One Customer, Two Mandates

Author: Ran Weissblech, CFRCP/BFRCP, Int.Dip(AML), LL.B, Fellow, Digital Euro Association, Member of Compliance Institute's Consumer Protection Working Group.

CPC 2025, the EUDI Wallet, and the compliance desk in 2026

Consider an illustrative scenario. A consumer in Cork opens her phone, taps a credential from her Government Digital Wallet into a new bank's onboarding flow, and her current account is live in under three minutes. Two weeks later, she authorised a card payment with the same wallet. The transaction fails. She complains. The bank refers her to the wallet provider. The wallet provider refers her back to the bank.

The scenario is illustrative, not a real complaint. Under Regulation (EU) 2024/1183 (eIDAS 2.0), every Member State must make at least one digital identity wallet available to citizens by the end of 2026. From late 2027, banks, payment institutions and e-money firms must accept the wallet for Strong Customer Authentication where SCA applies.

The challenge for compliance functions is a reconciliation problem. Brussels demands technical interoperability. The Central Bank of Ireland demands specific consumer outcomes. When eIDAS 2.0 and the Consumer Protection Code 2025 meet in the same customer journey, the regulated firm owns whatever happens inside it. Law firm briefings have analysed each regulation in isolation. This piece treats convergence as the operational problem facing Heads of Compliance now.

The Governance Paradox

The Board must look past the convenience and see the underlying dependency. The wallet appears to be a plug-and-play solution for KYC. In practice, firms encounter difficulty when selective disclosure (proving a user is over 18 without revealing a date of birth) meets a legacy core banking system designed for the data retention requirements of the Criminal Justice Acts.

If the system cannot persist the data the wallet minimises, the next audit will be a difficult one.

This is the scrutiny point under the Section 48 Consumer Protection Regulations. Under the Central Bank (Supervision and Enforcement) Act 2013, the CBI looks for evidence that the Board considered the risks of digital-first journeys before they went live. The CBI's General Guidance on the Consumer Protection Code, updated December 2025, reinforces the expectation that firms must be able to demonstrate proactive governance over digital service design rather than retrospective justification. Not a checkbox. Evidence.

The AML Paradox: Minimisation versus Retention

The inherent tension is between privacy and auditability. eIDAS 2.0 is built on data minimisation. The wallet gives the firm only what it needs. The Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010 to 2021 require firms to retain verified audit trails for five years.

Firms are caught between two opposing legal mandates. A practical compliance approach is to design what could be called a Persistence Layer. Not just storage. The digital signature and timestamp of the wallet credential must be saved in a format a CBI inspector can verify three years from now. If the front door is digital, the audit trail cannot be ephemeral.

Section 48 and the Cork Scenario

In an outcome-focused regime, referring the customer back to the provider is a conduct failure. When the CBI inspects compliance with the Section 48 Consumer Protection Regulations, they focus on consumer detriment. If the consumer in Cork is left in a loop between her bank and a government app, the bank is the party that will face the supervisory consequences.

This requires a shift in how firms treat the wallet provider. Resolution scripts, staff training, and complaint-handling protocols must be designed to solve the customer's problem first and settle the inter-provider liability in the background.

The Payments Dimension

The Payment Services Regulation will reshape this further. PSD3 and the PSR reached provisional political agreement in late 2025. Official Journal publication is expected in H1 2026. The PSR will apply directly 18 months after entry into force. PSD3 requires national transposition within 18 months. Operational application across the EU is expected in late 2027 to Q2 or Q3 2028.

The PSR introduces direct PSP liability where a firm fails to implement appropriate fraud prevention mechanisms. It extends impersonation fraud refund obligations beyond PSP staff impersonation to broader categories. The shift from staff-impersonation to broader impersonation refund liability is the change that will keep fraud teams awake.

The PSD2 and eIDAS 2.0 liability question sits unresolved alongside this. PSD2 makes the payment service provider liable for unauthorised transactions, subject to defined exceptions. eIDAS 2.0 places liability on the issuing Member State for negligence in wallet provision. The Regulatory Technical Standards on SCA have not yet been updated to reflect wallet-based authentication.

Where the Frameworks Collide

PSD3 and the PSR apply to the same customer interactions that CPC 2025 governs. The PSR's fraud prevention liability extends a firm's exposure precisely at the authentication step where the wallet operates. CPC 2025's outcome lens then asks whether the customer was treated fairly when fraud occurred. Two frameworks. One transaction. One firm carrying the weight of both.

This compounds the Governance Paradox. The firm cannot treat wallet adoption as a payments project under PSD3 and a conduct project under CPC 2025 with separate workstreams. The frameworks share the same customer interaction. Governance structures that split them across committees will find the seams under inspection.

The AML Paradox extends into payments. The Instant Payments Regulation requires the payer's PSP to verify the payee's name against the IBAN, querying what the payee's PSP holds. Where the record came from a wallet attestation, the PSP must preserve cryptographic evidence for both VOP queries and AML audit.

For Heads of Compliance, the practical shift is simple to state and difficult to deliver. Wallet readiness is no longer a 2027 question. It is a 2026 question, because PSD3 and CPC 2025 expectations are already shaping how firms must design the journey the wallet will eventually authenticate. The architecture decisions taken this year set the supervisory exposure for the next five.

Preventing Digital Redlining

The risk of exclusion runs alongside the conduct question. Under the Standards for Business Regulations 2025, the CBI is increasingly sensitive to Digital Redlining. If wallet-based onboarding is a dream and the manual alternative for the elderly or non-tech-savvy is a nightmare, the firm carries a conduct risk.

The CBI will expect Management Information that compares the two paths. Are abandonment rates higher for vulnerable groups? Is success parity equal across demographics?

Considerations for Firms, Heads of Compliance and Board Members

Four areas warrant attention.

1. **Contractual Mapping**. Formally classify the wallet provider within your Third-Party Risk Management framework. A state-issued solution should not automatically be treated as low risk. Regulatory accountability remains with your firm.
2. **Consent Granularity**. Review your UI and UX carefully to ensure customers can clearly distinguish between the data required for Strong Customer Authentication (SCA) and any optional information collected for internal profiling or analytics. Transparency will matter as much as compliance.
3. **The Resolution Protocol**. Prepare frontline teams for wallet failures before they happen. Customers will expect immediate resolution, regardless of whether the fault sits with your systems, the wallet provider, or another intermediary. Staff should have clear scripts, escalation paths, and authority to act quickly.
4. **Audit Trail Verification**. Test whether your AML record-keeping obligations can withstand the limitations of selective disclosure within the wallet framework. Ensure critical records remain accessible and defensible even after older software versions are retired.

Conclusion

The EUDI wallet is a conduct risk event with direct supervisory implications. The mandate originates in Brussels. The consequences will be enforced locally. Firms that address these operational friction points now move from reactive compliance to evidence-ready posture before the inspections begin.

Index of References

1. Central Bank of Ireland, Consumer Protection Code 2025, published 24 March 2025, effective 24 March 2026.
2. Central Bank Reform Act 2010 (Section 17A) (Standards for Business) Regulations 2025.
3. Central Bank (Supervision and Enforcement) Act 2013 (Section 48) (Consumer Protection) Regulations 2025.
4. Central Bank of Ireland, General Guidance on the Consumer Protection Code, December 2025 update.
5. Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (eIDAS 2.0).
6. Commission Implementing Regulations on the European Digital Identity Wallet, adopted November 2024.
7. Directive (EU) 2015/2366 (PSD2) and Commission Delegated Regulation (EU) 2018/389 (RTS on SCA).
8. Proposal for a Directive on Payment Services and Electronic Money Services in the Internal Market (PSD3) and Proposal for a Payment Services Regulation (PSR), provisional political agreement 27 November 2025; Council 'I' Item Note 23 April 2026; publication expected H1 2026.
9. Department of Finance, National Payments Strategy, October 2024.
10. Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010 to 2021.
11. Arthur Cox, The EU Digital Identity Wallet: What companies need to know, November 2025.
12. William Fry, PSR/PSD3: EU Payment Services Legislation is Agreed, November 2025.
13. Norton Rose Fulbright, PSD3 and PSR: From provisional agreement to 2026 readiness, March 2026.
14. Matheson, Revised Consumer Protection Code: Entry Into Force, March 2026.