the digital euro project:

1. Financial inclusion considerations
2. Fraud and risk management
3. Holistic design review

The EACB's views on the consultation questions as well as a number of questions for clarification are presented below.

1. Financial inclusion considerations

Questions: We invite reflections in particular on the following questions:

- *Completeness: which other aspects would need to be considered to make the digital euro as inclusive as possible?*
- *Synergies: which opportunities for synergies do you see for the digital euro inclusion measures and other initiatives addressing digital financial inclusion?*
- *Trade-offs: which challenges do you see in implementing the suggested measures, if any?*

- The Payment Accounts Directive grants the right to all EU citizens to open a basic payment account with essential features linked to it. Thus, it is still unclear what the contribution of digital euro will be for financial inclusion.
- It is not clear whether the ECB is focusing on financial inclusion or digital inclusion. The level of financial inclusion is already high in Europe and we wonder how the digital euro will include more people. Digital inclusion is a totally different objective and should not be mixed up, especially not in argumentation.
- Slide 4: What are the reasons behind the figures presented by the ECB? Why are 13 million adults in EU unbanked? Because of price? Or are they more comfortable outside the financial system? Different reasons probably require different solutions.
- Digital inclusion is indeed a challenge as some features are required for a relatively small group of citizens. A European public solution for digital euro could reduce costs in general, because not all PSPs would have to develop and maintain the services that would fall under the general approach.
- Regarding the impact on people with disabilities: The close cooperation with the European Blind Union (EBU) during the currency design phase in the 1990s led to the development of euro banknotes and coins with features that visually impaired people can handle with confidence¹. As the digital euro would be the digital form of cash, how it would be ensured that visually impaired people can also use the digital euro? Is there a cooperation with EBU?

2. Fraud and risk management

Questions:

- *Does ERPB share the view from the functional analysis, with a role for a central fraud support service (CSS)?*

¹ <https://www.ecb.europa.eu/euro/visually/html/index.en.html>



- *What is ERPB view on potential opportunity for PSPs to combine (specific) digital euro fraud case information, with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP?*
- *Would ERPB have any suggestions to complement the fraud prevention approach?*

- The stakeholders should be seen much broader. All actors contributing to making a transaction happen should contribute to preventing fraud, for example, telecommunication companies. In the current infrastructure, PSPs are severely hindered in sharing fraud information also across industries.
- Option 3 could be the most efficient and effective one if the CSS is independent from the ECB to avoid privacy related (transaction) data going to the ECB.
- What does the ECB expect from supervised intermediaries during the different phases of the transition to the full option 3 version? Are temporarily used investments required by intermediaries?
- Combining (specific) digital euro fraud case information with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP could improve the process but relates to the privacy part.
- Irrespective of which option is used, it should be totally clear who is responsible for what and who is responsible for the reimbursements and what are the rights and responsibilities of the payer and the payee.
- Limitation of the transaction amount, limits also the risks involved. In other words, the required checks and controls are based on the transaction amount – low transaction amount requires little or no checks (and related privacy issues).
- The defined policies around fraud management have an impact on the implementation and running costs of the digital euro and should be part of the compensation model.
- The ECB slides lacks clarity on, after implementing as much fraud prevention as possible, who will carry the burden of the residual successful fraud of different types (the fraud that is not prevented). Note that in this respect the cash infrastructure has a completely different distribution of risk than cards or account-to-account.
- The ECB slides ultimately only deal with fraud prevention and detection. Other fraud related topics should also be dealt with, such as resolution, and establishing the fraud risk appetite for the infrastructure and individual participants.
- Some kinds of fraud are not addressed in the slides, such as fraud that would exploit technical flaws in the digital euro infrastructure (in this case, no payers or payees could be involved at all), and fraud that concerns the purchase rather than the payment (e.g. when you pay for a box containing a brick rather than a laptop).
- It should be noted that strict fraud management policies may impact financial inclusion, such as when former fraudsters are barred from participation in the infrastructure.
- Aspects of fraud management are tied more to the PSU than to the payment infrastructure(s) used.
- The upcoming revision of PSD2 should also be taken into account as it will have an impact on the fraud and liability issues. Fraud mitigation and prevention, security and operational resilience, measures to combat fraud more effectively, especially new types of fraud such as phishing, spoofing, and social engineering leading to APP fraud will be significant issues in that context.

3. Holistic design review

Question: We invite feedback on all aspects of the High Level Product Description. It will feed into the final documentation on which basis the Governing Council will assess the digital euro investigation phase.



- Slide 20: It is stated that "*Funding should be possible from accounts held at PSP other than the digital euro servicing PSP*"? Does this mean that the digital euro servicing supervised intermediary (who was responsible for the onboarding) should offer services that the funding of a digital euro account takes place from an account which is not in the books of that supervised intermediary? Which means that the digital euro account would be linked to an account with another PSP? But also the other way around: This is a tricky one and could potentially give BigTechs the front-end leaving the banks performing the administration. Cross-PSP reverse waterfall seems to be instantaneous and atomic (an undivided part of a transaction). No details are provided on how this could be implemented and how this would fit the legislative context of PSD2 regarding e.g. authorisation. For us it seems a very complex structure. We suggest to have only waterfall connectivity with an account maintained by the supervised intermediary which is also providing the linked current account. In case of account switch of the commercial bank account, the digital euro wallet should also switch.
- The ECB slides do not seem to address fundamental issues that arise from holistically reviewing the isolated design choices:
- How is the digital euro 'always a liability of the central bank' if at the same time the Eurosystem is not 'seeing holdings nor tracking payments to single user'? This implies that keeping track of the evidence for the PSU's holdings is someone else's liability (most likely the intermediary). Also, fraud resolution liabilities seem to be on the intermediaries. This fundamentally impacts the foundational concept of the design to provide pure central bank liabilities to the general public in a digital form.
- Slide 4: How would the digital euro bring 'increasing resilience' without extra costs for society? What would the digital euro add to the current resilience of payments in euro (commercial bank money and coins and banknotes)?
- Slide 5: Which benefits does the ECB see for the three groups (citizens, merchants, intermediaries)?
- Slide 8: What would the legal tender status of digital euro add for merchants and intermediaries?
- Slide 10: Would government payments be allowed for non-individuals such as businesses and self-employed?
- Slides 11 and 44: On these slides it is stated that the holding limit will be decided close to launch. Who will decide on that, the ECB or the co-legislators? We also want to stress that without a low per-user cap (maximum € 500) on the potential holdings of digital euros, it could render the financial system very unstable in a scenario where a shock induces bank runs and large scale flight-to-safety flows to the digital euro, in which case healthy banks and other financial institution will collapse in rapid order. Please refer to the EACB's earlier comments related to the potential impact of a digital euro on cooperative banks and financial system as a whole.
- Slide 23: How would "*Easily porting the digital euro holdings from one PSP to another*" increase resilience? What is the benefit compared to the current way of working with commercial bank money?
- Slide 30: Will the consumer bank be compensated for all the costs for providing the service? If yes, does that mean that the merchant pays the costs (as a fee to the merchant acquirer) for both the costs of the acquirer and the consumer bank? How does this relate to the commercial bank products? What are the incentives for the issuing bank to offer digital euro services to retail clients?
- Slide 31: With regard to the compensation model, who decides on potential 'price caps'? Are they related to reasonable costs? Are they equal in all European countries?
- Slide 32: Is (reverse) waterfall via another PSP than the digital euro servicing PSP also part of the basic services?
- Slide 33: Price-based tools: From our perspective, the digital euro holdings should be without remuneration. It goes, amongst others, in conflict with privacy.



- Slide 39: Why is it important to raise the figures of use of internet banking services? Why is usability the key step? Maybe (part of the) citizens who currently don't use internet for banking services, do so deliberately and for different reasons?
- Slide 41: Why should (de)funding be free of charge? Does that mean that every supervised intermediary would be obliged to deliver this functionality? From our perspective, (de)funding via cash could be charged, as the current situation with commercial bank money.
- Slide 44: We support the suggestion to explore the investment cost on the basis of the design of digital euro, however a clear position of the issuer (ECB) is required upfront. Not about the detailed amount, but about the starting points and methodologies to determine the cost. Otherwise providing a more detailed feedback is not possible.
- The whole 'compensation model' only looks at transactions. Banks would also lose interest income (deposits would flow to the ECB), would have to invest to make the digital euro available and keep it running and make a lot of costs onboarding customers. The compensation model should take into account the broader effects of introducing a digital euro.
- The compensation model principles do not provide insight in how intermediaries of different profiles (issuer, acquirer, bank, non-bank, providing other payment services to the PSU or not) could build a viable business on the main negative assumptions of the model: no income from individuals (from free basic use), no settlement cost, no significantly higher inter-PSP fees, no significantly higher merchant fee income. No proof is presented that it is possible to design an infrastructure that is attractive for all parties involved.
- The feasibility of the overall plan, even if rolled out in a staggered approach, requires further analysis, as the scope of ambitions is very large and includes almost all currently known payments infrastructure functionality as well as new functionality such as the waterfall concept and offline. Would it be feasible to implement? If implemented, would it be likely to attract users and transaction volume in a free market competitive setting vis-à-vis commercial payment infrastructures?

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department (m.vanberkel@eachb.coop)
- Mr Farid Aliyev, Senior Adviser, Payment Systems (farid.aliyev@eachb.coop)

19 June 2023

ERPB written procedure on holistic review

EBF response

EBF response to ERPB Written Procedure on digital euro holistic review: high level product description

Alignment of the design with the strategic objectives of the ECB

The EBF appreciates the opportunity to comment on the digital euro high level product description, which comes after one year of structured and time-intensive engagement with the industry, on multiple complicated issues, wherein what was mostly possible to offer was initial views and assessments.

What follows below is intended to be considered as key issues hopefully to be **addressed together by the ECB and the banking sector, in a true open strategic dialogue, before the forthcoming Governing Council decision in the autumn.** The continued absence of such a dialogue is to the detriment of the digital euro project and risks compromising its success. Moreover, at this bringing-it-all-together stage, it is also very important for the industry to have clarifications on the criteria by which the previously submitted responses on the different design elements have been taken into account or discarded.

As a starting point of our analysis of the holistic review, we emphasize the importance of assessing the digital euro design functionalities against the originally stated ECB objectives for the issuance of a retail digital euro. We find that, in many respects, the 'big picture' of how the digital euro would fulfil its strategic objectives and how it would fit in the European payments market, is still missing. More specifically:

- In order to **preserve the monetary anchor role of the euro, protect Europe's strategic autonomy and foster innovation**, the digital euro must be attractive to users, offering innovative solutions that are not available today (or could not be available in the near future) with account- and card-based services.

These objectives sound reasonable on paper, but it is still not clear to us to what extent these are actual problems that can be addressed only by a digital euro. In particular, although preserving the monetary anchor is the main argument to create a digital representation of the euro and to enable citizens to hold it, there has not been public debate about this concept, which is not at all obvious. Also, it appears reasonable to preserve citizens' access to public money, as a public good. However, there are many open questions that should be analysed to assess if the digital euro responds (and is the only way to respond) to this objective. **Given the significant effort and cost that implementing a digital euro will entail, we would like to see further analysis from the ECB that supports these motivations before the decision to move ahead is made.**

- **A digital euro that simply replicates use cases already covered by other payment instruments does not stimulate innovation.** To achieve that, it should be built in such a way as to enable new use cases: **the digital euro must act as a raw material** to accelerate the European digital economy. It should be built as a new form of central bank money but not as a new payment solution / payment option, while the distribution and access to it should be via existing or new payment solutions built and operated by the private sector. Moreover, if the

digital euro is to be an answer to foreign CBDCs and private stablecoins, it must enable conditional transactions typical of these solutions, otherwise it will be by default less attractive to users. As mentioned also in the EBF contribution on the financial inclusion questionnaire, the design of **the digital euro should be attractive also to the more advanced and tech-savvy segment of the population and businesses**. These are in fact the segments most likely to look (or already looking) for innovative payment solutions. Therefore, the efforts to include features aimed at financial inclusion should not be to the detriment of designing the digital euro as an innovative raw material upon which intermediaries may develop advanced services meeting the needs of those user segments.

- The **overlap with the current payment instruments**, especially considering that digital euro basic services will be free of charge for individuals, risks cannibalising the payment services offered by intermediaries, with the result that the related **investments already made** – and the ones which are ongoing – **will be wasted**. In this respect, **we strongly recommend the ECB to work with the market on an impact study of a digital euro on the payments market before any design decision is made in a definitive manner**.

Looking at the holistic review, we note the **absence of a very important aspect - infrastructure**:

- At this stage, it becomes **crucial to clarify the underlying technology and infrastructure model** envisaged for a retail digital euro. These will be crucial in terms of the cost and the effort that will be required by intermediaries to provide digital euro services, and they may condition the use cases and the degree of innovation that the digital euro could facilitate.

The infrastructure required for the development of the digital euro is an essential aspect for intermediaries to estimate the costs of its development and deployment. However, since the market research disclosed in February 2023, the ECB has neither followed up nor asked for any specific feedback regarding this topic. In particular:

- Further clarifications should be shared on connectivity between intermediaries and the Access Gateway via internet or NSP, since both the implementation cost and the level of security and resilience in the two channels is considerably different.
- Even though some aspects of the infrastructure are being discussed on specific workstreams of the Rulebook Development Group, this discussion should take place more widely. It is crucial that banks and other intermediaries participate in it, to assess potential impacts and opportunities of the different design options.
- As an initial approach and as long as the digital euro is focusing on existing use cases, we believe that leveraging as much as possible on existing instant payments infrastructure and existing payment processes and components should be a fundamental consideration by the ECB when reflecting on the digital euro infrastructure. To that end, a thorough investigation would need to take place. Building on the current infrastructure would provide some advantages, e.g. regarding the costs of deploying the digital euro for intermediaries (adaptation of POS terminals, etc.), which can be considerable. In comparison to creating a completely new infrastructure, reusing the existing ones would be the most cost-efficient and time-efficient

way to deliver to consumers across Europe the digital euro and support ECB in materialising its goals in a faster and more predictable time frame. .

- Related to this topic, the ECB has presented in the prototyping exercise an UTXO data model for the back-end prototype for online payments. We understand that this approach does not mean that any decision has been made in that respect. However, we have some concerns about this potential approach that we would encourage the ECB to clarify:
 - We would like to discuss if and how this model would be compatible with the ISO 20022 standards. The SCT Inst scheme is based on the use of ISO 20022, which is the (very extensive and standardised) format that standardises the financial messaging (payments, cash reporting, cash management, etc) of the main market infrastructures (SWIFT, Target, EBA, CHAPS UK soon, Fedwire US in 2025...). Also, the pending legislation on instant payments will oblige all credit institutions to implement instant payments based on ISO 20022 before the digital euro can be issued. At the same time UTXO does not appear to be *per se* sufficient to enable innovative services (e.g., conditional payments).
 - The prototype refers also to self-custody wallets, “which could potentially allow for more privacy – pending legislative developments”, and to some kind of KYC utility, identity verification services, that “would facilitate digital identity proofing and customer onboarding in a technically standardised manner”. It would be useful to understand better the views of the ECB on this topic and to discuss with the industry those potential additional services.

Zooming in on the **design decisions that shape a digital euro** according to the holistic review, we note the following:

1. User experience for individuals and businesses

- With regard to the **roll-out approach**:
 - There is need for the ECB to share further information on **what the staggered approach would look like**, detailing what use cases will be part of each phase and specifying what user journeys are included in each of them. The staggered approach should be as simple as possible and very robust, and add functionalities as we learn from how the digital euro is used by citizens and merchants, and identify potential needs that require further functionalities. Once the first release is achieved, we will be able to upgrade it and move to other services that involve increased complexity to the market. The roll-out approach (and the ongoing work within the Rulebook Development Group) should clearly prioritise the user journeys envisaged as part of the first release.
 - We also believe that **the use cases that have been prioritized for a digital euro can also be served by instant payment solutions. Therefore, synergies between the digital euro and instant payments should be sought** by leveraging on the infrastructures and solutions already in place or being developed for instant payments (rather than building new ones from scratch for the digital euro). This includes front-end solutions already very successfully in place in some euro area countries and

those that will be deployed shortly in some other countries. There is no need for a dedicated front-end interface solely for the digital euro for the users of such front-ends. For instance, the ECB includes as “supporting services” introducing an “*alias lookup to minimize use of data in settlement component. Not to be operated by Eurosystem*”. We propose to: (1) Reuse existing Proxy Lookup systems. Instead of developing a new centralized directory, we suggest to interconnect national solutions, which would reduce adaptation costs and provide huge synergies in terms of development and maintenance, and consider the EPC SPL framework. (2) Reuse the figure of the Instructing Party (IP) that serves for the instruction of the TIPS messages.

- With regard to the **offline functionality**:
 - In some countries **existing card and wallet solutions for use at POS are already built with the default assumption that the payer or/and payee have no or limited network connectivity**.
 - Should the offline functionality of the digital euro come as a separate structure, with no visibility for intermediaries, **some critical issues will need further investigation**. In the offline scenario, holdings are stored in a secure device and require prefunding. With this configuration, it is not clear: i) how the offline balance can be displayed in the intermediary app; ii) how an offline transaction can be executed within the intermediary app; iii) how the controls on the holding limit balance would be put in place; iv) who would be responsible for that. Even if there is the possibility to set a limit on the number of digital euro online that can be converted to offline, an offline device can receive incoming payments, potentially overcoming the threshold set for the holding limit. Therefore, it should be verified whether the device itself can monitor the available amount. Moreover, it is necessary to put limits on offline payments, so as to avoid fraud and maintain same AML control as is the case today for digital payments. It is logical that, if transactions are made without the involvement of PSPs, also the disputes need to be resolved without them. Additionally, the architecture of the feature and how it ties into the online digital euro functionalities requires further elaboration. Furthermore, as PSPs have to comply with AML/CFT rules, they need to have visibility on the information on the payee/payer and this cannot be performed on all offline transactions, increasing ML/FT and fraud risks. Finally, if offline features are to be implemented, they should not be included in the first release because the development of such functions is very costly and time-consuming. The fact that offline functionalities should not be included in a first release is further strengthened by the outcome of the ECB prototyping exercise which is that *“However, questions remain as to whether the existing technology is capable of delivering, in the short to medium term (five to seven years), a production-ready and secure offline solution in line with the Eurosystem’s requirements and on the scale foreseen for the digital euro.”*

2. Making digital euro available: a public-private collaboration

- With regard to **the role of intermediaries**:
 - The **repartition of roles between Eurosystem and private sector should be revisited** as the work carried out at present on the Rulebook seems to deviate from the distribution option principles, where the

relationship with the customer should always remain with the distributing intermediaries that should be free to set their own products for the digital euro, provided that the basic principles to ensure a homogeneous feeling for the user are respected.

- For (de)funding, the possibility to fund from accounts held at a PSP other than the digital euro servicing PSP should not be permitted, as it increases the operational complexity and possible risks without adding significant value.
 - It would be also important to specify the functionalities allowed to each intermediary so as to clarify potential differences between credit institutions and other PSPs. In view of such differences, the need for stricter regulatory requirements across all PSPs should be explored, in order to establish an equal level of regulatory requirements for all intermediaries of the digital euro, ensuring that **all of them fulfil the same guarantees to intermediate a public means of payment.**
 - Funding and defunding in cash should not be a mandatory feature, since not all intermediaries handle cash. This functionality would result in added operational complexity, particularly as regards the management of the (reverse) waterfall part, and new questions would arise in case of fraud or disputes management. Moreover, it should not be free of charge, since it entails high costs for intermediaries.
- With regard to the **compensation model:**
 - **The proposed compensation model is currently built around transactions, and hence ignores non-transaction related costs and revenues lost.** These non-transaction related items however cover the large majority of the costs concerned. Relevant costs, for which compensation should be considered include e.g. interest income lost due to funding moving towards the digital euro, and package fee revenues lost¹. Other non-transaction related costs include start-up investments, maintenance costs, fraud and redress, tax and supervisory reporting duties, and many more. This means that the compensation model in its current form is thoroughly lacking and needs to be made more comprehensive to cover both transactional and non-transactional aspects. The compensation model should be aligned with that of existing payment services. Incentives for issuers are essential in any payments market, to build network effects, and will be even more important in the distribution of the digital euro. The digital euro compensation model should ensure a fair competition with existing payment methods in order to avoid the risk of marginalizing or crowding out existing payments solutions.
 - **The list of core and optional services needs to be revisited** as it was set at a time where the implications of the functionalities were very unclear, and the principles of the compensation model not known. For example, there should be limits both on the amount and on the number of transactions, while funding in a given period of time and waterfall operations cannot be provided for free. This would make the use of a digital euro infrastructure more viable economically. We also do not agree with some services being labelled as "core": for instance, recurring payments should be defined as an optional

¹ Source: Onderzoek naar de kosten en baten van het betalingsverkeer voor financiële instellingen 2021 (betaalvereniging.nl), p.57, showing that transaction-based revenues cover only 25% of the relevant revenues of payments in the EU.

service (as described in the third progress report) and be offered voluntarily by intermediaries. The concept of “core” cannot be equalled to “free of charge”, if it leads to an unsustainable economic model. This issue needs to be addressed with a thorough analysis and an appropriate compensation model needs to be discussed, including for core services, if necessary.

- It is clear that some basic services cannot be paid by end users, failing which the adoption rates will not be adequate for the public purposes that the digital euro is intended to achieve. At the same time, it is also clear that the **cost of building the infrastructure to enable the circulation of the digital euro, as well as the cost of its distribution, cannot be borne by private actors alone.**
 - A partial, additional solution to make the compensation model more robust could come from public support from a share of the seigniorage increase, as foreshadowed by the ECB itself, which could help sustain economic stability for private intermediaries. However, a predominantly subsidised model is not an economically sustainable model in itself and it must be studied carefully.
 - The compensation mechanism for digital euro transactions that use the reverse waterfall mechanism should be further investigated, especially in scenarios where the PSP holding the digital euro wallet (that would receive the inter-PSP compensation) is different from the PSP holding the payment account to which the digital euro wallet is linked (that in the current scenario would not be entitled to the inter-PSP compensation).
 - Given that a digital euro could significantly impact the intermediaries’ income statement, we would like to reiterate that their participation into the deep-dive sessions to design the compensation model is essential.
- With regard to **financial stability**:

It is important to set **low holding and transaction limits** to avoid an adverse impact on current monetary policy/commercial bank money. **In terms of transaction limits, we would suggest referring to average current cash holding** (according to the ECB SPACE study) **and payments instruments (e.g. daily/monthly limit for card spending)** and set limits on the maximum amount for each transaction and on the number of operations within a specific timeframe. In addition, it is important to consider the role of daily/monthly limits for containing fraud risks. Moreover, transactions using the reverse waterfall should not be higher than the overall holding limit. As to the possibility of including tiered remuneration in the mix of tools to control digital euro holdings, this would add unnecessary complexity and uncertainty, and would be ineffective during periods of crisis, as the sensitivity to interest rates can be very low in those cases: the interest rate of the second tier would need to be extremely penalizing to effectively prevent bank runs. In any case, if tiered remuneration is introduced, it should only be as a complement to fixed cap.

3. Privacy and data protection

Privacy stood out in the ECB public consultation of 2021 as the most important feature of the digital euro for European citizens. Therefore, the principle that **‘ECB does not see payment data’** requires further elaboration and is a key point to overcome doubts

and fears in the public opinion about the central surveillance capabilities of the digital euro infrastructure.

At the same time, it should be further stressed that intermediaries need to access users' and transaction data to ensure respect of AML/CFT rules, to prevent fraud and to provide services to their customers (ranging from refunds to any kind of value-added services) and always in compliance with the GDPR. It is therefore **crucial that intermediaries have access to payment transaction data in the same way as they currently do for digital means of payment.**

In addition, access to payment data allows banks to offer greater personalization and new value-added services, such as financial advice or sustainability-related recommendations. Therefore, consumers should always be able to decide whether their data from digital euro transactions can be used for additional purposes, as it is currently the case with other payment solutions. This is consistent with data privacy principles, by providing individuals with control over their data, as well as with the EU objective of promoting data-driven innovation in Europe.

4. Financial and digital inclusion

The added value of a "Eurosysteem digital euro app" remains unclear, especially considering that it would still need to connect to digital euro accounts at supervised intermediaries for users to access the digital euro. The rationale for how this would serve financial inclusion is very unclear and the same applies to the provision of a tool for smaller intermediaries. It is also noted that smaller intermediaries often rely on tech providers for the development and maintenance of digital solutions. The cost of interfacing PSPs' services to a separate and "external" digital euro app could substantially increase the **cost of distribution and account management**, as well as raise important and still unresolved **security and liability issues**. However, if the stand-alone Eurosysteem digital euro app is confirmed, it would be advisable to include it in a subsequent release, giving priority to other developments for the first release.

5. Points still to be clarified which are relevant for the design

We would like to conclude our feedback to the holistic review by listing some additional points that are relevant to the design of a digital euro and in our view still need to be clarified:

Pg. 4	<ul style="list-style-type: none"> Digital euro to be built as new form of central bank money but not as a new "payment solution" / "payment option" – distribution and access to be via existing or future new payment solutions built and operated by the private sector.
Pg 11	<ul style="list-style-type: none"> The distinction between a business user and a professional using a personal wallet/account for receiving payments needs clarification, in order to avoid circumvention of rules and profiting from a free use intended for individuals. The ECB must prioritize the analysis of the impact of financial stability and banks' balance sheets – this includes holding limits, transaction limits and remuneration models.
Pg. 16-19	<ul style="list-style-type: none"> Within the slides "Visualising digital euro end user experience" it is not clear what is meant by the P2P offline use case with card. We feel it is still very unclear how such a card setup would work exactly. Who would be the issuer? How would the offline card use case work and for what?

	<p>Is it only for smaller transactions (will there be limits)? Who can obtain such a card (e.g., residents vs non-residents)? Who will bear the costs related to card issuance and infrastructure? How to ensure such a card can be accepted at the PoS?</p> <ul style="list-style-type: none"> • The design of an offline functionality should be focused on partially replicating the cash-experience where only the funding/defunding of the wallet is visible to the intermediary, but not (up to a certain limit) the individual offline payment transactions. • Offline payments must be in line with AML/CFT obligations and fraud prevention limits already in place for cash and card payments.
Pg. 21	<ul style="list-style-type: none"> • Intermediaries must be given adequate time, technical specifications and resources to establish needed infrastructures and interfaces – a similar approach was defined for the PSD2 readiness of third-party service providers when linking their front-end solutions to the interface of the account holding banks. PSD2 required ASPSPs to provide their technical specifications of the API to TPPs six months prior the actual effective date of the access to ensure TPP can sufficiently prepare.
Pg. 22	<ul style="list-style-type: none"> • Default process should be onboarding via intermediary app: a prescriptive approach should be avoided and the onboarding must be subject to the intermediaries' onboarding procedures – the intermediary is the primary obliged entity under AML law and should be free to choose the appropriate and compliant onboarding procedure. • Onboarding / ECB app: redirect functionality to the intermediary required in the ECB App which the user chooses for onboarding. • Onboarding / ECB card: if a digital euro card will be introduced, redirection to the intermediary which the user chooses for onboarding must be implemented in the ECB website.
Pg. 23	<ul style="list-style-type: none"> • Portability: we reiterate our previous comments that an EU identifier for digital euro wallets is complex and implementing account portability has no precedent and will add a lot of complexity and cost.
Pg. 32	<ul style="list-style-type: none"> • Incident Management is missing – what happens if the transaction does not work due to technical faults – Use Case Customer uses the digital euro wallet provided by ECB vs. the intermediary app. • It is not clear in which cases an intermediary refuses onboarding.
Pg. 33	<ul style="list-style-type: none"> • Challenges with the obligation to convert between cash and digital euro 24/7/365: <ul style="list-style-type: none"> ◦ Enhancement of ATMs entails significant IT investments to combine functionalities of "cash out" and "cash in" with the real-time connectivity of the wallet on the smartphone and the physical digital euro card and other relevant functionalities. ◦ Furthermore, this new functionality must be incorporated in existing market-standards for interbank ATM management ◦ ATM deposit and withdrawals of cash are subject to dedicated limits for practical, security and AML-prevention reasons • Explanation is needed about "tiered remuneration being reconsidered".
Pg. 39	<ul style="list-style-type: none"> • The financial inclusion ambition of the digital euro must be analysed from the perspective of digital inclusion. Many aspects of digital exclusion are related to the citizens involved, rather than the specific digital service or infrastructure they would want to use.

The EBF looks forward to continuing engaging with the ECB on this crucial project and would welcome any additional discussion specifically on the content of this analysis.

For more information contact:

Alexandra Maniati

Senior Director, Innovation &
Cybersecurity, a.maniati@ebf.eu

Anni Mykkänen

Senior Policy Adviser, Payments &
Innovation, a.mykkanen@ebf.eu

About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure, and inclusive financial ecosystem, and to a flourishing society where financing is available to

19 June 2023

ERPB written procedure on digital financial inclusion EBF response

EBF response to ERPB Written Procedure on Digital financial inclusion

1. Completeness: which other aspects would need to be considered to make the digital euro as inclusive as possible?

- In the context of a digital euro, **financial inclusion cannot be decoupled from digital inclusion**. Currently, a relevant part of the citizens (normally less educated and/or less technologically savvy population) in the euro area lack basic digital skills that would be needed to make a payment with digital euros or any other digital means of payment. Unless measures to improve digital skills are implemented, the introduction of the digital euro may increase the risk for creating a new form of a digital divide.
- Currently we see **no value-add by the digital euro compared to private sector means of payment when it comes to financial inclusion**. Banks are already ensuring inclusiveness both in terms of access to services and adapting services to different population segments. In addition, banks are subject to legislation – which we would expect to also apply to digital euro – such as the Payments Account Directive and the Accessibility Act, that set legal obligations in terms of access and inclusion. Therefore, it must be duly assessed whether the proposed functionalities aimed at inclusion will have a real impact on the objectives pursued.
- We observe that the predominant reasons for not having access to a payment account are i) difficulties in the KYC process or ii) a citizen explicitly does not want to hold and manage an account at an intermediary.
- While the ECB has increased its focus on ensuring a high degree of “usability”, we would like to see more concrete plans to achieve this part of the inclusion objective. Existing market solutions already strive for high usability. In addition, different solutions have been presented by the ECB such as offline payments or card payments. Although the ECB considers that these solutions will support financial inclusion, we suggest performing a **detailed impact assessment in order to consider to what extent these solutions are imposing a cost overburden on intermediaries, compared to any relative increases that could be achieved in financial inclusion compared to the present situation**.
- **We are particularly concerned by the obligation on intermediaries to issue digital euro cards**, which are already widely available to users (and part of the basic payment account as defined in the PAD). Card issuance would be a major additional cost with little added value or innovation compared to the current situation. Most users have a smartphone which allows users to have digital wallets with digitalized cards for payments, which is similar to having a digital euro wallet. Adopting digital-only solutions would also help to create a more sustainable, more efficient and secure payment process. Finally, it should not be forgotten that those already using stablecoins will not find the use of a digital euro card appealing nor competitive. As the digital euro is meant to be an alternative for EU consumers, the use of the digital euro card will only increase the distance between CBDCs and privately issued stablecoins thus risking a low uptake of the digital euro. It seems that in order to be more inclusive on the one side of the spectrum, innovation is lost on the other hand.
- Across the EU and considering existing 5G/mobile network coverage, roaming policy, etc., and the high availability of systems with mirror support and disaster recovery models in intermediary banks, **the implementation of an offline model may not significantly increase financial inclusion in the Eurozone**. As also reiterated in the holistic review written procedure, there are still many questions

on the feasibility of the offline function. Furthermore, use cases related to offline payments are also covered by online functionalities while they have higher fraud risks for users. For this reason the limits set for offline payments (holding limits, transaction limit, maximum amount per period) should be lower than those for online payments. As previously mentioned in former contributions, if users experience issues due to the use of offline functionalities, these functionalities could become a reason to avoid using the digital euro, instead of a way of enhancing financial inclusion.

- As also stated in our previous contributions, **the stand-alone digital euro app will not improve financial inclusion** as unbanked population will need establish a relationship with an intermediary in any case. Therefore, the rationale for the stand-alone app should be reconsidered as we do not see any added value in it.
- On the advocacy strategy, the ECB mentions developing **targeted educational campaigns** among the actions to support financial inclusion. Intermediaries will play a key role bringing the digital euro closer to citizens and businesses and integrating it into their daily financial lives. We invite the ECB to work together with banks and other intermediaries and their respective associations on these educational campaigns. It is also very important involve consumer associations in educational information programs, to capture the point of view of the final recipient of the initiative. In the context of activities like this, it is important to create a network of private and institutional subjects who can contribute their respective skills and professionalism.
- In terms of communication, it is important that the digital euro is neither confronted with existing payment means, nor presented as a means of having "safe" money. We have seen examples –which should be entirely avoided - where the digital euro is presented as a way to make online payments “faster, easier and more secure” and as a way of accessing a risk-free payment means, implying that commercial bank money is risky (which is definitely not the case in the Euro area).
- Regarding the public approach, any measure taken (e.g. free provision of physical cards, in-person onboarding, etc.) should not be extended to all citizens, but only to vulnerable ones, and via voluntary provision of services by some distributing intermediaries. The definition of vulnerable users must be very clear to ensure that this dedicated service is for limited use only. We would like to stress that this point is crucial for the industry as we believe that only a targeted approach towards vulnerable users might contribute to the objective of financial inclusion. We also would like to point out that more clarity is needed in terms of responsibilities and allocation of costs with regard to the dedicated onboarding channel via public or private dedicated licensed entity per member state providing access to digital euro services and the necessary supports to those vulnerable to digital financial exclusion.

2. Synergies: which opportunities for synergies do you see for the digital euro inclusion measures and other initiatives addressing digital financial inclusion?

- On the one hand, one of the goals of the EU Commission in its “Digital Decade” is to increase the level of digital skills to 80% of the adult population. This could also make the use of the digital euro among the unbanked/under skilled people more effective.
- On the other hand, financial inclusion has been a topic which intermediaries have been and are addressing when releasing new digital means of payments. Leveraging on current payments infrastructure while promoting added value services will help intermediaries to bring their own ways to promote financial inclusion to the digital euro project.

3. Trade-offs: which challenges do you see in implementing the suggested measures, if any?

- The uptake of the digital euro could lead to an unintended, faster decrease in use and acceptance of cash in some situations, which could amplify the exclusion of certain groups of citizens.
- The implementation of some of them, such as the offline payments or the card usage, will also have big impacts on intermediaries that will face increased difficulties during its development and deployment. The development of these use cases for a minority adoption will require investment that exceeds the benefits and are sustainable for intermediaries. In terms of trade-offs, the design of the digital euro should not only respond to financial inclusion objectives, but to be attractive also to the more advanced and tech-savvy segments of the population and of businesses, thus the efforts to include features aimed at financial inclusion should not be to the detriment of designing the digital euro as an innovative raw material upon which intermediaries may develop advanced services meeting the needs of those user segments.

For more information contact:

Alexandra Maniati

Senior Director, Innovation &
Cybersecurity, a.maniati@ebf.eu

Anni Mykkänen

Senior Policy Adviser, Payments &
Innovation, a.mykkanen@ebf.eu

About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure, and inclusive financial ecosystem, and to a flourishing society where financing is available to

19 June 2023

ERPB written procedure on fraud prevention and detection EBF response

EBF response to ERPB Written Procedure on Fraud Prevention and Detection

1. General Remarks

- The digital euro, as a whole and in its potential different uses, should not be isolated from other payment instruments when we come to fraud prevention. This means not only its potential integration with the services already provided but also that its regulation should be consistent with the next version of the Payment Service Directive. Interaction with eIDAS and the related pilot works could also be explored.
- All innovative payment instruments have been characterized by an initial transitional phase in which there have been peaks of fraudulent phenomena. To limit potential critical issues, **it would be useful to be able to exploit all the experience accumulated by the financial operators in the fight against fraud.** The fraud patterns for the digital euro will not be at all different from those used against other payment services and systems and above all against the end customers themselves. Furthermore, it could be very useful to draw inspiration from other European experiences, especially with regard to those processes to combat fraud that have proved to be effective (forms of collaboration, information sharing, etc.). **However, the effectiveness of these processes can only materialize in the face of trust that is created within the community, which the regulator should help to establish.**
- One of the crucial issues is that relating to the trade-offs, which refers to the need to guarantee user privacy one hand, and actions against illegal activities. By no means, privacy should entail a sort of anonymization which could be used as a way for criminals of various kinds to execute payments without the possibility to be investigated. Nor should there be the possibility of taking funds of dubious origin out of the circuit (e.g., converting them in other types of funds) without adequate control instruments in place.

2. Responses to written procedure questions

1. *Does ERPB share the view from the functional analysis, with a role for a central fraud support service (CSS)?*

- The provision of some additional fraud-related information, especially in a new means of payment, could be beneficial for intermediaries. Nevertheless, it is important that the responsibility for authorizing payments will remain within the intermediaries.
- It is true that preventing fraud for the digital euro in isolation from other payment methods may reduce the attractiveness for fraudsters to use the digital euro – however, it is important to point out that it will re-direct the fraudulent activity to other payment means.
- **Therefore, to contribute to a safe payment environment in the EU, the digital euro fraud management should be embedded in EU-wide initiatives.**
- **In the meantime, and in the short-term, the preferred solution would be Option 1:**

- Intermediaries embed fraud management for the digital euro in their existing procedures and support these procedures by an external service provider;
- whilst intermediaries individually already make use of external service providers for post-fraud analysis, it would be beneficial to have a central support service (CSS), where CSS is involved indirectly only. The existence of a Central Support Service directly involved in pre- or post-fraud analysis (options 2 and 3) could have direct impacts on client experience that should be a responsibility of the intermediary.
- Option 1 is currently the prevailing situation in the EU payment industry (i.e., individual intermediaries perform their own fraud management, although their ability is enhanced in some cases via collaborative information sharing and initiatives at national/EU level) and that these intermediaries and service providers work on fraud data and payment patterns across multiple payment methods in a holistic manner.
- We also would like to stress that the proposed approach towards personal data ignores that it is not necessary to share personal data in fraud prevention to track patterns of fraud schemes.
- Additionally, the industry and the authorities partner to establish a connected approach across entities and Member States to improve fraud management and data sharing
- Key challenge for this EU-wide and industry-wide approach are the national data protection rules which prevent intermediaries from sharing relevant data – it requires a strategic public-private initiative to overcome existing regulatory, supervisory and technical barriers.
- Liability also plays an important role where the intermediaries are currently legally responsible for fraud handling – **if a third party, i.e., a Central Support Service (CSS), is involved, legal clarity must be provided in terms of roles & responsibilities.**
- In any case, we propose the following:
 - The CSS should be operated by a shared private sector entity and not by the ECB.
 - Costs aspects should be clarified. Who exactly will bear the costs, which are likely to be significant, of operating this new entity? While for now it seems the Eurosystem will not incur a fee on intermediaries for facilitating digital euro transactions, we are concerned that the introduction of costly support infrastructure/entities could change that in the future, as we have seen happen with other infrastructures in the past (e.g., TIPS).
 - Based on the proposed setup, we would also expect the CSS to have some overlap in responsibilities with the European Banking Authority and other authorities.
- AML/CFT/KYC is to be seen separate from fraud management and subject to different legal frameworks – a similar detailed analysis of AML procedures must be undertaken.

2. What is ERPB view on potential opportunity for PSPs to combine (specific) digital € fraud case information, with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP?

- Fraud management is a key factor to protect intermediaries' end users from potential fraud cases that would imply money losses. To achieve this, intermediaries have developed a wide variety of applications that check different parameters to avoid the execution of fraudulent operations.
- According to PSD2, PSPs shall ensure that the transaction monitoring mechanisms take into account, at least, each of the following risk-based factors:

- lists of compromised or stolen authentication elements;
 - the amount of each payment transaction;
 - known fraud scenarios in the provision of payment services;
 - signs of malware infection in any sessions of the authentication procedure;
 - in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.
- And regarding real time risk analysis they should be able to identify:
 - abnormal spending or behavioural pattern of the payer.
 - unusual information about the payer’s device/software access;
 - malware infection in any session of the authentication procedure;
 - known fraud scenario in the provision of payment services;
 - abnormal location of the payer;
 - high-risk location of the payee.
 - To achieve the level of protection of current digital payment methods, digital euro should, leveraging on current fraud processes applying to commercial euro allow intermediaries to capture at least the mentioned information in its fraud protection tools.
 - Furthermore, PSPs should initially adopt a low-risk appetite in operations related to the digital euro until it can be assessed whether the security measures adopted are sufficient to mitigate fraud to the greatest extent possible.

3. Would ERPB have any suggestions to complement the fraud prevention approach?

- In addition to what is defined in the analysis, there are services that we believe should be worked on from this centralized vision:
 1. Unique fraud and claims value chain, which allows global and specific metrics in real time.
 2. An awareness model that put the citizen in the center from the moment of inception of this initiative.
 3. Security & Fraud healthcheck models on the processes, not only related to onboarding of each entity, but also on the robustness of the processes of authentication, authorization, and elimination of transactional services related to the digital euro.

3. Detailed feedback on ERPB slides

Pg. 7	<ul style="list-style-type: none"> ● This slide should take in consideration two suggestions: <ol style="list-style-type: none"> 1. Key activities: awareness activities should be included. 2. Harmonization: looking at some national jurisdictions, there are specificities that should be reflected also in the context of digital euro. For example, at least in one country, there is a potential activity to be done in terms of the alignment with reporting obligations, therefore in case of DE introduction, intermediaries should add this activity on top to Fraud prevention integration.
-------	---

Pg. 9

- Market initiatives are putting in place similar solutions (e.g., FPAD for instant payments by EBA clearing). Potential synergies with those solutions should be evaluated. In any case, it should be confirmed if intermediaries should have free access to Central support services. Additional cost for intermediaries should be avoided.

For more information contact:

Alexandra Maniati

Senior Director, Innovation &
Cybersecurity, a.maniati@ebf.eu

Anni Mykkänen

Senior Policy Adviser, Payments &
Innovation, a.mykkanen@ebf.eu

About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure, and inclusive financial ecosystem, and to a flourishing society where financing is available to

EDPIA feedback to the ECB following the 8th ERPB technical session on the digital euro held on May 12, 2023

15 June 2023

ITEM 3 – Financial inclusion considerations of a digital euro

1. Completeness: which other aspects would need to be considered to make the digital euro as inclusive as possible?

We welcome the Eurosystem’s approach on the provision of a payment card as form factor. Indeed, such initiative shows how the digital euro promotes financial inclusion in an increasingly digital age. If limited to the offline use-case, the product (i.e., a smartcard) would be very close to previous similar solutions (e.g., GeldKarte, Moneo, Proton) which were received mixed success. Lessons may be learned from these experiences, for example the difficulty of knowing the card’s available balance, or the friction caused by the funding process, which may be even greater today as the ATM network is shrinking in some jurisdictions. Therefore, both funding and defunding methods could be considered as a way forward (i.e., via agents of the public or private dedicated licensed entity used as dedicated onboarding channel, at kiosks, or via smartphone implying a linked account).

In France, Moneo electronic purse previously proposed 3 distinct options:

- A co-branded option integrated in an existing scheme payment card.
- Moneo blue, which was linked to a bank account.
- Moneo green, which was not linked to a bank account.

The distinction whether the smartcard is linked to an account or not may be worth investigating, as the accessibility enabled by the card does not necessarily imply that the citizens benefitting from it are unbanked. Besides, it could allow the application of a tiered approach, with specific limits, features (e.g., support of online payment), and privacy levels. In this regard, the AMLD5¹ could provide a regulatory basis since it lists the conditions in which pre-paid products are exempted from customer due diligence (CDD) requirements, which may result in an increased privacy level.

2. Synergies: which opportunities for synergies do you see for the digital euro inclusion measures and other initiatives addressing digital financial inclusion?

The European Accessibility Act (EAA) is expected to enter in force in 2025 and covers a wide range of products and services, including banking services, e-commerce, smartphones, ticketing machines and ATMs, all of which will somehow be impacted by the digital euro roll-out.

Focusing specifically on ATMs, the cost and deployment time of any change is non negligible. We therefore consider it important to investigate the potential synergies between the implementation of EAA and the digital euro roll-out in such cases.

Trade-offs: which challenges do you see in implementing the suggested measures, if any?

- The question of the business model for intermediaries that are onboarding and providing services to eligible individuals still needs to be clarified.
- Offline technology brings additional complexity, not only at card level, but also at terminal level. An “online” payment card would be simpler to implement and roll-out.

¹ See AML Directive (AMLD5) here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843>

ITEM 4 - Fraud and risk management

1. Does ERBP share the view from the functional analysis, with a role for a central fraud support service (CSS)?

All market actors must be involved, with consistent levels of responsibility, to ensure best practices that efficiently tackle instances of fraud related to the digital euro.

Since the market has already established fraud prevention systems with demonstrable effects on user trust and transaction security, the development of a new dedicated fraud prevention system is not necessary.

Central support could be well enhanced through technological and functional standardization to support data sharing among the PSPs involved, guaranteeing the best efficiency and inclusion of all stakeholders.

In sum, PSPs, should be able operate in accordance with their own fraud risk assessment and management standards, and be the only entities with full visibility of consumer data. Such approach would ensure that the distribution of the digital euro maintains optimal privacy safeguards.

2. What is ERPB view on potential opportunity for PSPs to combine (specific) digital euro fraud case information, with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP?

PSPs can leverage their expertise, experience, software and databases built over the decades for understanding and preventing fraud-related dynamics. This would enable the euro digital payment system to reduce the effort (time and money) to reach the same level of effectiveness in fraud prevention and boost adoption.

3. Would ERPB have any suggestions to complement the fraud prevention and detection approach?

To increase the security and reliability of the European digital payment system, we suggest that the cumulative experience and assets developed globally by different digital payment systems be leveraged and interconnected, to prevent and detect fraud.

ITEM 5 - Digital euro holistic design review

1 - User experience for individuals and businesses

- **Access:**

- Option for non-resident euro area citizens and non-euro area businesses to pay and accept digital euros respectively is expected to support freedom of movement within the EU.

- **Off-line payments:**

- The underlying technology still needs to be industry-proof, and the design choices and related impacts (also on intermediaries) still need to be assessed.
- We would draw attention to the significant complexity that the acceptance network may be subject to with the simultaneous implementation of both online and offline use cases.

- **Use cases**

- We support the proposed staggered approach, which allows both the Eurosystem and the stakeholders involved to gain trust and experience before completing the deployment of all use cases
- Technology choice will play a key role. For POS payments, preference should be given to NFC technologies due to their better user experience, even if higher initial investments are expected.

- **Stand-alone digital euro app option**

- The role and responsibilities of the Eurosystem as the technical provider of the front-end application and interactions with PSPs' back-end systems are not yet considered adequately clear. It is important to understand in detail how they could complement the offerings of qualified intermediaries and support adoption.

2 - Making digital euro available: a public-private collaboration

- **Supporting services:**

- It is not clear yet who is the entity responsible for providing support services, outside the perimeter of services under the direct responsibility of the Eurosystem.
- In the dispute management process, it is important to define which entity will provide arbitration in case of unresolved disputes at the PSP level.

- **Compensation model:**

- A 4-party model is a supported choice to enable the remuneration of all parties involved and incentivize the distribution of the digital euro, while also triggering the necessary network effect.
- It is suggested to further clarify the services provided free of charge to PSPs by the Eurosystem, for the purposes of enabling the market to understand how to integrate and complement these different services.
- The (not-free) services provided to PSPs by the Eurosystem or other entities should be further detailed, as well as the rules for determining their costs.
- Free basic services to citizens should encourage inclusion of both users and intermediaries, without penalizing smaller PSPs that may lack the necessary resources.

3 - Privacy and data protection

- We suggest that PSPs have access to data for:
 - AML compliance and fraud prevention activities
 - Creation of value-added services to respond to evolving customer and competitive needs. This would be subject to user consent.
- The concept of "higher privacy for lower-value payments" needs to be carefully considered, since the value of a transaction does not necessarily define the level of risk.

4 - Financial and digital inclusion

Financial inclusion must remain an underlying component in the design of the digital euro payment system.

Among other initiatives, this is also achieved through the inclusion of citizens with special needs, according to eligible criteria to be defined, which enhances market best practices and intermediaries' experience.

It is considered important to also involve intermediaries in the definition of public interest services to be offered to the market under the same conditions and possible incentives. Such exercise would stimulate fair competition and avoid market distortions that cannot be foreseen to date.

EPIF input on the High-Level Product Description

16 June 2023

EPIF very much welcomes the opportunity to provide written input to the 8th ERPB Technical Session on the Digital Euro. The Digital Euro project is now in an important phase which requires a careful assessment of the high-level product description. EPIF members recognize the efforts made so far to ensure that the digital euro is a **convenient payment instrument** that accounts for **high levels of privacy** and **financial inclusion**.

Following the 8th Technical Session, participants were invited to provide feedback with a focus on six key areas: financial stability and holding/transaction limits; offline availability; compensation model; the roll-out approach; privacy and data protection; and financial inclusion. We would like to take this in turn, with a special focus on the **holding/transaction limits element**.

1. Financial Stability and holding/transaction limits

Regarding the subject of financial stability, EPIF recognises the ECB's necessity to maintain control over the amount of digital euros in circulation for the purpose of financial and monetary stability.

However, we wish to express our strong opposition to the proposed restriction of limiting each citizen to a single digital euro account. We believe this approach inherently gives an undue advantage to banks, potentially excluding other Payment Service Providers (PSPs) and inhibiting the financial freedom of citizens to manage their funds across different accounts as they see fit.

In light of these concerns, we would like to propose alternative methods which could provide a balance between the ECB's need for control and citizens' rights to financial flexibility:

- **Unlimited Transactional Wallets:** Instead of limiting the number of digital euro accounts, allow for an unlimited number of transactional wallets that cannot hold funds but can initiate transactions. In this scenario, funds would only flow into a wallet when a transaction is initiated through a "reverse waterfall" mechanism. This approach ensures transactional fluidity, whilst preventing excess accumulation of digital euros in multiple wallets, thus maintaining a degree of monetary control.
- **Single Wallet Multiple Controllers:** Permit only one wallet per citizen, but allow all PSPs, subject to user consent, to have control over the wallet and the ability to initiate transactions on its behalf. This approach would allow citizens to benefit from the services of multiple PSPs, without contributing to an increase in the quantity of digital euros in circulation, as the funds are contained within a single wallet.

We anticipate that these alternatives would help maintain the balance between necessary control and financial freedom. This approach also encourages competition, fosters innovation, and grants citizens the power to choose which PSPs they wish to interact with. We encourage the ECB to thoroughly consider these alternatives in their development of the Digital Euro.

2. Offline availability

Allowing for the usage of digital euros in offline “contexts” is an important feature to ensure both financial inclusion and that the digital euro remains as close to cash as possible as a payment instrument. Offline usage would also allow for a broader range of use cases and foster innovative solutions to be developed in this space. It is however crucial to assess the implications of the offline availability in terms of security of the funds, as well as compliance of PSPs operating the transactions in terms of AML/KYC requirements.

3. Compensation model and free provision of basic services

As previously noted, EPIF supports the four compensation principles highlighted by the ECB: free basic use by private individuals; network effects generating economic incentives for acquirers and merchants; comparable economic incentives for distributing PSPs; and the Eurosystem bearing its own costs. These principles must be translated into a carefully designed compensation model in order to ensure that the digital euro remains attractive for all parties involved.

EPIF particularly supports making the digital euro free of charge for end-users for basic usage and align with the ECB that core services should include all the three management areas: user, liquidity and transaction. Nevertheless, and in line with the ongoing work with the Digital Euro Rulebook Development Scheme, some points remain to be further discussed.

Whilst what constitutes a core service has been clarified, different use cases are being explored but with no clarification on whether *all* supervised intermediaries would have to provide *all* use cases and user journeys when entering the Scheme. Should this be the case, certain PSPs willing to join the Digital Euro Scheme might find themselves unable to do so as certain user journeys might be too far away from their product/services.

4. Roll-out approach

As previously noted, EPIF fully supports the phased-introduction of the digital euro into the EU payments space, both in terms of its geographical scope (i.e., initial introduction in the Euro Area) and use cases/user journeys. We foresee, for example, the possibility to first launch an online version of the digital euro, with a secondary introduction of offline functionalities given its particular technical challenges.

A phased-introduction would also allow the ECB and supervised intermediaries to fine-tune their delivery of the digital euro as challenges emerge in order to ensure that uptake increases in time.

5. Privacy and data protection

Privacy is a core element of the digital euro and must be upheld at all times. Not only has it been defined by the ECB has a primary objective when first presenting the digital euro, but it is also noted by citizens as a crucial element for adoption. EPIF therefore agrees with the ECB on its three key “privacy pillars”: a baseline scenario following current practice for electronic transactions; the possibility for higher privacy levels for low-value and close proximity; and limiting the Eurosystems’ visibility of *individual* payments data and holdings. The latter is particularly relevant to minimize the “Big Brother” concerns of European citizens and needs to be clearly articulated to end-users upon the actual launch of the digital euro.

Against this background, EPIF remains concerned with the disadvantage that other payment instruments might face vis-à-vis the digital euro should the applicable regulatory requirements differ. We understand that the applicable AML requirements for the digital euro will fall within co-legislators but it is crucial to not separate the discussions from the ongoing negotiations on the new AML/CTF Regulation. Under the new Regulation, exemptions for low value, low risk transactions have been removed e.g., e-money products. Should this exemption be allowed for the digital euro (which EPIF supports) it should also be granted to other payment instruments in the same

circumstances. This would respect the “same risk, same regulation” approach and prevent an unlevelled playing field between the digital euro and other payment instruments.

EPIF also sees merit in allowing for self-custody wallets, which could support the Eurosystem’s emphasis on privacy. We agree with the [ECB's summary report of lessons learned](#) from the prototyping exercise, which noted that “self-custody wallets . . . could potentially allow for more privacy” and “be more cash-like and give the end user full control over their digital euro.” The report went on to state that self-custody could also promote greater innovation and expand customer choice in the digital euro space. We strongly believe the Eurosystem should design the digital euro system to allow end users the choice of opting into a self-custody wallet service, including by designing system rules that work for self-custody wallets and a wallet provider licensing framework that offers a path for self-custody wallets to receive all required licenses and approvals. We do not expect all end users to opt into a self-custody wallet, but the digital euro system should at least allow them the opportunity to do so to the extent they value the privacy and control these services would provide. Please see our recommendations for “e-KYC credentials” and tiered KYC in our “Financial Inclusion” response.

6. Financial inclusion

EPIF fully aligns with the ECB to enhance (digital) financial inclusion through the digital euro and welcomes the clarifications about how this will be achieved. We agree with the four main areas proposed by the ECB to be leveraged upon to enhance financial inclusion: form factors, onboarding and portability, embedded functionalities and advocacy.

- **Form factors:** EPIF supports the “digital euro app” initiative, notably on its compatibility with the European Accessibility Act. Questions however remain concerning the responsibility to develop/operate the app; EPIF also in principle supports the provision of a physical digital euro payment card but again raises the question of the issuance responsibility as well as whether *all* supervised intermediaries will need to offer such solution regardless of their business model;
- **Onboarding and portability:** We agree with the basic principles of making onboarding available both in person and remotely, as well and guarantee easy switching.
 - We however reiterate again that allowing other PSPs providing other than account-based solutions to fully integrate the digital euro space is one of the most important elements to include financial inclusion, notably for the underbanked population.
- **Functionalities:** We agree with the proposed aim of maintaining a healthy equilibrium between deposits and cash. A reasonable digital euro holdings threshold can guard against the risk of excessive withdrawals from bank deposits, and is consistent with a payments-focused use case where balances should align to spending requirements. The mechanism by which this threshold is enforced, however, can create unintended consequences that significantly impact the ability to deliver end user benefits.
 - The two major approaches are 1) a post-transaction waterfall (which sweeps excess funds out of the end user’s wallet after they have arrived) and 2) a pre-transaction cap (which allows a recipient to decline a transaction that will carry the balance above the threshold). Each have pros and cons.
 - An automated waterfall-based approach has the advantage of convenience, as users can receive amounts in excess of the threshold and have them swept into a bank account without taking further action. This also prevents “above threshold” transactions from failing due to insufficient wallet capacity. The waterfall also has disadvantages, however. First, it creates a barrier to access as it requires every user to link to a traditional bank account (which not all individuals possess). Second, it creates a barrier to competition for providing wallet services, as it requires wallet service providers to offer a seamless transfer capability to a traditional bank account. This makes self-custody wallets and wallets offered by non-bank entities more difficult. Third, it creates incremental reconciliation efforts since users will need to confirm that the digital pounds that leave their wallets exactly match the bank deposit pounds that enter their bank accounts.
 - A pre-transaction cap has the advantage of allowing for increased access (as it removes a bank account dependency), increased competition (as it removes a barrier to entry for wallet service

providers), and increased choice (as it facilitates self-custody offerings). On the downside, a pre-transaction cap requires an additional step of pre-transaction communication with the receiving wallet (although this has the advantage of allowing a wallet from to refuse funds from an undesirable sender). It will also result some transactions failing to complete due to “insufficient capacity.” We would expect such “insufficient capacity” failures to be extremely rare with a sufficiently high threshold, however, and the payment system successfully copes with a far higher volume of “insufficient funds” failures today.

- While each method has advantages and disadvantages, is it important to note that a pre-transaction cap does not preclude wallet providers from offering waterfall functionality that is triggered by balances below the maximum threshold. A digital pound that supports pre-transaction cap functionality therefore will offer users the choice to adopt either a wallet with value-added waterfall services linked to a commercial bank account, or an independent wallet that relies upon the cap to decline excess value sends. We recommend that the Eurosystem incorporate support for pre-transaction caps into the final design.
- **Advocacy:** The introduction of the digital euro will have to be accompanied by a clear communication campaign to European citizens focusing on the explanation of the added-value of the digital euro, its easy use and privacy assurance. EPIF members also recognize the ongoing discussions which are to be further settled in the upcoming legislative proposal around legal tender. On this, EPIF continues to note that whilst giving legal tender to the digital euro might be an important element to promote uptake, mandating its acceptance from day one might put certain PSPs (e.g., those in more remote locations, smaller players) in a difficult position.

Moreover, EPIF would also like to note the recent MIT Report ([“CBDC: Expanding Financial Inclusion or Deepening the Divide?”](#)) which concludes that “If a new CBDC’s design merely replicates the existing intermediary ecosystem, it will likely replicate the same currency affordances that the existing ecosystem produces. Consequently, it may also replicate the same limits to inclusion and other harms that the existing ecosystem perpetuates.” EPIF members agree with this assessment. We welcome a design that is supportive of new ways of delivering intermediary services. In particular, we see a benefit to (1) unbundling KYC, AML and custody functions so that they can be performed by separate, specialized providers and (2) establishing a “tiered KYC” framework:

Unbundling: KYC can be unbundled from custody through the use of digitally signed “e-KYC credentials,” which would make it possible for transaction parties to rely upon KYC screenings performed by other institutions. In this model, a KYC provider (which can be a standalone entity) verifies an end user’s identity according to regulatory requirements. A user’s [eIDAS wallet](#) could itself be used for this purpose, which would leverage another important EU initiative. Upon successful verification, the KYC provider issues a cryptographically signed “e-KYC credential” that is permanently bound to the end user’s wallet. The end user then provides the credential as proof they have undergone a KYC process when completing a transaction with their wallet. Unbundling KYC from custody enhances financial inclusion by facilitating self-custody wallets (removing the barrier of a bank account to access digital euros) and by broadening the range of institutions that can verify an end users’ identity. As noted above, government-provided eIDAS wallets could themselves be used for this function.

Tiered KYC: Inclusion can be further enhanced by extending the concept of unbundled KYC to include “tiered due diligence checks” (or tiered KYC) as defined in the [ECB report on prototype summary and lessons learnt](#). Tiered KYC would apply differing levels of scrutiny to transactions according to risk. The end user would have the option to obtain one of multiple “tiers” of e-KYC credential, where higher tiers allow the end user to make larger transactions and hold more funds in return for greater identity verification and transaction monitoring. This allows for increased levels of scrutiny to be applied to higher risk transactions – both focusing resources where risks are highest, and lowering burden for end users with more limited transaction needs. For example, end users registering with just phone number, email or other minimal unique identifier could be enabled to still access digital euros for very low-value, cash-like purchases.



8th ERPB technical session on a digital euro

ESBG input

ESBG welcomes the opportunity to provide feedback to the ECB on the various topics discussed at the 8th ERPB technical session.

Digital financial inclusion

1. Completeness: which other aspects would need to be considered to make the digital euro as inclusive as possible?

We believe a distinction should be made between financial inclusion and digital inclusion. On financial inclusion, more than 13 million adults, or nearly 4% of the adult population in the EU are unbanked¹. However, splitting the data provided between countries in the euro area and those outside, it can be concluded that less than 5 million of these, representing 1,6% of the adult population, reside in the euro area whilst the remaining over 8 million of these, representing over 10% of the adult population, reside outside the euro area. For the latter category a digital euro would not be an immediate solution. Besides, it should be noted though that the Payment Accounts Directive (PAD)² gives people in the EU the right to a basic payment account regardless of a person's place of residence or financial situation. Whilst financial inclusion might not be the issue in the euro area, we do see the need of improving digital inclusion and it is unclear how the digital euro would enhance this. At this stage, we fail to understand how the digital euro can address this compared to other/private sector means of payments. People are preferring cash over digital options for various reasons (e.g. budgeting, privacy) which might not be addressed by the digital euro sufficiently. This could cause similar problems for broad acceptance by the public of the digital euro, like other digital solutions face too. Removing existing obstacles that hamper the acceptance by the public at large of digital solutions will need a more holistic approach and financial education, including digital skills, will be crucial.

In relation to approaching the public, both the objective and the methodology are unclear. We understand that the focus will be on unbanked clients, so those without an existing relationship with any intermediary, and that the issue can be solved via the ECB app and cards. The onboarding process for this is unclear, due to the fact that we don't know if the activation of the ECB app would redirect to an intermediary or not, and who will be obliged and responsible under KYC/AML/CFT regulation.

¹ ESBG Press Release, "Number of unbanked adult EU citizens more than halved in the last four years", 14 July 2022, available at <https://www.wsbi-esbg.org/number-of-unbanked-adult-eu-citizens-more-than-halved-in-the-last-four-years/>

² Directive 2014/92/EU of the European Parliament and of the Council



2. Synergies: which opportunities for synergies do you see for the digital euro inclusion measures and other initiatives addressing digital financial inclusion?

As seems today, the digital euro might lead to dyssynergies with other initiatives addressing digital financial inclusion rather than synergies. The digital euro will cause high implementation and running costs for intermediaries and does not provide such added value. Thus, intermediaries will face high-cost implications for putting in place services that already exist. This will have a negative impact on their capacity for innovation in general.

3. Trade-offs: which challenges do you see in implementing the suggested measures, if any?

We believe that the funding/defunding process via cash will be very challenging. The wide disparities in how access to cash is provided in the different European countries will make it challenging to provide the funding/defunding process of the digital euro via cash as a universal service in Europe and will cause high costs for intermediaries that distribute cash today.

More in general, we experienced that accessibility comes at costs and various investments (e.g. employees, tools).

Another challenge will be the issuance of a card for payments in digital euro, particularly regarding who will be the issuer of this card (ECB or PSP) and how the portability of this card from one intermediary to another can be managed.

Fraud prevention and detection

1. Do you share the view from the functional analysis, with a role for a central fraud support service (CSS)?

We believe that option 3 seems to be the best option in the long term. We understand that the CSS would be separated from the ECB (settlement provider). The role and the associated responsibilities of the different actors involved in this process should be clarified. For example, it should be clarified who is responsible of the reimbursement in case of fraud and if such aspects and financial consequences will be considered by the compensation model. Furthermore, methods concerning user behaviour could be considered useful and should be coherent to existing solutions to avoid multiple systems in place. A challenge in this regard would be aspects to privacy, e.g. to share data related to fraud with other banks. If the CSS is not going to be managed by the Eurosystem, it should have an appropriate governance.



In addition, liability for fraud cases in accordance with PSD2 should be reviewed thoroughly, the claiming process should be clear and proper fraud dispute mechanisms should exist.

2. What is your view on potential opportunity for PSPs to combine (specific) digital € fraud case information, with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP?

We believe that the principle proposed could improve the whole process. The services mentioned in CSS option 2 (post-fraud analysis, providing threat intelligence and situation awareness, etc) could be an opportunity for banks to combine with their own (case) information. It would be useful that the ECB considers already existing private solutions that deliver similar services, and design any fraud processes with an interconnection with them.

3. Would you have any suggestions to complement the fraud prevention approach?

We support the strategic fraud risk mitigation approach as mentioned in the slides (eight key activities in retail payment fraud management) and should be carried out in a diligent manner to improve the insight in the current environment.



ecb.degov230512_it
em4fraudpreventior

4. Would you have other reflections on other aspects in this regard?

N/A.

High Level Product Description

1. Do you have any feedback on a particular / all aspect(s) of the High Level Product Description?

Firstly, we would like to stress that the low level of details provided in the High Level Product Description do not allow for a thorough analysis. Nonetheless, we would like to reiterate our main considerations and particularly the clear need of a real added value the digital euro should have in comparison to existing solutions or solutions that are currently under development. The use cases currently being discussed for the digital euro are already covered by



existing payment solutions. This shows that the digital euro would cause on the one hand high costs for different parties, while not improving the situation for users and providers and no clear indications on how a fair compensation model could work.

The document stated that “legislators assigned the legal tender status to euro banknotes. The digital euro could also be given legal tender status”. This is something that must be looked at carefully. Bringing a new competitor in the form of a digital euro to the scene may distort the level playing, notably if the digital euro is a competitor that is being funded by public money and if it can benefit from mandatory acceptance stemming from its expected legal tender status. This may hamper private initiatives in their efforts to maintain or build European champions in payments going forward, as some private parties already pull back such investments. It should also take into consideration that perception, both by consumers as well as by merchants, could be that legal tender status equals free of charge.

Furthermore, the innovative aspects of the digital euro might be negligible while its introduction could hamper real innovation in domestic cases and demands. Moreover, there are several difficult aspects from a technical, privacy and financial stability view as well as the potential implications on the level playing field in payments.

Although the high level product description has a page (p.33) titled “...designed to avoid causing financial instability”, the following sentence on the same page implies that the conversion of deposits into cash should depend on people’s storage-risk appetite. The lack of very clear limits to this conversion preference from deposits to digital euro poses a significant risk to financial stability.

We consider individual limits to holdings in digital euro a critical tool to prevent an excessive build-up of liquidity in digital euro accounts or wallets, which could seriously impinge on the transmission of monetary policy through the credit channel as well as raise financial stability issues due to bank runs that could be facilitated by a digital euro. Individual limits could be set, for instance, based on the amount of cash payments that most consumers make during a certain period or the amount of cash that consumers typically carry in their wallets (e.g. €1.000 or less).

Therefore, it is very concerning and worrying that the ECB is considering the remuneration aspect (p.33). The digital euro should not have a remuneration. We do not see that remuneration would be an efficient tool to protect deposit outflows. Leaving remuneration rates at 0% would resemble the treatment of cash, which is what the digital euro should try to emulate. Also, remuneration could lead to asymmetries between cash and the digital euro with potential implications on different values among central bank money (cash vs. digital euro) and in times of financial stress, deposits would flow very quickly to the digital euro, independent of the remuneration. Furthermore, as tiering rates are a policy tool, another layer of uncertainty is added to deposit flows.

In addition, it is stated that imposing holding limits requires identification (p.22). Therefore, it would be one account/wallet per citizen. However, the latter has not been decided or investigated. From a financial stability point of



view, assurance should be given that the project will only progress when the identification problem has been solved. If the Eurosystem will settle without seeing holdings nor tracking payments to a single user, which entity/organization is going to be the entity with all the information on holdings? If it is not going to be the Eurosystem and it would not be based on national interoperability, that entity should have proper governance.

We must insist again, that the compensation model (p.30) is transaction-based only and that generally speaking such (indirect) transaction fees only represent a small part of the relevant revenues in payments. Given this, such (indirect) transaction-based compensation does not cover investments and fixed cost.

Financial institutions that are issuers of payment cards currently receive an interchange fee to compensate them for the value provided - including distribution of the product - to the merchant under a payment scheme. The proposed compensation model should offer similar levels of economic incentives as existing electronic payment alternatives. The scheme should be designed in order to be competitive with other providers, and expectations on merchant pricing should be competitive with that of other payment methods.

In addition, if the access to and the use of the digital euro is going to be free of charge for consumers, commercial banks must be compensated for the activities related to opening, maintenance, funding and defunding of the digital euro wallet/account, to name a few examples, taking into consideration that they currently charge commissions for such services too. Financial entities will lose account management fees (as there will be less clients with payments accounts), whilst no compensation will be due for the end-to-end management of the digital euro account or wallet. Therefore, also a remuneration to financial entities will be necessary to compensate for possible losses of account management fees.

The Eurosystem does not take into consideration the cost of financial intermediaries for the implementation of new systems (including but not limited to software and hardware cost, installation and configuration cost, infrastructure cost, professional services (PPSS) development cost, quality assurance cost) and human resources to be able to connect with the future scheme and the settlement process. Financial entities would require capital investment to interoperate and provide services on top of the core system as provided by the Eurosystem. The investment range can be expected to be very high, but much remains uncertain, as many aspects of the concrete model are still being analysed, and therefore it is difficult to make valid assumptions as each solution would require different cost estimations. Furthermore, a distinction should be made between implementation costs and maintenance costs, which likely will run in parallel for many years.



Furthermore, it should be highlighted that the industry, as a whole, should not bear the impact of the digital euro distribution. Accordingly, the impact should be neutral.

Banks should receive remuneration for the distribution and on-going management of the digital euro, or banks should have the prospect of a business model that allows a return on investments within a reasonable period of time, due to the fact that probably the distribution of the digital euro, as mentioned, will represent an additional cost (e.g. opening and maintenance of a digital wallet on an token/account- based system for millions of clients (customer service, balance enquiry, balance refund, etc.) technical connection to the ECB platform, tokenization platform, payment processing in a decentralized infrastructure, update of ATMs to enable cash withdrawal, training, to name a few).

The remuneration should be depending on the investments required for the distribution, and to the extent to which the Eurosystem supports the issuance and distribution of digital euro in the existing infrastructure and payment systems, and the ongoing developments and investments, such as instant payments. Therefore, to minimize the implementation and technical costs, any form of digital euro should take advantage of the existing payments infrastructure and instruments currently available.

More details should be provided in relation to the offline use case notably in relation to any connectivity requirement for funding and defunding - in particular in relation to the fraud controls that should be implemented. Financial entities will support full respect for privacy in low value payments carried out in an offline digital euro. The connection from the digital channel to the offline means (e.g. smart cards) would necessarily somehow identify the user, but this would resemble the current withdrawal of cash at ATMs or funding of pre-paid cards, and would still respect anonymity in the offline transactions that would follow it.

It would be important to describe how the digital euro app would work, including, for example, if it would be only be used by small intermediaries and if a euro area resident can use at the same time his or her banking app and the digital euro app.

Contact details:

European Savings and Retail Banking Group - aisbl

Rue Marie-Thérèse, 11 ■ B-1000 Brussels

Tel: +32 2 211 11 11 ■ Fax : +32 2 211 11 99

Payments@wsbi-esbg.org ■ www.wsbi-esbg.org

ERPB technical session on digital euro

Digital financial inclusion

Completeness: which other aspects would need to be considered to make the digital euro as inclusive as possible?

Children are often held back by parents from embracing money, both in access to their bank accounts and by only receiving small amounts of physical cash: Digital Euro presents an opportunity for children to learn about money in a new way – input from behavioural psychologists, teaching professionals and parents is needed to think positively about this, rather than seeing it as a barrier. Same for those without mental capacity as for child, a nominated adult connected to the person’s account could set conditions of use (eg maximum payments, maximum daily amounts). This approach could also help gambling addicts to pre-prevent themselves from spending in certain locations.

Similarly, the proposed wide range of ways to access Digital Euro can enhance ‘online’ engagement with money for those with lower digital or financial skills. Interaction of the benefits to these people, eg lower frauds, easier recoverability of funds etc. can help them to see that they need to try to adopt.

Information campaigns directed to different user groups and developed together with organisations for people will be essential, such as “education for children, elderly, etc”.

Synergies: which opportunities for synergies do you see for the digital euro inclusion measures and other initiatives addressing digital financial inclusion?

Crime reduction: many of the 4 categories of ‘at risk’ people are the most vulnerable in our society who are greater exposed to risks in protecting their money (both physical cash and accounts), digital Euro can give them both confidence and protection in using money, through the combination of the digital trail and the access of the crime prevention authorities to that, both as preventative and corrective measures.

In terms of synergies, it cannot be ruled out that as digital will be circulated more and more, physical cash will further lose market share. This will render the relative cost of cash acceptance more expensive.

Trade-offs: which challenges do you see in implementing the suggested measures, if any?

The more protections that are built in to facilitate financial inclusion, the more complex the system will need to be. There may be 'paid for' features for full Digital Euro that should be provided to vulnerable groups for free in order to enable them to safely use Digital Euro.

The more protection is implemented, there is a risk that anonymity is a trade-off.

ERPB technical session on digital euro

Fraud prevention and detection

Does ERPB share the view from the functional analysis, with a role for a central fraud support service (CSS)?

Generic comments and outstanding questions

- Impact on latency will need to be further analysed. It cannot be ruled out that there will be substantially more transactions made with digital euro than with any of the currently existing payment methods. If there is a concern on latency or outages then this would have huge impact on both end users and merchants. There should be detailed and communicated structure of technological failsafes that would safeguard the system from experiencing any latency issues or outages. Citizen confidence in Digital Euro will require option 3 real-time online support, in the same way as currently available for bank accounts, credit cards etc.
- Needs to be DEV+SEC+OPS from start
- What is the liability set-up in case of fraud. Is there a shift depending on fraud prevention measures?
- Is there a time-plan between soft launch and full launch?
- Formal role of CSS still unclear
 - What supervision would CSS be under?
 - Would/could CSS participate in any legal actions taken against fraud (police investigations, data gathering etc.)
 - Would it be a centralized body within ECB or would it be an external (3rd party) organization that would serve as CSS?

Option 2:

- Questions:
 - what kind of analysis would be conducted (scope, timeframes, repercussions, access to findings for merchants etc.)?
 - If fraud is detected by CSS, then what will be the role of CSS? Just monitoring or taking appropriate action?
 - what kind of support in fraud prevention would it play and at what level? Could merchants reach out to CSS for additional support in case of fraud incidents?
 - Could CSS take actions on end-users (fraudsters) to stop them from completing transactions before merchants notice fraud?
 - Would CSS take or participate in any liability if fraud happens at a merchant that has implemented the most sophisticated fraud prevention measures?

Option 3

- Should be available as close as possible to the go live
- Questions:
 - What's the impact on UX if real-time online support is implemented? Impact on latency and checkout time?
 - What's the scope of real-time support? What specific additional responsibilities would be covered and towards which institutions/organizations/3rd parties would they be?
 - On what grounds the decision on whether to have full visibility of data would be taken? Would the decision be communicated to the parties involved (end user, merchant)? How can full visibility be reconciled with Eurosystem's promise not to see any personal data?
 - When the need to see all data is not there anymore, would that access expire or would it need manual turning off? Would the parties involved be informed when access to full data was given and when it was taken and also what data was accessed (types and categories of data)?
 - Will CSS have the option to transfer the right to full visibility of data to other parties (banks, police, governments) and if so, would this be communicated to the parties that the data concerns? Could CSS share data with other parties also when there is no fraud involved?
 - Will it be possible for the end-user to perform a forced pseudonymization of his/her data in spite of CSS right to full visibility? Will CSS have the right to override that right?

What is ERPB view on potential opportunity for PSPs to combine (specific) digital € fraud case information, with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP?

n/a

Would ERPB have any suggestions to complement the fraud prevention approach?

- It would be beneficial to the merchant community if the CSS were able to share specific data with merchants with the objective to improve their internal fraud solutions. CSS should therefore not just be a black box but should be open to share best practices and relevant insights with key stakeholders (probably not only merchants but also intermediaries).

- Key activities (page 7) should include education of citizens of how Digital Euro can reduce fraud and make our society safer (fewer muggings and shop robberies) and reduce inflation/costs (cheaper cost of processing money will reduce cost of goods and services).
- Combination of Digital Euro digital trail and CCTV (retailer and local authority) can help crime fighting authorities to identify criminals committing 'in-person' crimes.
- Tax evasion can be reduced by Digital Euro take-up, which in turn can help Governments to keep tax rates lower for all citizens. Again, it comes back to public education and understanding of direct and indirect benefits to law-abiding citizens.

ERPB technical session on digital euro

High level product description – comments

Generic comments:

- Would be helpful for the document to include some context regarding wider societal benefits of Digital Euro (fraud/crime prevention, lower costs, increased inclusion...)
- Referencing the upcoming legal act would be beneficial to have wider context.
 - Legal tender discussion currently not picked up but ultimately of crucial importance, specifically for the merchant sector.
 - Adopting the digital euro, even when bearing legal tender status, should not result in an obligation for merchants to offer digital euro acceptance services across all available interfaces, channels and use cases

Additions and request for clarifications

- Page 8: Monetary anchor
 - Why is this important? What exactly is meant by this? This needs to be better explained so that non-experts will be able to understand.
 - What would happen if no central bank money was in circulation for retail payments? What would be the impact on the economy and on the ECB in terms of financial stability?
 - Why is monetary anchor needed if there is deposit insurance in place?
- Page 9
 - Top 2 advantages of cash cannot be applicable 1-1 to digital euro with current design features.
 - How will digital euro improve spending awareness compared to commercial bank solutions? What will be the added value? This has not been addressed in detail so far and is a crucial point for consumers.
 - Full anonymity as with cash is not foreseen. Should there not be low-risk digital euro products exempt from KYC obligations, granting anonymity? Can the offline digital euro be such instrument?
- Page 11
 - Zero daily holding limit → waterfall and reverse waterfall (for refunds) must not be subject to additional fees and will have to work optimally even for refunds at the start of the business day
- Page 13
 - Will users still have to perform KYC if they request to use offline digital euro instrument?
- Page 14:
 - Alias/proxy: as indicated, this technology will be launched depending on the user adoption of the pay-by-link feature. We estimate Alias/proxy payments to be highly relevant for online payments, so it would have to be developed as of the first release.
- Page 20

- It should be called out that (reverse) waterfall with a linked account can only be possible via a credit institute. PIs or EMIs cannot offer this feature.
- It should be mentioned that limits applicable to credit institutions' credit transfers will also be applicable to the reverse waterfall scenarios. Digital euro transactions may exceed a specific holding limit but may not surpass the limits put in place by the respective credit institution.
- Page 21
 - What will the standalone app mean for PSPs. Will they all have to provide APIs for the digital euro app to connect to the different intermediaries? Or will the ECB serve as intermediary where consumers opt for digital euro app? Or will ECB assign a single intermediary that will hold relationship with **all** consumers that use digital euro app instead of PSP app?
- Page 28
 - Governance structure of scheme is still unknown. How will different stakeholder be involved in the scheme?

In-depth comments

Page 30 – compensation model

Compensation Model The Eurosystem has proposed a “4-party model” for remuneration, which it describes as the “[b]est performing compensation model in the market.” This model was created for credit card networks, however, which utilize credit (short-term loans) and is built on top of bank payment rails (with the complex settlement processes that come with this). The technical architecture, economic incentives and delivery costs are so significantly different for a CBDC that the “4-party model” does not effectively map to digital euro payments and could inhibit the emergence of innovative new business models and services. In particular, we are concerned that the proposal for a fee that the “Merchant Bank pays...to compensate Consumer Bank for providing a free service [to the consumer]” (slide 30) will suppress rather than promote the development of a vibrant market for consumer wallets and service offerings. We point to UPI’s experience in India, which struggled to achieve adoption until interchange fees were dropped and new non-traditional fintech providers began providing consumer-facing apps as discussed below.

For a card transaction, the interchange fees of the 4-party model are shared between the issuing bank, card network and acquiring bank, and are primarily meant to compensate (1) the issuing bank for credit risk if the consumer fails to pay back the short-term loan, (2) the merchant bank for credit risk if the issuing bank fails to settle an authorized transaction, (3) the card network for maintaining its systems, and (4) all of the relevant intermediaries for fraud (based on which entity bears the fraud risk under the applicable local fraud liability rules). Neither these roles nor these costs exist in the same fashion for a CBDC: (1) The consumer’s wallet provider bears no credit risk because a transaction will fail if the consumer does not have a sufficient balance to fund it, meaning there is no credit involved at all. (2) Similarly, the merchant’s wallet provider bears no credit risk from the consumer’s wallet provider because the transaction settles

in real time rather than days later, and the merchant will never receive digital euros through the merchant's wallet unless and until the transaction settles. (3) None of the parties pays a fee to maintain the digital euro system (akin to the card network) because the Eurosystem would provide this free of charge under its proposed approach. With respect to (4), fraud will still exist, but this is a fraction of the interchange fee, and can be addressed in other ways.

At the same time that a CBDC eliminates most of the activities the 4-party model interchange fee model for card transactions was designed to cover, administering an interchange fee adds complexity and administrative costs (as well as the fee itself) to processing CBDC transactions. Among the efficiencies offered by a CBDC is that transactions settle instantly, passing directly from the sending wallet to the receiving wallet. Interchange fees will require the receiving wallet to execute subsequent transactions to transfer money out of the receiving wallet to a third wallet, belonging to the consumer's wallet provider. This not only creates additional transactions but introduces reconciliation requirements and related administrative burdens for all parties.

Given that most of the functions covered by the interchange fee today will be provided by the Eurosystem itself and free of charge (i.e., operating the central processing system), and that the cost to provide PSP services will be extremely low as a result, it is fair to question whether a global interchange fee is needed. For merchants and merchant acquirers (i.e. merchant wallet providers), the answer would clearly seem to be no. Merchants can negotiate prices for the services built on top of the Eurosystem's free public infrastructure with merchant wallet providers directly, choosing the offering that best meets their needs. Allowing price-service combinations to be defined dynamically by competitive forces (rather than set globally by an interchange fee) will ensure innovation in service offerings and efficiency in pricing levels.

For consumers and consumer wallet providers we believe the answer is also no. While we recognize the importance of providing consumers with free wallet options for transacting in digital euros, we do not believe that an interchange fee is required to subsidize their development. Providing consumers with free basic services to hold and transfer their digital euros will position companies to also offer a range of optional value-added services, for which they can charge. We believe that value added services, offered by intermediaries to customers and merchants (such as new services based on conditional payment logic) are the natural revenue streams for intermediaries in a digital euro system given that they will no longer hold credit or counterparty risk. The innovation this promotes will in turn drive increased adoption of digital euros for payment, creating a virtuous circle. Because the Eurosystem provides the core infrastructure to settle transactions as a public good, the cost of providing basic wallet services will be dramatically lower than today's payment instruments, making free basic services viable. This is an example of how the different design and corresponding cost efficiencies of a digital euro can spark innovation and allow for different business models.

It also matches the experience of UPI in India. While UPI is wildly successful today, processing $\frac{3}{4}$ of all digital payments in India, it launched with traditional interchange fees and failed to gain traction for the first several years. Between its Apr 2016 launch and Jan 2018, when traditional interchange fees were charged, it grew to only 152M monthly transactions. In Jan 2018 the government began subsidizing interchange fees, along with other promotion efforts, and monthly volumes increased from 152M to 1.3B

by Jan 2020. The government then dropped interchange fees entirely in Jan 2020, and monthly volume skyrocketed from 1.3B to 9.4B in May 2023. While dropping interchange fees to zero made UPI acceptance more attractive to merchants, the real impact was to make it cheaper and easier for non-bank actors to provide UPI apps (which the government encouraged). This led to a proliferation of new apps focused on delivering improved user interfaces and value-added services. Paytm, a major UPI provider, offers over a dozen services on its app that span from payments (utilities, rent) to financial services (loans, insurance, investments) to commerce (discount vouchers, ticket sales).

The proliferation of apps and use cases led to increased consumer demand, which led to increased acceptance by merchants and increased participation by banks (which are central to UPI, as it is a means of transferring bank deposits rather than a standalone digital currency). Today the National Payments Corporation of India, which operates UPI, lists 25 3rd party apps and 441 participating banks. Over 95% of transactions are processed by the 3rd party apps, all of which were launched following the elimination of the interchange fees which would have provided them with a direct revenue stream.

Adoption of new payment methods is typically driven by demand (primarily from consumer end users, but also from merchant end users) rather than supply (i.e., the number of intermediaries). Because there is so much unknown about what services will spark consumer demand, we believe a digital euro will be most likely to succeed if it promotes the greatest possible level of experimentation and innovation and drives strong demand from end users. This is facilitated by limiting mandated services to the minimum needed to ensure policy objectives (e.g. KYC, Strong Customer Authentication requirements), and maximizing the flexibility of private actors to negotiate their own offerings (e.g. funding/de-funding mechanisms) and economic models. We support the Eurosystem's decision to offer the digital euro without charge to the public, and expect that—as in India—a large number of entities will be eager to build services to facilitate the public's ability to access it. Mandatory interchange fees, associated with a legacy technology and business model, are not required to subsidize these services, will introduce unnecessary cost and operational complexity, and risk distorting the development of a newly emerging market for PSP services. We believe that consumers and the private sector actors seeking to serve them are well suited to define the economic models that work best, and we encourage the ECB to allow this to emerge organically.

Slide 35 – Privacy

We support the Eurosystem's emphasis on the importance of privacy and believe that allowing for self-custody wallets could further this objective. We agree with the [ECB's summary report of lessons learned](#) from the prototyping exercise, which noted that “self-custody wallets . . . could potentially allow for more privacy” and “be more cash-like and give the end user full control over their digital euro.” The report went on to state that self-custody could also promote greater innovation and expand customer choice in the digital euro space.

The core function of a wallet in the context of a digital currency is to store the private keys that evidence ownership and provide an interface for end users to use these keys to sign transactions that the end user instructs. A self-custody wallet stores the end user's private key locally within the end user's control (e.g. on a device in the user's possession), whereas a custodial wallet is one where a third party stores the keys on its own machine (e.g., a centralized cloud) and grants access to the end user through an online interface (e.g. protected via username/password). With a self-custody wallet, the end user signs transactions directly, using the private key on her device. With custodial wallets, the custodian signs transactions on the end user's behalf, and, as a result, both maintains its own control over the end user's data, including the private keys themselves and all transaction details using the private keys. This is why the ECB Summary report described self-custody wallets as "more closely mirroring an end user's control of euro banknotes in their physical wallet."

We strongly believe the Eurosystem should design the digital euro system to allow end users the choice of opting into a self-custody wallet service, including by designing system rules that work for self-custody wallets and a wallet provider licensing framework that offers a path for self-custody wallets to receive all required licenses and approvals. As stated in the [ECB Study on the payment attitudes of consumers in the euro area](#), cash was the most frequently used payment method at the point of sale (POS) and was used in 59% of transactions. It is possible to deliver the cash-like privacy afforded by self-custody wallets for low value transactions while simultaneously ensuring robust financial crime enforcement for higher value transactions.

We do not expect all end users to opt into a self-custody wallet, but the digital euro system should at least allow them the opportunity to do so to the extent they value the privacy and control these services would provide. Please see our recommendations for "e-KYC credentials" and tiered KYC in our "Financial Inclusion" response.

Slide 39 - Financial inclusion

A recent MIT Report ("[CBDC: Expanding Financial Inclusion or Deepening the Divide?](#)") concludes: "If a new CBDC's design merely replicates the existing intermediary ecosystem, it will likely replicate the same currency affordances that the existing ecosystem produces. Consequently, it may also replicate the same limits to inclusion and other harms that the existing ecosystem perpetuates."

We agree. We welcome a design that is supportive of new ways of delivering intermediary services. In particular, we see a benefit to (1) unbundling KYC, AML and custody functions so that they can be performed by separate, specialized providers and (2) establishing a "tiered KYC" framework:

Unbundling: KYC can be unbundled from custody through the use of digitally signed "e-KYC credentials," which would make it possible for transaction parties to rely upon KYC screenings performed by other institutions. In this model, a KYC provider (which can be a standalone entity) verifies an end user's identity according to regulatory requirements. A user's [eIDAS wallet](#) could itself be used for this

purpose, which would leverage another important EU initiative. Upon successful verification, the KYC provider issues a cryptographically signed “e-KYC credential” that is permanently bound to the end user’s wallet. The end user then provides the credential as proof they have undergone a KYC process when completing a transaction with their wallet. Unbundling KYC from custody enhances financial inclusion by facilitating self-custody wallets (removing the barrier of a bank account to access digital euros) and by broadening the range of institutions that can verify an end users’ identity. As noted above, government-provided eIDAS wallets could themselves be used for this function.

Tiered KYC: Inclusion can be further enhanced by extending the concept of unbundled KYC to include “tiered due diligence checks” (or tiered KYC) as defined in the [ECB report on prototype summary and lessons learnt](#). Tiered KYC would apply differing levels of scrutiny to transactions according to risk. The end user would have the option to obtain one of multiple “tiers” of e-KYC credential, where higher tiers allow the end user to make larger transactions and hold more funds in return for greater identity verification and transaction monitoring. This allows for increased levels of scrutiny to be applied to higher risk transactions – both focusing resources where risks are highest, and lowering burden for end users with more limited transaction needs. For example, end users registering with just phone number, email or other minimal unique identifier could be enabled to still access digital euros for very low-value, cash-like purchases.