Future of Payments

JOURNAL OF FINANCIAL SERVICES

PUBLISHED BY: **PROJECTIVE GROUP INSTITUTE**

01
2025

Projective
INSTITUTE

JOURNAL OF FINANCIAL SERVICES

Future of Payments

Contents

Dear reader,

Welcome to this, the inaugural edition of the Projective Group Institute's new Journal of Financial Services!

We're very excited to be launching our Journal at a time of immense challenge and change for the financial services industry, and we've drawn upon the deep subject matter expertise of the many renowned contributors to this edition of the Journal to bring you what we hope you'll find to be a highly stimulating series of articles.

We'll be publishing editions of the Journal on a regular basis, and each time we will be focusing on those topics our Advisory Board members, who are leading academics and executives, are telling us are of key strategic importance to them. And it's for that reason that we've chosen to focus this edition on the world of Payments.

Payments has gone from being an often-overlooked, quite slow-changing, typically back-office, function to becoming one of the most transformed - and transformative – functions in the financial services industry. And all of that has happened within the space of only a few years. Digitization, cloud native technology, financial crime and fraud, artificial intelligence, and many other recent developments, combined with ever-greater regulatory scrutiny and ever-increasing client expectations, have created the perfect storm for legacy Payments providers and have opened this area up to newer and more agile competitors.

We focus on the drivers of that transformation, the implications of those drivers for the various players in the Payments value-chain, and the key decision points firms will therefore soon face if they intend to remain leaders in this field.

I'm conscious that in creating the articles in this Journal, many individuals have spent many hours researching and writing, and I'm very grateful for their time and expertise!

I look forward to getting your feedback on our new Journal of Financial Services, and to speaking with you again soon.

Stefan Dierckx, Founder & CEO, Projective Group

Future of Payments

CBDCs and the digital euro: AML compliance moves closer to the end-user

Christian Sillaber,
Senior Researcher, Department of Private Law, University Bern

ABSTRACT

The emergence of CBDCs, and specifically the development of the digital euro, presents a complex landscape of challenges and opportunities within the AML/CFT framework. This article provides an analysis of the bifurcated AML/CFT approaches embedded within the digital euro's design, highlighting the tension between legacy compliance models and novel privacy considerations. The online variant of the digital euro showcases enhanced KYC, continuous transaction monitoring, and robust digital identity integration, with oversight centralized under the recently established AMLA. These mechanisms promise to exceed traditional banking surveillance and traceability, leveraging real-time data and audit trails to set new benchmarks for AML efficacy. Conversely, the digital euro's offline variant - intended to emulate the anonymity and immediacy of cash - depends primarily on transaction limits, presenting intricate calibration challenges. This paper argues that the digital euro's AML/CFT regime is poised to serve as a regulatory bellwether for broader E.U.-wide adaptation to rapid technological change. As public attitudes and stakeholder resistance evolve in response to policy trade-offs, it is essential that AML/CFT objectives are pursued without compromising innovation, fundamental rights, or equitable economic participation.

1. Introduction

The monetary landscape is undergoing a radical transformation with the advent of Central Bank Digital Currencies (CBDCs).[1] These government-issued digital currencies promise to reshape our digital economy by offering a secure, efficient, and real-time means of payment that integrates seamlessly into the digital fabric of everyday life.

Unlike cryptocurrencies, which are often associated with volatility and regulatory uncertainty, and private digital payment systems such as WERO or Venmo, which are backed by debt issuance, CBDCs are issued through sovereign authority. Amid increasing interest in CBDCs [Bidder et.al (2025)],[2] the digital euro emerges as a particularly noteworthy initiative, distinguished by its regional scope and its intended use for augmenting [E.C. (2023a)] retail cash transactions [Armelius et al. (2021)]. Pursuant to European Union regulation [E.C. (2023b)], the European Central Bank (ECB) is actively exploring the viability of a digital form of cash intended to coexist with physical euro banknotes and coins.

One of the distinctive characteristics of the digital euro - and, by extension, other central bank digital currencies, such as the recently announced e-rupee project [Reserve Bank of India (2025)] as well as the Bank of Japan's CBDC pilot program [Bank of Japan (2025)] - is its potential to enable direct peer-to-peer (P2P) payments, akin to transactions conducted with cash but within a digital framework [Sillaber et al. (2024)]. This feature is particularly interesting, as it responds to an increasing demand for privacy in financial transactions, an essential aspect of personal finance in an age with increasing concerns regarding data privacy.[3]

The aforementioned anonymity features, while appealing to users and beneficial from a resilience standpoint, raise significant concerns for regulatory authorities tasked with preventing illicit financial activities. Money laundering, terrorist financing, and other criminal enterprises could take advantage of features that provide anonymity, thereby posing substantial risks to the integrity of financial systems and eroding public confidence. Accordingly, achieving an appropriate balance between user privacy and effective anti-money laundering protections represents a critical challenge that must be addressed as policymakers and regulators develop legal frameworks for CBDCs [Lagarde et al. (2022)].

This paper explores the intricate relationship among CBDCs, privacy, and anti-money-laundering/combating the financing of terrorism (AML/CFT) measures. Using the emerging digital euro as an example, it discusses how anti-money laundering compliance can be seamlessly integrated into the technical design of central bank digital currencies without compromising their potential to facilitate private P2P financial transactions. The paper highlights that a promising solution lies in technologically advanced methods that embed AML/CFT measures directly within the mechanisms governing access to, and use of, the digital euro.

2. The design of CBDCs: The digital euro

The European legislative initiative to introduce a digital euro is regarded as a pivotal step in adapting the euro monetary system to the digital age [Panette (2023), Miha (2025)]. This project, as first formalized in the European Commission's draft regulation [E.C. (2023a)], seeks to establish a CBDC as a digital version of the euro, with the stated objective of designating it as legal tender throughout the Eurozone. The central policy objective is to ensure that public money remains accessible, trusted, and competitive within the rapidly evolving landscape of private digital currencies [Auer et al. (2023)], emerging stablecoins [Aldasoro et al. (2025)], and technology-driven alternative means of online payment [ECB (2024)].

According to Article 7(1) of the draft regulation, the digital euro is equal to non-digital euros and physical cash, thus anchoring its role as a complementary - and expressively not substitutive - instru-

1. As of July 31, 2025, according to CBDCTracker.org reports, four central banks have officially launched a CBDC, while approximately 30 other national banks are either developing proof-of-concept projects or are in the pilot phase.
2. Wholesale CBDCs are gaining significant attention for their potential to enable efficient, high-value settlements, especially in light of the growing adoption of tokenized deposits and atomic settlement applications. On the other hand, retail CBDCs face obstacles, as evidenced by countries like Sweden, Canada, and the U.K., which have scaled back their initiatives due to limited public interest and challenges in adoption. It should be noted that while both types of CBDCs are under development, this paper focuses specifically on retail CBDCs.
3. The European Commission identifies privacy as the most significant risk noted in the Eurosystem report on the public consultation regarding a digital euro; ECB (2021).

ment within the existing monetary system [Lemke (2024)]. The ex-lege legal tender status further obligates acceptance of the digital euro for the settlement of debts and transactions across member states' territories, meaning it must be accepted under the same conditions and with the same finality as cash or non-digital central bank money.[4]

The legislative framework envisions the digital euro as comprising two distinct variants: the **online** and **offline** forms (Recitals 17 and 34 of the draft digital euro regulation). This approach acknowledges the varied payment environments and use-cases present in contemporary digital economies.

The online variant is designed for transactions executed through internet-connected devices, contingent upon stable network connections and supporting IT infrastructure (Recital 4 of the draft digital euro regulation). The design of this system is intended to align with workflows and conveniences established in prevailing commercial banking and private payment platforms. In contrast, **the offline variant** features a limited set of functions focused on facilitating direct value transfers between individuals in physical proximity, without involving intermediating infrastructure or requiring continuous Internet connectivity (Recitals 58, 69 of the draft digital euro regulation). Its purpose is to provide a "cash-like" experience within the digital landscape, thereby ensuring resilience during instances of network unavailability, safeguarding privacy for low-value transactions, and promoting inclusivity for individuals who have restricted access to the broader online environment (Recitals 5, 6, 16 of the draft digital euro regulation).

The essential role of access to both online and offline digital euro ecosystems is reserved for supervised PSPs, which serve as the primary entry and exit points for end-users (PSPs as defined in Article 4, point (11) of Directive 2015/2366). Entry into either ecosystem, whether through the establishment of an online account or by provisioning an offline device, requires a contractual relationship between the user and a PSP.[5] By design, this relationship is contingent upon the completion of "know your customer" (KYC) procedures [ECB (2025)]. Whether the user chooses an online account - managed and authenticated by their PSP of choice - or opts for the additional provisioning of an offline-capable digital euro device (incorporating secure hardware features), the foundational logic remains consistent: all individuals must successfully undergo rigorous identity verification procedures before being granted access.

The stated goal of requiring strong (digital) identities has direct consequences for the inclusion of underbanked or unbanked individuals, a concern expressly acknowledged in the legislative proposal (Recital 5 of the draft digital euro regulation). While special onboarding mechanisms may be introduced to facilitate access for these groups, the minimum threshold, KYC-compliant onboarding, remains (Recital 29 of the draft digital euro regulation). Any participation in the digital euro ecosystem (whether online or offline) is, therefore, by legislative design, irreversibly linked to the user's verified real-world identity.

Direct access to the online digital euro without intermediaries, analogous to self-custodied wallets in decentralized cryptocurrencies, is not foreseen [ECB (2025)].[6] The offline variant, notwithstanding its infrastructure-light transactional mode, requires that user devices undergo enrollment and, potentially, periodic synchronization via PSP infrastructure,[7] if only to ensure compliance with global account limits and to potentially facilitate risk-based AML/CFT controls whenever the device is connected (Recitals 25, 32 and 33 of the draft digital euro regulation). For funding and defunding operations, transfers between both systems will be permissible (Article 23(2) of the draft digital euro regulation). To bridge the operational gap between these systems, the legislative draft also outlines hybrid transaction models, wherein a single transaction process may be divided between online and offline components (Recital 40 of the draft digital euro regulation on "waterfall" and "reverse waterfall" functionalities).

While much of the technological implementation details of these systems remain to be defined, the two variants are not only technologically dis-

4. Article 9 of the draft digital euro regulation stipulates several important exceptions to the obligation to accept the digital euro, most notably for small businesses, for good faith reasons, for non-business transactions, and pursuant to party agreement.
5. Compare Article 13(6) of the draft digital euro regulation: "[..] users shall only enter into a contractual relationship with [PSPs]. Digital euro users shall not have any contractual relationship with the [ECB] or the national central banks."
6. While not a decentralized means of access, integration into the EDI wallet could render access more transparent and ubiquitous (cf. Article 25 of the draft digital euro regulation).
7. Although the progress report lacks specificity, it suggests a significant capacity for programmability and updateability functionality of the offline devices [ECB (2025)].

tinct but also differ fundamentally in their environmental assumptions and AML/CFT expectations. The online version assumes an omnipresent, robust network environment and can, therefore, support real-time compliance monitoring and transaction screening. In contrast, the offline digital euro's independence from network infrastructure presents unique technical challenges.

The digital euro proposal introduces an "overlay network", a regulatory compliance layer connecting individual PSPs (Recital 25 of the draft digital euro regulation: "[..] by establishing alone or jointly with national central banks a single access point of digital euro user identifiers and the related digital euro holding limits"). This network, which may be directly accessible to regulatory and oversight bodies, is tasked with ensuring that system-wide account and transaction limits are enforced, regardless of the specific infrastructure of individual PSPs or the delineation between online and offline access (Recitals 31 and 34 of the draft digital euro regulation). Although much remains unknown at present, the overlay network could prove instrumental in monitoring aggregated transaction behavior, enforcing global caps - for example, the maximum amount an individual may hold across all accounts - and detecting anomalous usage patterns indicative of illicit finance, though the specific limits and conditions have yet to be determined. While technical standards for this overlay network are still under development, the architectural principle remains clear: compliance is embedded not only at the user onboarding and access layers, but also at the systemic level.

In summary, the approach to the digital euro seeks to reconcile two primary objectives: ensuring a high degree of transactional freedom, privacy, and resilience for end users - particularly in offline contexts - while simultaneously embedding AML/CFT requirements as non-negotiable prerequisites for both entry into, and use of, the digital euro ecosystem.

3. AML/CFT risks

This subsection presents a systematic analysis of the AML/CFT risks and challenges inherent in CBDCs, using both the online and offline versions of the digital euro as examples. The discussion is organized across several key dimensions: (i) KYC procedures and onboarding, (ii) transaction monitoring, (iii) beneficiary and counterparty identification, (iv) record-keeping and auditability, as well as (v) jurisdictional and other legal considerations.

3.1 KYC and onboarding

As outlined, the online digital euro serves as the entry point to the broader digital euro ecosystem. Its issuance and distribution are conducted primarily through existing intermediaries, such as banks and regulated financial institutions, all of which are already subject to established AML/CFT frameworks (Article 4, point (11) of Directive 2015/2366). As a result, the additional KYC risk introduced by the online digital euro into the financial system is largely confined to those existing intermediaries. This model has also been applied by the Bank of England in its Digital Pound project [BoE (2025a)]. These entities maintain primary responsibility for customer onboarding and identity verification, utilizing existing AML/CFT infrastructures and prudential protocols (Recital 79 draft digital euro regulation).

However, significant uncertainty exists regarding access pathways for unbanked and underbanked populations. At present, the mechanisms through which these groups will access the digital euro remain undefined.[8] The absence of clear onboarding processes for this demographic risks the emergence of a parallel, less regulated channel for digital euro acquisition, which could be exploited for illicit financial activity.

In conclusion, although the online digital euro's KYC risks are largely comparable to those present in traditional commercial banking systems, the unresolved onboarding processes for underbanked and unbanked individuals present a material - but not insurmountable - anti-money laundering challenge. Whether process differences and risks will emerge between populations utilizing strong dig-

8. The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) and the European Banking Authority (EBA) are tasked to "...issue guidelines specifying the interaction between AML/CFT requirements and the provision of basic digital euro payment services with a particular focus on financial inclusion of vulnerable groups including asylum seekers or beneficiaries of international protection, individuals with no fixed address or third country nationals who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons." (Article 14(5) draft digital euro regulation).

ital identities and those relying on traditional identification methods remains to be seen.

3.2 Transaction monitoring

Turning to transaction monitoring, the online digital euro is expected to replicate traditional banking payment flows. Under the envisioned architecture, transactions pass through regulated intermediaries with full visibility into each transaction. Thus, the risk profile closely mirrors that of existing systems [Sillaber et al. (2024)]. Efforts related to AML/CFT, including transaction screening, pattern recognition, and suspicious activity reporting, will largely remain functionally analogous to current practices. Transactions conducted through the online digital euro will provide compliance teams with granular data points, facilitating the application of analytical tools and thresholds consistent with prevailing banking standards (Recital 65 draft digital euro regulation). Because both the sender and the receiver will be robustly identified, the quality of data available for analysis is expected to surpass that of current systems. The Bank of England also adopts a similar strategy, emphasizing its objectives for interoperability [BoE (2025a)].

In contrast, the offline digital euro presents significant monitoring challenges. Designed for P2P transactions without the involvement of intermediaries, offline digital euro transfers do not generate centralized - or for that matter any - records or allow for validation through regulated entities (Recital 71 draft digital euro regulation). As a result, neither real-time nor retrospective transaction surveillance is possible due to the cryptographic and technological structure powering offline transfers, such as secure devices or wallets capable of independent communication. The detection of illicit transactions is comparable to the risks associated with the use of cash, in which anonymity and the lack of a structured audit trail undermine the effectiveness of law enforcement and compliance efforts.

3.3 Beneficiary and counterparty identification

With respect to beneficiary and counterparty identification, the digital euro benefits from a foundational design principle: account holders must be linked to a robust, verifiable digital identity (Recital 58 draft digital euro regulation). The optional use of the European digital identity (EUDI) wallet has the potential to increase the quality of record-keeping and traceability beyond current standards [E.U. (2024)]. Consequently, the risk of misidentifying counterparties or obscuring payment recipients is reduced, if not eliminated.

By contrast, offline digital euro transactions are conducted on a P2P basis.[9] In the absence of intermediary validation or recipient identification, counterparty risk is analogous to that encountered with conventional currency. Tracing recipients or confirming their legitimacy remains virtually impossible using standard compliance tools. Consequently, beneficiary risks in offline scenarios are comparable to those associated with cash.

3.4 Record keeping and auditability

From a record-keeping and auditability perspective, the contrast between the two variants is pronounced. The online digital euro, linked to digital identities and intermediated transaction flows, inherently generates comprehensive records of transaction histories.[10] This connection greatly facilitates audit trails, compliance verification, and forensic investigation, as digital footprints are readily available for regulatory examination. The design contemplates the capacity to maintain immutable, tamper-evident ledgers, thereby supporting enhanced auditability and accountability [FIU (2023)].

By contrast, the offline digital euro does not incorporate any record-keeping or data retention features within P2P transfers (Recitals 34 and 35 of the draft digital euro regulation). Transactions in this environment are, in effect, private and transient exchanges between end-users. The absence of record retention significantly impairs retrospective auditability and complicates the enforcement of AML/CFT requirements. Without centralized or decentralized logs, compliance becomes reliant on downstream detection, often occurring only when transactions are converted back into the regulated financial system, thereby introducing potentially significant delays and enforcement blind spots.

9. This may not apply to transactions exceeding certain thresholds, where the infrastructure automatically divides the transaction into online and offline components ("waterfall").
10. See Annexes II through V of the draft digital euro regulation regarding the data that the ECB, PSPs, and Support Service Providers may collect.

3.5 Jurisdictional and other legal considerations

While broader jurisdictional and legal issues extend beyond the scope of this analysis, a significant benefit of the digital euro in the context of AML/CFT laundering is instantaneous settlement (Recital 64 of the draft digital euro regulation). The design enables immediate finality of transactions, in stark contrast to otherwise multi-day settlement cycles. This immediacy significantly reduces counterparty settlement risk, thereby indirectly supporting AML/CFT regimes by enhancing transactional certainty, minimizing avenues for fraud, and constraining opportunities for layering or complex structuring schemes intended to obscure illicit provenance [FIU (2023)].

Additionally, the digital euro's cross-border interoperability and the integration in divergent legal and technical systems remain unresolved challenges [FIU (2023)]. Potential fragmentation could hinder AML/CFT efforts by enabling regulatory arbitrage and creating inconsistencies in the application of identification and monitoring standards. If left unaddressed, such jurisdictional heterogeneity risks undermining the coherence and effectiveness of AML/CFT controls that are critical to digital currency systems.

3.6 Summary

The AML/CFT risks inherent in the digital euro differ substantially between its online and offline forms. The online version allows for the adoption of existing KYC and transaction monitoring frameworks, bolstered by enhanced digital identity integration and comprehensive recordkeeping, thereby providing a more robust foundation compared to legacy bearer and banking instruments. In contrast, the offline digital euro raises classic challenges associated with cash-like anonymity and transactional opacity, further complicated by the absence of oversight and recordkeeping. Systemic considerations help mitigate these risks, as settlement finality and technological robustness contribute positively to AML/CFT controls. However, the unresolved question of access for unbanked and underbanked populations presents a potential vulnerability that requires further examination to prevent the emergence of blind spots in AML/CFT compliance.

4. Regulatory balancing and AML/CFT measures

The effective implementation of AML/CFT is a stated design goal of the digital euro (Recital 78 of the draft digital euro regulation). The draft regulation attempts to balance robust AML/CFT controls with the preservation of user privacy.[11] It delegates to the EBA and the AMLA the critical task of formulating guidelines to define the relationship between AML/CFT obligations and inclusive access to basic digital euro payment services (Article 14(5) draft digital euro regulation). This governance arrangement seeks to harmonize regulatory oversight across Member States while ensuring access, particularly for unbanked and underbanked populations (Article 14(5) draft digital euro regulation).

The draft regulation's approach is explicitly risk-based, reflecting the organizing principles of the E.U.'s AML framework. Notably, it expressly precludes full anonymity - an alignment with the Commission's comprehensive AML/CFT package [E.U. (2024b)]. Simultaneously, it innovates by suggesting heightened privacy for offline, cash-like digital euro payments, while subjecting online transactions to the same data protection, privacy, and AML/CFT requirements that govern private digital instruments.

The analysis of the preceding section has highlighted several technical and operational challenges that may complicate AML/CFT compliance, notably P2P transfers and onboarding processes designed to accommodate users outside traditional banking channels. The discussion that follows will address the issues along the already introduced axes of (i) KYC and onboarding, (ii) transaction monitoring, (iii) beneficiary and counterparty identification, (iv) recordkeeping and auditability, and (v) jurisdictional and ancillary legal considerations.

4.1 KYC and onboarding

AMLA, established in July 2025 as a central supervisory actor (Recital 86 AMLA regulation), is charged with developing guidance on KYC requirements and rules for onboarding to the digital euro. Notwithstanding the absence of finalized guidance on

11. See "Stakeholder consultations" of the draft digital euro regulation: "Privacy was considered the most important feature of a digital euro by both citizens and professionals participating in the consultation" [Brunnermeier and Landau (2022)].

onboarding (see, for example, the open regulatory questions reflected in Article 14 of the digital euro proposal), emerging publications and the draft digital euro regulation advocate for the application of risk-based measures to KYC and onboarding procedures.

The digital euro ecosystem is planned with the rollout of the European Digital Identity and its wallet (EUDI Wallet) in mind [E.C. (2021)]. Under the proposed regulatory regime, PSPs are required to accept the EUDI Wallet for customer identity verification, encompassing both new and existing customers (Recital 58 draft digital euro regulation). The wallet will facilitate access to digital identity attestations and enable remote customer due diligence (Article 25(1) draft digital euro regulation). Notably, this identity solution is anticipated not only for remote onboarding but also to extend to all payment devices in retail contexts (Article 25(2) draft digital euro regulation).

Crucially, the draft regulation highlights an explicit distinction between privacy interests and supervisory obligations by providing that users' identities remain with the PSPs (Article 34 draft digital euro regulation). Both the ECB and PSPs are required to implement "state-of-the-art technical and organizational safeguards" to shield user identities from access by the ECB at the front-end level, thereby seeking to reconcile privacy-by-design imperatives with AML/CFT objectives (Article 32 draft digital euro regulation).

As a logical consequence, in instances where an online euro wallet is linked to payment accounts at other PSPs, those providers assume the status of joint data controllers, thereby bearing heightened obligations under the General Data Protection Regulation (Article 26 GDPR "Joint controllers").

For the envisaged offline variant of the digital euro, the efficacy of AML/CFT laundering controls is primarily derivative of the online onboarding process. Offline wallets are based on digital identity attestations previously validated in an online environment, implying a necessary, albeit indirect, dependency on robust online onboarding and verification practices (Recital 69 of the draft digital euro regulation). The integration of risk-based KYC procedures thus extends de-facto into the offline sphere, although the technical implementation of offline KYC surveillance is limited to core safeguards relying on trusted hardware.

4.2 Transaction monitoring

Transaction monitoring regimes for CBDCs frequently aim to strike a careful balance between the objectives of preventing illicit finance and respecting data minimization and privacy principles [ECB (2025)]. Transaction monitoring, continuous assessment for suspicious activities, predicate offenses, and sanctions screening are core expectations, drawing directly from established best practices within the traditional payments ecosystem.

The digital euro's online variant will be, by design and necessity, congruent with existing payment rails regarding transaction monitoring surveillance. Full transaction monitoring, leveraging artificial intelligence/machine learning (AI/ML) based systems and network analytics, will be facilitated by persistent ledger connectivity, enabling advanced pattern recognition, real-time flagging of suspicious activities, and extensive checking against EU/OFAC sanctions [FIU (2023)]. Article 32 of the proposal envisions a centralized (potentially federated) transaction monitoring mechanism (Article 32 draft digital euro regulation: "General fraud detection and prevention mechanism"), operated either by the ECB or designated support service providers, to assess real-time fraud risks and provide post-settlement detection support to PSPs. Importantly, while the detection mechanisms are expected to leverage identifiers such as unique account numbers and session metadata (e.g., IP address ranges), Article 32(6) imposes explicit privacy requirements, precluding direct user identification by support service providers: "The providers of support services will be subject to contractual safeguards that prevent the linking or onward transmission of any personal data that can only be processed for specific purposes, and when strictly necessary" [ECB (2025)]. Furthermore, for the enforcement of holding limits and exceptions in emergencies, Recital 77 foresees the establishment of a single access point for user identifiers and holding limits. The regulation frequently emphasizes that this must respect the GDPR's mandates for data minimization and security by design, possibly incorporating decentralized storage to mitigate data breach risks. Upon request from a competent authority (FIU), PSPs must furnish collected data to support AML/CFT investigations (Article 37).

Distinctly, the digital euro's offline mode intentionally mirrors certain privacy attributes of cash (Recital 71 digital euro proposal). The disconnected operation of the offline wallet precludes imme-

diate transaction-level monitoring; data retention is expressly forbidden for offline transaction flows (Article 37(2)), except for PSPs' record-keeping related to funding and defunding events, in accordance with Article 40 of Directive (EU) 2015/849. To mitigate resulting risks, the regulation authorizes the European Commission to impose transaction and holding limits on offline balances (Article 37(5)), a risk-based tradeoff justified by the limited exposure at stake [Brunnermeier and Landau (2022)]. Furthermore, periodic synchronization, for updating balances and monitoring compliance with limits, may supplement supervisory mechanisms without undermining privacy.

4.3 Beneficiary and counterparty identification

Beneficiary and counterparty identification represent foundational concerns in AML/CFT compliance frameworks. Effective identification is central to robust transaction monitoring, profiling, and the prevention of illicit financial flows.

The digital online euro aligns with the trend of traditionally account-based systems[12] by requiring strong, verifiable (digital) identity linkage for all account holders. In particular, the standardized user identifier and user alias association improves the quality and granularity of record-keeping, offering regulators and intermediaries deterministic identification of both counterparties and beneficiaries in electronic transactions. As a result, the risks of misattributing transaction parties, creating false identities, and obscuring payments are expected to be significantly reduced; though it remains to be seen how the creation of aliases will be harmonized and practically implemented in practice. PSPs can leverage these identity guarantees to develop high-integrity profiles for both payers and payees.

Conversely, digital offline euro transactions, which occur through P2P exchanges in close physical proximity (e.g., near field communication (NFC) based device-to-device transactions), recreate the practical anonymity of cash. During offline transfers, no personal or transactional data are exchanged or monitored, and counterparty identification is neither feasible nor required (Recital 75 draft digital euro regulation). PSPs handle personal data only when digital euros are moved between online digital euro payment accounts and local storage devices, similar to personal data processing associated with ATM cash withdrawals.

Thus, while digital online euros advance AML/CFT objectives through robust identity binding, offline functionalities require an adaptation of existing risk-based AML frameworks to address the persistence of anonymity similar to that of physical currency [Lemke (2024)]. To mitigate the risks previously described, the Regulation authorizes the European Commission to impose transaction and holding limits on offline balances (Article 37(5)), a risk-based tradeoff again justified by the limited exposure at stake. Additionally, periodic synchronization, intended for updating balances and monitoring compliance with caps, may enhance supervisory mechanisms without compromising privacy.

4.4 Record keeping and auditability

AML compliance for CBDCs hinges on robust mechanisms for record-keeping and auditability, which facilitate both real-time monitoring and ex-post investigation.

As outlined, the digital euro draft proposal envisions robust digital identifiers as foundational to both its online and offline variants. Central to this framework are "user identifiers", unique pseudonymous strings assigned to clearly distinguish each user in online transactions (Article 2(27)), and "user aliases", which provide an additional layer of pseudonymity to protect user identities, visible only to PSPs and the users themselves (Article 2(28)). The regulatory structure mandates that audit trails must, at a minimum, include these identifiers along with transactional metadata and session details, such as IP address ranges.

PSPs processing online transfers, therefore, maintain detailed transactional records. Under the proposed regulations, each transaction generates immutable, tamper-evident records that are closely associated with user identifiers or their aliases. These logs, which document account numbers, timestamps, and session metadata, are designed to fulfill strict privacy-by-design requirements, preventing identification of users by any party other than the responsible PSP, explicitly excluding the ECB and national banks (Recital 71 draft digital euro regulation).

12. Not to be confused with the question of whether transactions themselves are account-based or value-based at the technical level [Armelius et al. (2021), Brunnermeier and Landau (2022)].

From an AML/CFT perspective, this architecture enables granular auditability: it supports compliance verification, suspicious activity reporting, and forensic investigations, thanks to the ready accessibility and integrity of the records. Nevertheless, ensuring interoperability with legacy financial audit systems will likely remain a significant priority [Lemke (2024)].

In contrast, the P2P nature of the offline digital euro is intentionally designed without detailed record-keeping. Transactions in this mode are ephemeral: no persistent audit logs or user linkages are maintained on the device or card during transfers, in line with privacy-enhancing protocols [Armelius et al. (2021)]. For AML/CFT efforts, this design introduces significant auditability gaps, as transactional data is absent - with the exception of balance information - until a wallet synchronizes with a PSP or the central system (for example, during recharging or conversion of funds). Legal obligations for PSPs arise at the moment of synchronization, when balances must be verified against minimum audit trail requirements. While this process partially addresses audit blind spots, delays and technical contingencies (such as device loss or theft) remain unresolved risks for continuous AML compliance.

4.5 Jurisdictional and other legal considerations

As previously discussed, AML/CFT compliance in the context of cross-jurisdictional CBDC operations is dominated by the need to ensure that digital currencies do not become vectors for illicit finance across borders [FIU (2023)]. AML regimes for CBDC systems reflect a movement toward centralized oversight, with the proposed establishment of the AMLA as the central supervisory and coordinating authority. AMLA's federated operational approach aims to harmonize supervision, impose uniform sanctions, and centralize information flows across PSPs and intermediaries facilitating or processing CBDC transactions, especially where cross-border operations are involved.

For the online digital euro, stringent AML compliance obligations are imposed on PSPs, and intermediaries, regardless of the cross-border nature of transactions.[13] Distribution of the system to third-country persons is contingent on a formal agreement of their countries with the E.U., as set forth in Article 19 of the digital euro proposal [FIU (2023)]. Such agreements require third-country national banks and competent authorities to abide by ECB rules, disclose relevant usage information, and adopt regulatory standards that are materially equivalent to those in the Union, particularly regarding AML obligations (Article 10 draft digital euro regulation). Failure to maintain equivalency or to address strategic AML deficiencies can result in the suspension or termination of access, with the ECB exercising oversight on foreign PSP compliance (Article 20 draft digital euro regulation).

Offline functionality, while technically distinct, does not circumvent AML requirements in cross-border settings. Offline devices physically moved to third countries distributing offline digital euro must also uphold ECB-imposed limits and adhere to substantive AML controls, as stipulated in Article 19(5).[14] The legal framework is designed to allow restriction, suspension, or termination of third-country participation in cases of inadequate AML frameworks, grounding operational risk mitigation in binding intergovernmental agreements and enforceable regulatory standards.[15]

4.6 Summary

In summary, the digital euro presents differentiated responses to AML/CFT risks depending on its mode of use. The online variant essentially builds upon and enhances existing KYC and transaction monitoring frameworks, with the digital E.U. identity wallet expected to significantly improve data quality and accessibility for AML compliance. In contrast, the offline variant requires an explicit policy decision: permitting full transactional anonymity, albeit limited by transaction and holding caps, which entails accepting a residual level of AML risk. This tiered approach represents carefully calibrated trade-offs between AML safeguards and user privacy, aligning legal compliance with the realities of practical implementation.

13. Access to foreign nationals, however, is possible, as Article 13 of the draft digital euro regulation explicitly allows visitors to the E.U. to onboard.
14. Recital 47 of the draft digital euro regulation emphasizes the objective of aligning with the G20 agenda concerning cross-border payments and remittances.
15. It remains to be seen whether blacklisting will be possible (and effective) for foreign nationals' devices, especially if those devices do not, or may never, reconnect to the online environment.

5. Conclusion

A closer examination of the complex AML/CFT challenges and opportunities arising from the ongoing development and anticipated deployment of CBDCs, particularly with regard to the digital euro, reveals an interesting balancing act. The analysis reveals that the AML/CFT framework for the digital euro is inherently bifurcated, reflecting not only legacy compliance models but also novel privacy considerations and risk-based trade-offs. The online variant emphasizes well-established KYC procedures, continuous transaction monitoring, and integration with digital identity infrastructure: features that are likely to surpass the surveillance and traceability capabilities of traditional banking or physical cash. This approach, overseen by the recently created AMLA, may represent a watershed moment for the effectiveness of AML/CFT measures by leveraging high-quality, real-time data and robust audit trails.

Nevertheless, the digital euro carries significant operational and systemic risks. Real-time settlement centralized at the ECB or designated intermediaries introduces new centralization risks and the possibility of operational single points of failure. By contrast, the offline functionality, designed to mimic the privacy and immediacy of cash, relies on restrictive transaction limits as its primary AML safeguard. Calibrating these limits involves significant systemic repercussions: if set too low, they may undermine the public's ability to access resilient offline liquidity during crises, potentially encouraging capital flight or substitution with physical cash or alternative emerging stablecoin alternatives [Lagarde and Panetta (2022)].

In light of these findings, the importance of robust and adaptive AML frameworks in the context of the digital euro cannot be overstated. AML/CFT policies must do more than merely extend existing standards; they must address the paradigm shifts brought about by programmable and data-rich digital money. Innovations in AML, including machine learning-based anomaly detection, privacy-preserving analytics (e.g., enabled by zero-knowledge proofs), and dynamic risk scoring, should be prioritized for pilot implementation, supported by rigorous transparency and oversight arrangements. Policy developments must anticipate and specifically regulate technological and operational barriers to AML/CFT compliance, such as cross-jurisdictional data fragmentation, identity portability, and resistance to surveillance from both public and private actors. Legal and ethical considerations require renewed focus on proportionality, necessity, and accountability as core principles, to ensure that AML/CFT measures do not become overreaching, erode civil liberties, or exacerbate financial exclusion.

The trajectory of CBDC adoption suggests that public perception and stakeholder resistance will continue to evolve partially in response to the perceived trade-offs between privacy and transparency. Ultimately, the AML/CFT framework for the digital euro will serve as a bellwether for broader regulatory and technological adaptation within the E.U. Policymakers must ensure that AML objectives are neither compromised in the name of innovation nor used as tools to undermine fundamental rights and economic inclusion.

References

Aldasoro, I., M. Aquilina, U. Lewrick, and S. H. Lim, 2025, "Stablecoin growth – policy challenges and approaches," Bank for International Settlements, https://tinyurl.com/yc52ka2j

Armelius, H., C. A. Claussen, and I. Hull, 2021, "On the possibility of a cash-like CBDC," Sveriges Riksbank

Auer, R., G. Cornelli, and J. Frost, 2023, "Rise of the central bank digital currencies," International Journal of Central Banking 19, 185-214

Bank of Japan, 2025, "Central bank digital currency experiments progress on the pilot program (May 2025)," Payment and Settlement Systems Department Bank of Japan

Bidder, R., T. Jackson, and M. Rottner, Matthias, 2025, "CBDC and banks: disintermediating fast and slow," BIS working papers no. 1280, Bank for International Settlements

BoE, 2025a, "Product Strategy," Bank of England, https://tinyurl.com/stdhf75d

BoE, 2025b, "Interoperability models for UK based payments," Bank of England, https://tinyurl.com/5n869hwu

Bidder, R., T. Jackson, and M. Rottner, 2025, "CBDC and banks: disintermediating fast and slow," Bank for International Settlements

Brunnermeier, M. K. and J.-P. Landau, 2022, "The digital euro: policy implications and perspectives," European Parliament

E.C., 2021, "Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity," June 3, European Commission

E.C., 2023a, "Proposal for a Regulation of the European Parliament and of the Council on the legal tender of euro banknotes and coins, COM/2023/364 final," European Commission, June 28

E.C., 2023b, "Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro, COM(2023) 369 final," European Commission, June 28 (cited as: Digital Euro Proposal)

ECB, 2021, "Report on the public consultation on a digital euro," European Central Bank

ECB, 2024, "Study on the payment attitudes of consumers in the euro area (SPACE)," European Central Bank

ECB, 2025, "Progress on the preparation phase of a digital euro: third progress report," European Central Bank

E.U., 2024a, "Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro (Text with EEA relevance)," European Union, March 19

E.U., 2024b, "Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (Text with EEA relevance)," European Union, June 19

FIU, 2023, "The AML/CFT implications of central bank digital currency and the digital euro," Financial Intelligence Unit of Latvia

Jenko, M., 2025, "Interview with Piero Cipollone," conducted by Miha Jenko on July 10, 2025

Lagarde, C., and F. Panetta, 2022, "Key objectives of the digital euro," The ECB blog, 13/2022

Lemke, C., 2024, "Function follows form or form follows function – the legal nature of CBDC," European Property Law Journal 12:2-3, 211-279

Panette, F., 2023, "Shaping Europe's digital future: the path towards a digital euro," speech to the Committee on Economic and Monetary Affairs of the European Parliament, September 4, 2023, available at https://tinyurl.com/3d4ub76d

Reserve Bank of India, 2025, "Report of the Central Board of Directors on the working of the Reserve Bank of India for the year ended March 31, 2025," Reserve Bank of India.

Sillaber, C., and M. Eggen, 2024, "Privacy in payments: what a CBDC can do better than commercial bank money," https://tinyurl.com/4h4hbpsr

WE MAKE THINGS HAPPEN.

Leading change in Financial Services.

BELGIUM
UNITED KINGDOM
THE NETHERLANDS
FRANCE
GERMANY
SWITZERLAND

www.projectivegroup.com

Projective INSTITUTE