

EU RegCORE Client Alert

Financial Services

November 2026

Dr. Michael Huertas
Tel: +49 160 97375760
michael.huertas@pwc.com

EU RegCORE Team
de_regcore@pwc.com

EBA factsheet on white labelling – what banking and payment firms need to evidence

QuickTake

On 9 November 2026, the European Banking Authority (the **EBA**) published a consumer factsheet, "*Look beyond the brand – what to check before buying banking or payment product/services*", building on its 14 October 2025 Report on white labelling, EBA/REP/2025/30 (the **Report**).[1] Although addressed to consumers, the factsheet matters as much to firms. It sets out, in plain terms, the questions that customers, complaints bodies and supervisors may ask of any product sold under a partner's brand: who provides it, who is responsible and how rights can be exercised.

Those questions draw directly on the Report, which found that more than a third of the banks surveyed use white labelling, confirmed that the provider bears ultimate responsibility for compliance and led the EBA to

[1] See EBA, Factsheet on white labelling - what to check before buying banking or payment services (9 November 2026), pp. 1-2, and EBA, Report on white labelling, EBA/REP/2025/30 (October 2025).https://commission.europa.eu/publications/2027-commission-work-programme-and-annexes_enhttps://commission.europa.eu/publications/2027-commission-work-programme-and-annexes_enhttps://commission.europa.eu/publications/2027-commission-work-programme-and-annexes_en

include white labelling in its 2026 supervisory priorities.[2] For providers and their partners, the factsheet is therefore an early indication of the standard against which their customer journeys are likely to be judged. This Client Alert reflects the position as at 12 November 2026.

Why the brand does not shift responsibility

"White labelling" describes an arrangement in which a financial institution (the **provider**) supplies financial products or services that are distributed to customers solely under the brand of another entity (the **partner**), which may or may not itself be regulated. The factsheet gives everyday examples: a grocery shop offering a payment card that is in fact provided by a financial services company, or a pay-later option at an online checkout that is supplied by a firm other than the platform displaying it. It asks customers to establish who actually provides the product, what it is, what it costs, who handles complaints, how to terminate, how personal data are used and whether an offer may be a scam. It is consumer education and creates no new authorisation regime or implementation deadline.

For regulated firms, however, each of those questions corresponds to existing duties, and customers' own checks do not, by themselves, establish that the provider has discharged them. The product and partner review set out below is this alert's practical recommendation, not a requirement of the factsheet.

The Report found that 35% of banks responding to the EBA's Spring 2025 Risk Assessment Questionnaire (**RAQ**) engage in white labelling, across account and payment services, credit provisioning and open banking.[3] It identified no area of EU law requiring amendment, but committed the EBA to supervisory convergence work in 2026, and white labelling featured in the 2026 Union Strategic Supervisory Priorities (**USSP**).[4] Scrutiny will therefore take place under existing rules.

Three questions for management now

- **Who does what? – Banks, e-money and payment institutions acting as providers.** For each partner, map who contracts with the customer, accepts instructions, performs customer checks, holds funds and handles complaints, and record whether each task is outsourced, performed by an agent or relied upon.

- **What did the customer actually see? – Product and compliance teams.** Retain the screens, versions of terms and delivery records a customer actually receives through the partner, and reconcile provider identity, licence status, prices and complaint routes against the provider's own disclosures.

- **What happens if the partner becomes unavailable? – Partners, investors and acquirers.** Test exit, disruption and partner-failure scenarios for representative account types, and use the findings to inform launch, expansion and transaction terms.

None of these questions is new. Each reflects a finding in the EBA's own work, and firms that can show supervisors how they have answered them will be better placed when that work turns into supervisory dialogue. The EBA's publications, and the findings that matter most for firms, are summarised below.

---

[2] See coverage of the EBA 2026 work programme here and the 2027 programme here.

[3] See EBA, Report on white labelling.https://legal.pwc.de/en/news/articles/european-commission-publishes-its-annual-work-programme-2026-a-focus-on-financial-services-issues

[4] See our coverage on the USSP here.

What the EBA has published

The factsheet is the consumer-facing output of a workstream that began with the EBA's 2024–25 priorities on innovative applications. The Report draws on a May 2024 survey answered by 23 national competent authorities (**NCAs**) and the Single Supervisory Mechanism, a January 2025 industry and consumer workshop and the EBA's semi-annual RAQ covering 85 banks. Its analysis is largely qualitative because white labelling agreements are confidential and rarely captured in supervisory notifications.

The table below summarises the findings that are likely to matter most for firms.

Topic	EBA finding	Implication for firms
Scope	White labelling means distribution under the partner's brand only. Co-branded products fall outside it, and it differs from banking-as-a-service, which can retain the bank's brand.	These boundaries organise the Report; the applicable law still depends on each entity's activities and permissions.
Products and customers	Three clusters: account and payment services, credit provisioning (including buy now pay later) and open banking. Most products are offered to consumers and SMEs.	Consumer-facing rules on information, credit and complaints will usually be engaged.
Participants	Credit and e-money institutions are the main providers. Non-financial partners, including retailers, telcos and some BigTechs, are increasingly common.	Providers need to ensure that unregulated partners understand permissible activities and required measures.
Consumer risks	Mis-selling and misleading information, fraud, difficulties in complaints handling, data protection concerns and financial exclusion.	Disclosures should show clearly who provides the product and how to complain.
Provider and partner risks	Business model, operational, reputational and step-in risk, a lack of direct customer relationship and regulatory and compliance risk, including AML/CFT.	Exit plans and data-access rights need to work in practice, not only on paper.
Supervisory challenges	Opaque arrangements, inconsistent qualification as outsourcing or agency across Member States, unreliable passport notifications and no direct supervision of many partners.	The same arrangement may be qualified differently in different host Member States.
Next steps	No EU-law amendment needed. Supervisory dialogue and case studies in 2026, a questionnaire for NCAs, continued RAQ monitoring and a focus on consumer-facing disclosures.	Supervisors are likely to ask firms how each arrangement is qualified and documented.
Consumer factsheet	Seven checks for consumers, from identifying the provider to recognising fraud, with the takeaway that the brand alone does not determine customers' rights.	Each check maps to an existing duty that firms should be able to evidence.

Opportunities as well as risks

Crucially, the Report also recognises opportunities of the white label model. It identifies cost efficiency, an expanded offer, better targeting of products, a larger customer base and faster digital transformation for providers constrained by legacy systems. It also sees scope to improve financial inclusion, create new revenue streams and foster competition by lowering partners' barriers to entry, with some partners later acquiring their own licence. Whether these benefits or the associated risks predominate depends on the features of each arrangement, including whether white labelling is a core or ancillary activity. A provider

whose only or dominant activity is white labelling depends mainly on partners to attract customers, while an ancillary provider also distributes under its own brand.

Fees vary with the arrangement. Providers generally charge partners flat set-up and recurring fees plus per-use fees, such as per-transaction or per-API-call charges or commissions on volumes. Partners may charge providers broker or platform-access fees, or charge customers for access to the interface in addition to the product's own price, and any pure technical provider in the chain charges separately. Cross-border use is growing: 11 NCAs reported home-state firms serving other Member States through white labelling, and 9 host NCAs observed incoming arrangements.

Identifying the provider and allocating responsibility

The Report observes that providers, as the entity with which the customer ultimately contracts, bear ultimate responsibility for regulatory compliance. They typically perform AML/CFT checks, receive and control customer funds, operate back-office infrastructure for record-keeping and regulatory reporting and ultimately handle complaints. Partners typically operate the customer-facing interface, collect onboarding information, market the product and disclose its terms. The factsheet makes the same point from the customer's side: both companies should be named in the terms and conditions, and the provider should state its licence or registration status.

Outsourcing, agency or reliance

The regulatory qualification of an arrangement depends on its precise terms. The Report identifies three principal routes. Where the provider outsources customer due diligence (**CDD**) tasks to the partner, it remains responsible for compliance and the allocation must be clearly documented. Where the partner acts as a payment agent, agent-specific obligations apply in addition to any outsourcing requirements, and these vary between Member States. Where the partner is itself an authorised obliged entity, the provider may in specific cases rely on its CDD under the third-party reliance provisions. The Report notes that the same arrangement may be qualified differently in different Member States, which may require multiple compliance processes for cross-border offerings, and that white labelling of certain products may be limited or precluded by national law. On 18 September 2026, the EBA published final Guidelines on the sound management of third-party risk regarding non-ICT services (EBA/GL/2026/09), which will replace the existing Guidelines on outsourcing arrangements when they apply; as at the cut-off of this alert they await translation and are not yet applicable.[5] Distribution, agency, outsourcing, ICT services and credit intermediation can overlap, so each activity should be assessed by entity and jurisdiction, including for cross-border delivery.

For payment institutions, Articles 19 and 20 of the second Payment Services Directive (**PSD2**) address agents, outsourcing and responsibility: the institution remains fully liable for the acts of its agents and of entities to which it outsources activities. That does not make every provider liable for every act of an independent commercial partner, which is why the qualification matters.[6] Electronic money institutions may distribute and redeem electronic money through persons acting on their behalf, but may not issue it through

[5] See our coverage on this here.

[6] See Directive (EU) 2015/2366 (**PSD2**).

agents; they may provide payment services through agents under PSD2. The functions of a branded wallet should be allocated accordingly.[7]

BigTech, marketplace and crypto-asset partners

The Report records that fewer than 5% of banks responding to the Spring 2025 RAQ had white labelling agreements with BigTechs, down from 10% in 2024, possibly because earlier pilots had ended. It warns that smaller institutions may face imbalances in bargaining power, growing data asymmetries and operational risk from frequent interface changes, and should address the implications for their own supervisory obligations ex ante and on an ongoing basis. Marketplaces may use a payment service provider's acquiring services rather than obtaining their own licence; depending on how services are branded, those agreements may also constitute white labelling.

The Report also anticipates growing use of white labelling in the crypto-asset sector, including issuance of stablecoins as a service for entities that wish to integrate a crypto offering without necessarily requiring their own authorisation under the Markets in Crypto-Assets Regulation (**MiCAR**). That does not create an exemption: authorisation, notification and conduct requirements must still be assessed separately for each participant according to its activities as issuer, offeror or crypto-asset service provider. Its discussion of the proposed Framework for Financial Data Access as a driver of white labelling should now be read against the Commission's stated intention, recorded in its 2027 work programme annexes, to withdraw that proposal.[8]

Translating consumer reminders into firm controls

Each of the factsheet's checks corresponds to existing duties. The comparison below takes payment services as the main illustration and sets each EBA reminder against selected existing duties under PSD2 and the EU's General Data Protection Regulation (**GDPR**) and our recommended implementation, which the factsheet does not prescribe. The PSD2 information entries concern framework contracts, subject to the Directive's scope and permitted derogations. Applicability depends on the product, role and relevant law, and deposit and credit products require separate application of their own product rules.[9]

EBA consumer reminder	**Selected existing duties**	**Recommended implementation**
Identify the provider and contracting party	Provider, supervisory and register information under PSD2 Article 52(1); disclosure of payment-agent capacity where applicable under Article 19(7).	Reconcile identities and permissions across the app, contractual terms and required durable-medium information.
Understand the product and fit with the customer's needs	Description of the payment service's main features under PSD2 Article 52(2)(a); application of the relevant deposit, electronic-money or credit regime.	Record product classification and explain the resulting protections and obligations.
Understand cost, interest and duration	Relevant charges, interest and exchange-rate information and contractual duration under PSD2 Articles 52(3) and 52(6)(b).	Reconcile advertised and contractual prices, identify separate partner fees and control material changes.

[7] See Directive 2009/110/EC (**EMD2**).

[8] See MiCAR, Regulation (EU) 2023/1114, Arts 16, 48 and 59–60; European Commission, Commission Work Programme 2027, Annexes, COM(2026) 710 final (4 November 2026), Annex III, item 5 and note 2, p. 14.

[9] See EBA, Factsheet on white labelling, See PSD2; and GDPRhttps://eur-lex.europa.eu/eli/dir/2026/806/oj/eng.

Know how to complain	Effective complaint procedures and applicable response periods under PSD2 Article 101.	Test receipt, routing and escalation across both firms; retain dates and identify the responsible owner.
Check termination and whom to notify	Termination information and applicable framework-contract termination rights under PSD2 Articles 52(6)(c) and 55.	Test each relevant contract separately and explain continuing balances, charges, rights and access.
Check how personal data is used and shared	Lawful processing, transparency and allocation of duties according to actual roles under GDPR Articles 5–6, 13–14, 26 and 28.	Match privacy information to actual data flows, purposes and access controls.
Watch for pressure, implausible offers and impersonation	Relevant security, notification and authentication duties and assessment of unauthorised-payment claims under PSD2 Articles 69–74 and 97–98.	Test fraud-reporting and blocking routes, coordinate escalation and explain genuine customer contact channels. The factsheet also refers customers to the EBA's factsheets on buying financial products online and on online frauds and scams in an AI world.

Evidence of what the customer received

For PSD2 Title III information requirements, the payment service provider bears the burden of proving compliance. Publishing a template does not, by itself, establish what a particular customer received. As a practical matter, we recommend that providers retain the actual customer screens, versions of terms and delivery records, and control partner changes to product descriptions, prices and contact routes.[10] Advertised and contractual prices should be reconciled, separate partner fees identified and material pricing changes approved. The factsheet suggests two practical tests that firms can apply to their own journeys: whether a customer would find wording such as "service provided by…" or "issued by…" identifying the provider, and whether it is clear when a payment option is in fact a form of credit. It also reminds customers that a loan is repaid to the provider, not to the brand. The Report notes that partners sometimes display the provider's licence on their websites in a way that leads consumers to believe they are dealing directly with a regulated entity.

For PSD2 complaints concerning rights and obligations under Titles III and IV, providers must generally respond within 15 business days of receipt. Where, exceptionally, the answer cannot be given within that period for reasons beyond the provider's control, it must send a reasoned holding reply, and the final response must be received within 35 business days of receipt. Member States may maintain or introduce more advantageous provisions. In practice, we recommend that routing between partner and provider supports that timetable, and that receipt, escalation and response dates are recorded for both firms.[11] The Report notes that complaints-handling difficulties may be greater where the provider and partner are located in different Member States. The factsheet also reminds customers that terminating may require notice to both the brand and the provider. Each relevant contract should therefore be tested separately, and customers told what happens to balances, charges and access after termination.

[10] See PSD2. See also EBA, Report on white labelling.

[11] See PSD2 including the possibility of more advantageous national rules.

Fraud and product protection

The factsheet closes its checklist with a warning: if an offer seems too good to be true, or the customer is pressured to act quickly, it may be a fraud or scam. White labelling can make that risk harder to spot, because customers may not know which company genuinely works for the provider or the partner, and the Report notes that fraudsters exploit precisely that uncertainty, sometimes using virtual IBANs to impersonate others. The EBA's fraud warning does not, however, alter the statutory consent, evidence and liability rules. PSD2 rules apply alongside the user's duties to protect credentials and notify misuse, and where a user denies having authorised an executed payment transaction, the recorded use of a payment instrument is not, by itself, necessarily sufficient to prove authorisation, fraud or gross negligence. Each case still turns on those rules and its facts, and a general warning should not be treated as conclusive evidence that the customer breached those duties. Firms should instead test fraud-reporting and blocking routes and explain the genuine customer contact channels.[12]

The factsheet also asks customers to check the nature of the product, warning that a payment option might also constitute a form of credit, and to understand the total cost, interest and any extra fees. Under white labelling, those features are often presented by the partner rather than the provider, so the explanation needs to be precise. For eligible deposits, the ordinary EUR 100,000 coverage level applies per depositor per credit institution, so different brands do not ordinarily create separate limits; electronic money safeguarding should be distinguished from deposit guarantees.[13] Member States must apply national measures implementing the revised Consumer Credit Directive (**CCD2**) from 20 November 2026, and its wider scope can capture buy now pay later (**BNPL**) models, subject to exclusions and transitional provisions. Firms should check the creditor, payment period, charges and national implementation before relying on any exclusion.[14]

Making controls work through the partner

Customer due diligence

The Report finds that providers usually perform AML/CFT checks themselves, sometimes relying on preliminary screening by partners, and should carry out ex ante checks on prospective partners, with additional scrutiny where the partner's money laundering and terrorist financing risk is higher. About half of Member States assess white labelling risks specifically, mostly rating them medium or high. Under the current Anti-Money Laundering Directive (**AMLD**), statutory reliance leaves ultimate responsibility with the relying obliged entity. The third party must be eligible, the relying entity must obtain the necessary CDD information and it must take adequate steps to ensure that relevant identification and verification records are supplied immediately on request; an unregulated retailer is not automatically an eligible third party. Outsourcing and agency follow a separate route. The Anti-Money Laundering Regulation (**AMLR**) will introduce directly applicable CDD rules, with its own outsourcing and reliance framework generally applying from 10 July 2027; its timing and access requirements should be assessed on their own terms rather than by carrying over the current AMLD rule.[15] By 1 January 2026, the EBA's standalone AML/CFT mandates and functions had

---

[12] See PSD2, Arts 69–74, in particular Art. 72(2), and Arts 97–98.

[13] See Directive 2014/49/EU (DGSD); EMD2 and Directive (EU) 2026/804 introduces new rules for qualifying client-funds deposits, with national measures applying from 11 May 2028.

[14] See Directive (EU) 2023/2225 (**CCD2**).

[15] See Directive (EU) 2015/849, Arts 25-29; Regulation (EU) 2024/1624. See also EBA, Report on white labelling.

transferred to the Anti-Money Laundering Authority (**AMLA**). Existing EBA guidelines and standards continue until replaced, while the EBA retains its prudential work on money-laundering risks.[16]

A practical gap identified by the Report is data access: under outsourcing or reliance agreements, the provider may lack direct access to KYC records, transaction data and monitoring results because systems were not designed to share them. Failure to establish appropriate access arrangements may itself breach AML/CFT obligations. Separately, AMLD Article 19 prescribes enhanced measures, including senior management approval before establishing a new correspondent relationship, for cross-border correspondent relationships involving the execution of payments with a third-country respondent institution; that specific requirement does not extend to every white labelling arrangement.

The Report describes two common onboarding models. In the first, partners' customers are redirected to an interface developed, hosted and managed by the provider, which may be white-labelled to the partner's brand. In the second, the partner collects the customer information, sometimes performs initial verification and submits the application for approval. In both, the customer becomes active only once the provider approves, and providers usually perform ongoing risk monitoring themselves using real-time tools integrated through APIs. Where a retailer onboards customers for a white-labelled payment card, the agreement should specify which entity performs each step, which standards apply, how quickly records are supplied on request and how the provider audits the retailer. All reliance or outsourcing arrangements should be documented and auditable for supervisory purposes. Due diligence records alone do not authorise a payment; applicable authentication requirements remain relevant.

Personal data and accessibility

The Report identifies the risk of data misuse, breaches and unauthorised access where multiple entities hold customer data, and of either party using the data for other business purposes. The parties' data-protection roles should be allocated according to their actual activities, purposes and lawful bases; a partner is not automatically a processor or a joint controller, marketing consent cannot generally justify all compliance processing, and the commercial arrangement does not justify unrestricted access to customer data. Privacy information should match the actual data flows, purposes and access controls across both firms.

Accessibility also matters. Consumer organisations warned that digital-only delivery can exclude consumers who are not digitally confident and suggested that compliance with the European Accessibility Act can help to mitigate that risk.

The Report also encourages national action to improve digital and financial literacy, so that consumers can use digitally distributed services effectively, identify suspicious providers and enforce their rights.

Disruption, exit and step-in risk

Dependence runs both ways: a core white labelling provider relies on its partners, while partners face disruption if a provider discontinues a product, fails or loses its licence. For ICT services within the Digital Operational Resilience Act (**DORA**), contracts must address data recovery and assistance with related ICT incidents. For services supporting critical or important functions, firms need exit strategies that are reviewed and tested, and contractual transition arrangements. The Report also notes step-in risk: a provider may need to support a partner for reputational reasons, and only banks are subject to specific requirements to

[16] See EBA, EBA and AMLA complete handover of AML/CFT mandates (19 January 2026).

identify that risk ex ante. Consider a hypothetical payment account where the institution holds the ledger but the retailer controls authentication and support through its app. If the retailer ceases trading, the account agreement may survive while ordinary access disappears. Firms should establish whether the customer terms support an alternative channel. Where introducing that channel requires changes to a consumer payment framework contract or its prescribed information, the change generally requires a proposal at least two months before it applies.[17]

Supervisory outlook

White labelling in the 2026 priorities

The EBA's 2026 work programme lists value chain evolution among its three thematic innovation priorities. It states that the EBA may follow up the Report's conclusions on common understanding among NCAs, the regulatory qualification of arrangements and consumer-facing disclosures, and that it will monitor the role of BigTech in EU finance. It schedules, as programme targets, consumer financial education and supervisory convergence actions on white labelling, and monitoring of BigTech in banking and payments, for Q4 2026, after a revised consumer factsheet on buying products online or via mobile phone in Q3. As chair of the European Forum for Innovation Facilitators in 2026, the EBA will also focus discussion on cross-sectoral business models such as embedded finance. A Q2 roadmap for implementing the EU Payment Package will sequence the mandates under PSD3 and the Payment Services Regulation, which white label providers should track. Under key topic 2 of the USSP, technology integration and resilience, supervisors are to give attention to technological integration as an enabler of value chain evolutions such as white labelling and to their potential reputational and operational impacts. Annex III expects competent authorities to reflect the priorities and related topics in their on-site and off-site supervision, taking account of their supervisory context. The EBA's 2027 work programme, published on 30 September 2026, retains white labelling among further considerations for supervisors.

The Report adds that supervisors rarely focus on white labelling in line supervision. It announced supervisory dialogue in 2026, including individual case studies on regulatory qualification, a common questionnaire that NCAs may use on a voluntary basis and continued monitoring of banks' engagement through the RAQ. In our assessment, this continuing work supports preparation for further supervisory engagement and could inform additional EBA guidance or recommendations within its mandate. The Report identified no area of EU law requiring amendment, and the publication sequence creates no automatic rulemaking commitment. Binding technical standards would require a legislative empowerment and Commission adoption, and legislative change would require its own adoption process.

Cross-border notifications and supervisory reach

The Report finds that commercial partnerships typically need not be notified to NCAs unless the partner qualifies as a PSD2 agent or the arrangement is a material part of, or change to, the business model. Passport notifications are often made on a generic basis and do not capture the business model, and visibility is weaker still in triangular passporting, where a provider in one Member State uses a partner in a

[17] See DORA, Regulation (EU) 2022/2554, Arts 28(8), 30(2)(d), 30(2)(f) and 30(3)(f); PSD2, Art. 54.

second to serve customers in a third. Firms should expect host authorities to ask which local requirements, including any applicable to agents, have been considered.

Who may inspect

Relevant authorities can use information requests and, where warranted, on-site inspections under existing powers. Payment institution supervisors may inspect to check compliance with PSD2 Title II, while European Central Bank involvement is confined to its prudential tasks within the Single Supervisory Mechanism. The EBA publications reviewed for this alert do not announce a dedicated white labelling common supervisory action or inspection campaign.

The product and partner review recommended in this alert gives firms evidence for supervisory engagement and a basis for resolving gaps in ordinary service, disruption and exit in preparation for supervisory engagement.

Product and transaction decisions

The management review

Management should receive a product and partner review based on a risk-based selection of actual customer journeys. For each applicable duty, it should identify the responsible firm, the entity performing the task, evidence of performance, any unresolved dependency, the remedial owner and deadline and the decision required. Where a gap prevents lawful performance, it should be resolved before launch or expansion, and testing should be repeated after material changes to interfaces, authentication, data access or subcontracting.

Exit arrangements should be tested without ordinary partner cooperation. Across representative account types and realistic volumes, firms can demonstrate customer contact, account matching, authentication, complaint routing and instruction processing to a lawful outcome, recording failed dependencies, recovery times and remedial owners. Firms should obtain the third-party rights needed for that alternative and assess their enforceability. A lawful outcome may include justified restrictions or an orderly cessation.

Acquisitions and programme transfers

For an acquisition or programme transfer, the findings can inform completion conditions, funded remediation or consideration. A price adjustment alone cannot cure a gap that prevents lawful performance from completion. Transaction documents should specify continuing information and assistance obligations and establish any required customer agreements, permissions, consents and transfer arrangements for a replacement provider.

Ordinary transition assistance should be allocated separately from remediation following breach. The documents should also address customer communications, reauthentication, additional servicing and overlapping-provider costs, including who funds urgent work while liability is disputed, and whether those resources will be available if the partner cannot pay.

Relevant dates

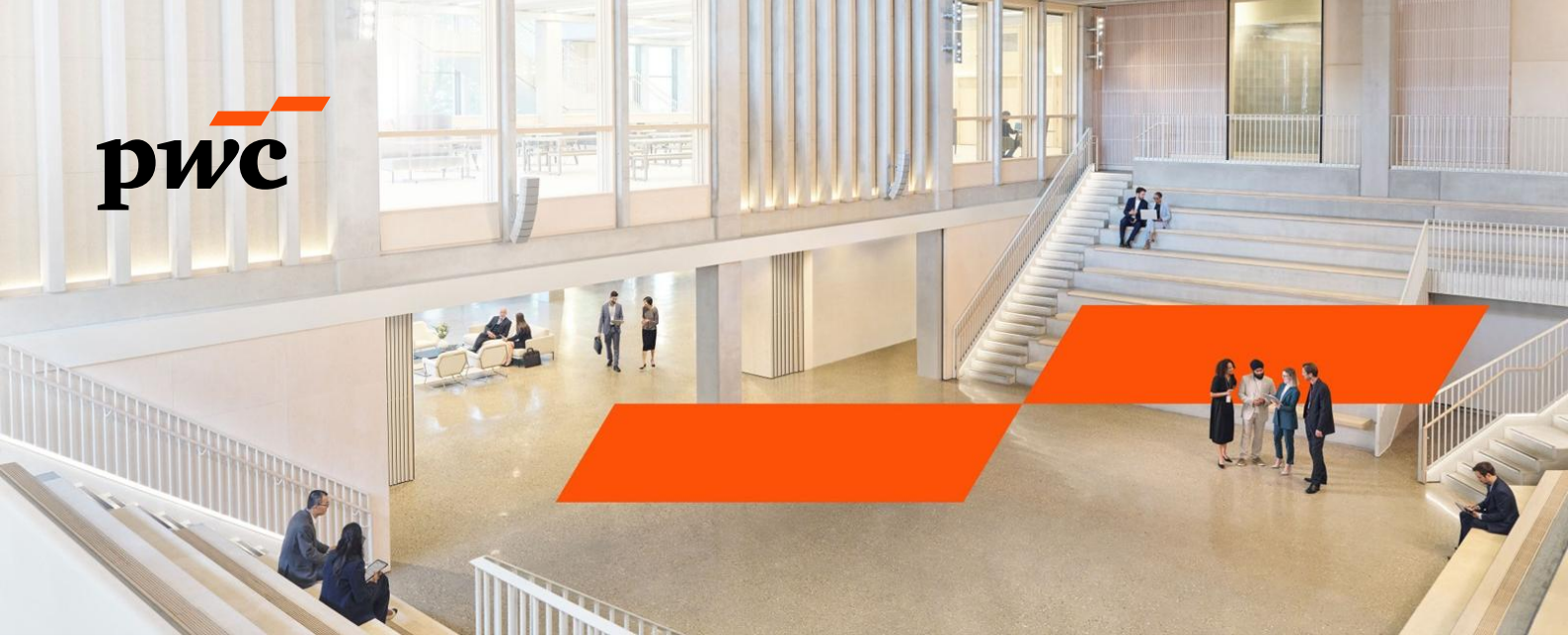
Several existing timetables apply to white-labelled products regardless of the pace of the EBA's convergence work.

Timing and source	Decision for the firm
20 November 2026 · CCD2	Confirm whether BNPL and other credit products distributed by partners fall within national CCD2 measures, and update creditor information and charges.
Q4 2026 · EBA work programme 2026	Prepare for supervisory convergence actions on white labelling by documenting the qualification of each arrangement.
10 July 2027 · AMLR	Review CDD outsourcing and reliance arrangements with partners against the AMLR framework.
11 May 2028 · Directive (EU) 2026/804	Assess client-funds deposit arrangements against new DGSD Article 8b and its aggregation rules.

Outlook

The factsheet tells customers to look beyond the brand, and firms should expect supervisors to ask the same of them. The Report identified no area of EU law requiring amendment and the EBA has not announced a dedicated inspection campaign, so the near-term test is likely to be applied under existing rules, through the supervisory dialogue, classification case studies and convergence work already scheduled. In our assessment, the questions will be practical: how each arrangement is qualified in each relevant Member State, which entity performs each regulated task and whether the provider can show what each customer actually received.

Firms that resolve those questions now will be better placed as several workstreams converge: the application of national CCD2 measures from 20 November 2026, the AMLR from 10 July 2027, the non-ICT third-party Guidelines once they apply, and the new client-funds deposit rules from 11 May 2028. Treating the white labelling review as a standing control, refreshed whenever a partner changes its interface, its subcontractors or its ownership, will also give management a sound basis for launch, expansion and transaction decisions, rather than a one-off response to the factsheet.



About us

PwC Legal advises financial services firms and market participants on regulatory developments of the kind discussed in this alert. Our multi-disciplinary and multi-jurisdictional team of sector experts assesses legislative and regulatory change against clients' legal entities, permissions and operating arrangements; reviews the resulting governance, contractual commitments and implementation dependencies; and supports clients in engaging with their supervisors, regulators and other market stakeholders, with coordinated advice across the relevant jurisdictions and disciplines.

This work is supported by our RegTech and SupTech tools for supervised firms, including PwC Legal's Rule Scanner, backed by managed solutions from PwC Legal Business Solutions. Rule Scanner supports horizon scanning and risk mapping of legislative and regulatory developments, sanctions and fines from multiple thousands of sources in over 170 countries.

Using the same technology, we can also digitise clients' internal policies and procedures into a version-controlled documentation inventory with a defined hierarchy and embedded glossary, so that changes in one policy are carried through to related documents, critical-path dependencies are mapped and developments requiring action are flagged.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award" and the "2025 Regulatory, Governance and Compliance Technology Award".

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Contact

Dr. Michael Huertas
Tel: +49 160 97375760
michael.huertas@pwc.com

EU RegCORE Team
de_regcore@pwc.com

© November 2026 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, which is a member firm of PricewaterhouseCoopers International Limited (PwCIL). Each member firm of PwCIL is a separate and independent legal entity.

www.pwc.de