European Banking Authority

EBA REPORT ON WHITE LABELLING

EBA/REP/2025/30 OCTOBER 2025

Table of Contents

List of figures

List of Tables

Abbreviations and glossary

AML/CFT	Anti-money laundering and countering the financing of terrorism
AMLD	Anti-Money Laundering Directive (Directive (EU) 2015/849)
API	Application programming interface
BNPL	Buy now pay later (as described in Recital 16 of Directive 2023/2225/EU)
CDD	Customer due diligence
ICT	Information and Communication Technology
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
KYC/KYB	Know your customer/know your business
NCA	National competent authority
PSD2	Payment Services Directive (Directive 2015/2366/EU)
SME	Small and medium-sized enterprises
White label partner	An entity offering financial products and services (provided by the white label provider) to customers under its own brand
White label provider	A financial institution providing financial products and services to customers through a white label partner

Executive Summary

The EBA has a statutory duty to monitor and assess market developments, including technological innovation and innovative financial services. As part of the EBA's 2024-25 priorities on innovative applications, the EBA is examining evolutions in the value chain for the distribution of financial products and services, with a specific focus on the use of 'white labelling' as a distribution model for banking and payments services in the EU.

White labelling refers to situation in which a financial institution (the provider) provides one or more financial products and services which are distributed and offered to customers under the brand of a partner (who may or may not be a regulated entity).

The report identifies that white labelling is a widespread business model, employed by 35% of the banks responding to the 2025 Spring RAQ. EBA data confirms that white labelling is being used to distribute a broad range of financial products and services (both domestically and cross-border), that can be grouped in three main clusters: account and payment services, credit provisioning and open banking services. The report finds that a large majority of white labelled products and services (such as deposit accounts, buy now pay later (BNPL) credit, e-money, payment services, and account information services) are offered to consumers and small and medium-sized enterprises (SMEs), while acquiring services, API-aggregation and data enrichment services[1], are mainly directed to SMEs and corporates.

White labelling arrangements vary depending on 7 key features: the regulatory status of the provider and partner, the allocation of tasks between them, the nature (core or ancillary) of the white labelling business model for the provider and partner, the products and services distributed, the target customers, the geographic distribution, and the fee model.

The report finds that potential benefits and risks for customers, providers and partners vary depending on the specificities of the white labelling agreement between provider and partner.

For instance, white labelling can benefit providers, partners and consumers in terms of cost efficiency and expanded offer; it can also contribute to enhancing financial inclusion. However, risks can also arise, including from potential mis-selling, fraud risk and weaknesses in AML/CFT controls, and a lack of transparency towards consumers as to precisely with whom they are contracting. Additionally, white labelling can pose challenges for supervisors, notably in terms of visibility over the full distribution channel.

The EBA has not identified areas of EU law that require amendments. However, the EBA identifies a need for supervisory convergence actions which the EBA plans to take forward in 2026, in

[1] API-aggregation refers to the process of combining multiple APIs into a single interface; data enrichment services consist into adding information to raw data to improve decision-making processes (e.g. for grating credit).

particular as regards the regulatory qualification (outsourcing, agency, other) of the arrangements between the parties and the assessment and identification of emerging risks.

To further enhance attention to white labelling, the model is being integrated into the key topics for supervisory attention set in the 2026 Union Strategic Supervisory Priorities (USSP). This report is expected to support NCAs in carrying out their supervisory activities including identifying the key features of white labelling and the potential risks. A questionnaire has also been developed to support NCAs in their day-to-day supervisory activities.

As regards consumer protection, the EBA intends to focus on appropriate measures to facilitate awareness by consumers of the key elements relating to white labelling.

Finally, the EBA will continue assessing the evolution of banks' engagement in white labelling via its regular Risk Assessment Questionnaire (RAQ) and wider innovation monitoring.

1. Introduction and purpose of the analysis

1. The EBA has a statutory duty to monitor and assess market developments, including technological innovation and innovative financial services[2]. In February 2024, the EBA Board of Supervisors endorsed the EBA's priorities on innovative applications for 2024-25[3], which include value chain developments, including 'white labelling' of financial products and services.

2. White labelling[4] comprises a business model in which a financial institution[5] (the provider) enters into an agreement with another entity (the partner, who may or may not be a financial institution) to distribute and offer one or more financial products and services under the partner's own brand only[6]. In some cases, partners do so by leveraging the provider's authorisation/license for the provision of financial products and services; in limited cases, partners may hold the relevant authorisation but may prefer not to provide directly the specific product or service and, instead, rely on the provider (e.g. for reasons of maintaining a streamlined business model carrying out only targeted financial services).

3. This report is intended to enhance understanding of white labelling as a business model by providing an overview of the landscape of white labelling in the EU (Section 3) and an assessment of potential opportunities (Section 4) and challenges (Section 5). The overview of challenges includes perspectives from consumers and competent authorities, including AML/CFT supervisors (where different), and identifies supervisory challenges. The report also sets out next steps to promote supervisory convergence and ensure adequate levels of consumer protection (Section 6).

[2] Article 9(2) of Regulation (EU) No 1093/2010 (EBA Founding Regulation), OJ L 331, 15.12.2010, p. 12–47.
[3] EBA Work Programme 2025, September 2024.
[4] White labelling should be considered as a different concept than Banking-as-a-service (BaaS), i.e. "the provision of banking services by banks through non-bank intermediaries (e.g. FinTechs, BigTechs and other firms) that serve as the interface to clients" (See BCBS, Digitalisation of finance, May 2024). Not all instances of BaaS fall under the EBA's definition, especially when these services maintain the branding of the (banking) provider.
[5] This report considers financial institutions that are under the scope of the EBA's sectoral mandate as defined by the EBA Founding Regulation, including credit Institutions (as defined in Regulation (EU) No 575/2013), e-money institutions (as defined in Directive 2009/110/EC), payment institutions (as defined in Directive (EU) 2015/2366), non-bank issuers of asset-referenced tokens (as defined in Regulation (EU) 2023/1114), and non-bank lenders, i.e. any lender that is not a credit institution and is authorised/registered at national level to grand credit of a kind referred to under the Directive 2008/48/EU and/or Directive 2014/17/EU.
[6] As such, financial products and services offered under the brands of both the provider and the partner (e.g. co-branded cards) are excluded from the scope of this report, as the customer has visibility on the details of the provider.

2. Methodology and limitations

4. The report has been informed by the following:

   a. Survey to competent authorities: the EBA issued a survey on white labelling in May 2024 ('the 2024 survey'), with the objectives to carry out a stocktake of use cases, to identify possible opportunities and risks, as well as any regulatory issues or supervisory challenges. In total, 23 NCAs responded to the survey; a response was also received from the Single Supervisory Mechanism (SSM).

   b. Workshop with industry and consumer organisations: the EBA organised a workshop in January 2025 ('the 2025 workshop') to gather further inputs on the topic. In total, 14 market participants and 3 consumer organisations attended the workshop representing a broad cross-section of partners and providers, products and services offered, and EU Member States/EEA jurisdictions.

   c. Market monitoring: the EBA conducts semi-annual Risk Assessment Questionnaires (RAQs) involving a sample of 85 banks. As part of the Spring 2024 and the Spring 2025 RAQs, the EBA included a question on banks' participation in white labelling business models.

   d. Desk-based research and industry engagement: EBA staff reviewed academic papers and analyses carried out by international standard-setting bodies. EBA staff also carried out wider desk-based research, news monitoring and industry engagement.

5. Data limitations arise due to: (i) the fact that white labelling does not appear to be systematically captured in supervisory onsite and off-site activities, including discussions about business models; (ii) the limited amount of data available to NCAs in 'host' Member States via supervisory notifications, which do not expressly capture the business model used for any cross-border provision of services; and (iii) the variety of products and services offered via white labelling and the limited availability of data in view of the confidential nature of such agreements, which impaired the visibility over the prevalence and nature of the arrangements. As such, the analysis set out in this report is mostly qualitative in nature.

3. White labelling landscape in the EU

6. White labelling as a business model appears to be widely used, both in terms of number and types of entities involved[7]. While traditionally linked to the distribution of banking products (a practice that continues, with 35% of banks responding to the 2025 Spring RAQ engaging in white labelling), white labelling is now being used for the distribution of a broadening range of financial products and services[8], including e-money and payment services. It is anticipated that white labelling may also be used increasingly in the crypto-asset sector.

White labelling business model gaining popularity

7. The 2024 survey shows a large majority of respondent (18 of 23) NCAs reporting that financial institutions established in their jurisdictions are providers in the context of service provision to customers in their 'home' Member State. Moreover, 11 NCAs indicated that the service provision may also extend to customers situated in a different jurisdiction, thus evidencing the cross-border dimension of the business model. NCAs referred typically to traditional financial products and services, but several also highlighted that the model may be used for more novel types of product and service (see Text box: White labelling of crypto-asset services and issuances of so-called stablecoins as a service).

Text box: White labelling of crypto-asset services and issuance of so-called stablecoins-as-a-service

The provision of crypto-asset services, including custody of crypto assets, and issuance of so-called stablecoins are relatively new activities which, in the EU, are regulated pursuant to the Regulation on Markets in Crypto-Assets (Regulation 2023/1114, so-called MiCA Regulation)[9].

Many issuers seek to offer their so-called stablecoins directly to customers. However, some may issue stablecoins for branding and use across a third party's ecosystem. This is known as issuing stablecoins-as-a-service. One such example can be observed in the US. There, PayPal (a licensed provider of money transfer services in the US) has partnered with Paxos (an issuer) for a stablecoin (PYUSD) that can be used on PayPal's infrastructure[10].

This model may be increasingly observed where traditional financial institutions seek to integrate new blockchain-based units of exchange/payment, but do not wish to directly issue the units themselves, or when entities wish to integrate a crypto service offering without applying for a MiCA license.

[7] See also FSI, A two-sided affair: banks and tech firms in banking, October 2024.
[8] See Joint-ESA Report on 2023 stocktaking of BigTech direct financial services provision, February 2024.
[9] MiCA regulates the offering to the public/admission to trading of so-called stablecoins in the form of 'electronic money tokens' and 'asset-referenced tokens' as well as the offering to the public/admission to trading of other types of crypto-assets, and the provision of crypto-asset services such as custodian wallet provision, and the operation of trading platforms/exchanges.
[10] See https://www.paxos.com/pyusd.

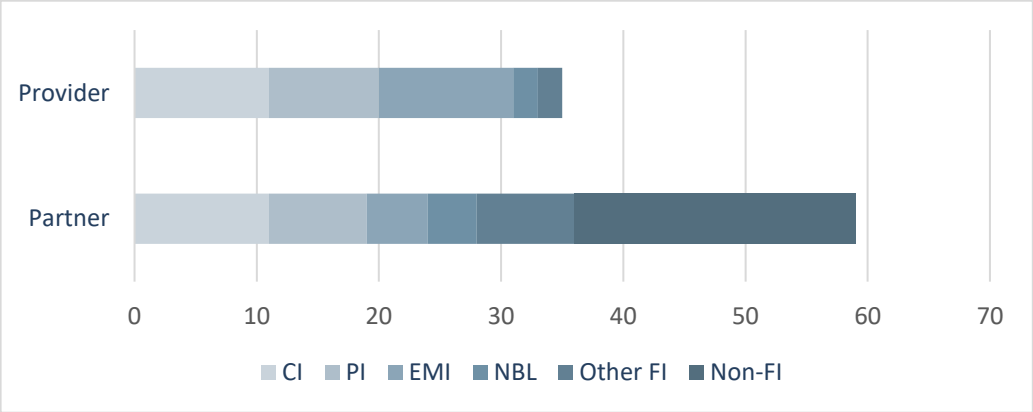
Key features of white labelling

8. In practice, white labelling may involve different arrangements that may vary depending on 7 key features: (a) the regulatory status of the provider and partner; (b) the 'core' or 'ancillary' nature of white labelling as a distribution model; (c) the financial product or service distributed via white labelling; (d) the target customer; (e) the geographic footprint; (f) roles of the provider and partner; and (g) the fee model.

A. Regulatory status of the provider and partner

9. The responses to the 2024 survey reveal a diverse landscape of entities involved in white labelling across the EU. Credit institutions and e-money institutions represent the prominent type of provider[11], followed by payment institutions. As to the partner, NCAs reported that, in some cases, the partner may be an authorised financial institution, such as a credit institution, payment institution, or non-bank lender, or may be unauthorised (see Figure 1 for an overview of the type of the most common entities acting as providers and partners as indicated by NCAs[12]). While the role of partner was traditionally confined to authorised financial institutions, the emergence of non-financial entities acting as partners marks a significant shift in the market, which may be driven by the rapid growth in the use of digital platforms to 'bridge' consumers with financial institutions[13].

Figure 1. Types of providers/partners reported by the NCA in the provider's Home Member State



[11] 12 NCAs indicated credit institutions and e-money institutions established in their jurisdictions operate as white label providers.

[12] As part of the 2024 survey, NCAs were asked to indicate the types of entities established in their jurisdiction that acted as providers and the combination of types of entities they were entering into agreements with as partners in their jurisdiction. NCAs were not expected to report the number of providers and partners active in their jurisdiction, but just to give an indication of the most common combinations of providers and partners engaged in white labelling. In total, 15 NCAs indicated at least one type of financial institution entering into white labelling agreements with non-financial partners.

[13] See EBA Report on the use of digital platforms, September 2021.

10. According to the 2025 Spring RAQ, fewer than 5% of the respondent credit institutions are entering into white labelling agreements with BigTechs[14], i.e. large technology companies with extensive customer networks, including firms with core businesses in social media, internet search, software, online retail and telecoms (see Text box: BigTechs). This result shows a decrease compared to the 2024 Spring RAQ, when 10% of the respondent credit institutions reported white labelling agreements with BigTechs. This decrease could be explained by the fact that the earlier RAQ results may have captured more cases at the pilot stage and thus were not reported in 2025 following the completion of the pilot.

Text box: BigTechs

White labelling presents an opportunity for BigTechs to embed financial services into their customer-facing product offerings without themselves seeking the authorisation to carry out those financial services[1]. Opportunities may also arise for financial institutions as BigTechs benefit from large customer bases and can leverage network effects to distribution products and services to customers beyond financial institutions' traditional client bases. However, when negotiating white labelling agreements with BigTechs, financial institutions, especially smaller ones, may find themselves at a disadvantage due to imbalances in bargaining power. In addition, BigTechs' vast data resources, large customer bases, and expertise in advanced analytics and Artificial Intelligence, paired with their deeper understanding of consumer preferences, may amplify over time data asymmetries between the provider and the partner. In addition, BigTechs' tendency to frequently make changes to their interface may lead to operational risks for providers. Therefore, financial institutions should be mindful of potential risks, and address ex ante *– as well as on ongoing basis – any implications regarding compliance with their own supervisory obligations.*

B. Core or ancillary nature of white labelling as a distribution model

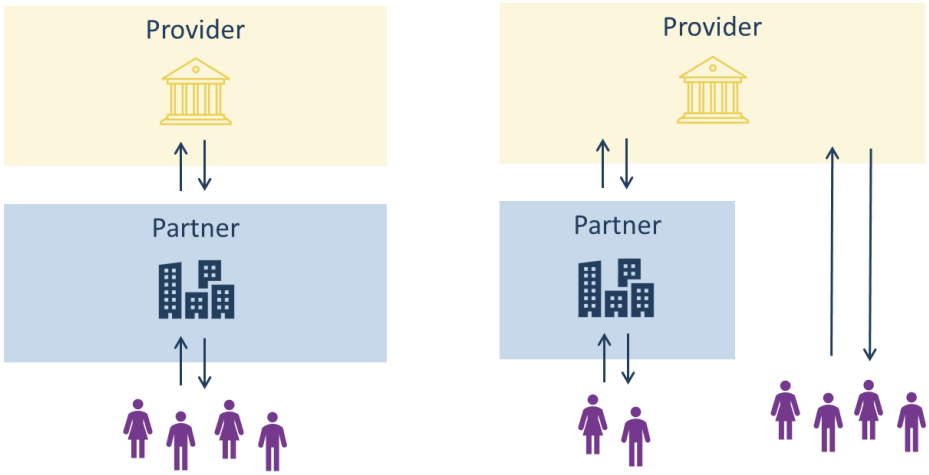
11. The 2024 survey and the 2025 workshop highlighted that white labelling may form a core or an ancillary part of the business models of the provider and partner[15]. For the provider, white labelling as a core activity means that the provision of services for white labelling is the only or dominant activity and, as such, the provider mainly depends on partners to attract customers and increase its business volume. When white labelling represents an ancillary part of the business model, the provider distributes financial products and services under its own brand as well as via white labelling, meaning that the provider has more than one distribution model for its products and services (see a visual description in Figure 2 below).

[14] See Joint-ESA Report on 2023 stocktaking of BigTech direct financial services provision, February 2024. This definition is consistent with the approach of the Financial Stability Board (BigTech firms in finance in emerging market and developing economies).

[15] In both cases, a third party, i.e. a pure technical provider, may be facilitating the partner's access to the back-end infrastructure of the provider. Said access is generally granted via an Application Programming Interface (API), i.e. a set of routines, protocols and tools for building software applications.

12. For partners, the white labelled product or service may be a core part of their customer-facing product/service offering, or may be one of many products or services offered by the partner. These other products or services may be financial or may be non-financial (this might be the case, for instance, in the context of partner operated 'marketplaces', see Text box: Marketplaces).

Figure 2. Visual representation of white labelling as core function (left side) and white labelling as ancillary service (right side)



13. Where the partner is authorised to carry out financial services, the white labelled product or service may be complementary to other financial services provided directly by the partner. For example, the partner may choose to enter into a white labelling arrangement to facilitate the offering of additional or more novel financial products and services, or to ensure the provision of very complex end-to-end services (e.g., in the payments sector).

Text box: Marketplaces

E-commerce platforms that act as intermediaries between merchants and customers are commonly known as marketplaces and are subject to the PSD2[16] in so far as they offer payment services. As an alternative to obtaining a PSD2 license, marketplaces may enter into agreements with payment service providers (the providers) to leverage their acquiring services[17] and execute payment transactions seamlessly and efficiently without the need for the marketplace itself to be authorised under PSD2. In such agreements, the provider processes payments, executes transactions, and is responsible for controlling the funds, thus ensuring that merchants' funds are handled separately from any marketplace fees and avoiding the risk of commingling funds, as prescribed by PSD2. Depending on how the payment services are offered and branded to merchants and customers, the agreement may constitute white labelling.

This enables marketplaces to focus on their core function: connecting merchants and customers in a secure and efficient manner. Marketplaces also offer a convenient online channel for

[16] Pursuant to Recital 11 of Directive (EU) 2015/2366 (the second Payment Services Directive), e-commerce platforms should be excluded from the scope of the PSD2 only when acting on behalf of either the payer and the payee; or, if they act on behalf of both, if the marketplace never enters into possession or control of client funds.

[17] These are payment services that allow the merchant to accept and process card payments from customers.

merchants to sell their goods without requiring them to develop their own payment gateways, significantly reducing barriers to entry for businesses looking to sell online.

A crucial aspect is the definition of responsibilities for the onboarding of merchants and the compliance with customer due diligence (CDD) requirements. While the specific implementation of this process varies greatly, it typically involves the merchant signing an agreement with the marketplace that incorporates terms and conditions of the payment institution, including clarifications regarding the allocation of responsibilities to ensure compliance with the AML/CFT requirements.

In combination with acquiring services, providers can also offer additional services, such as vendor pay-out, BNPL, transaction reconciliation, refunds and back-office services.

C. Types of products and services offered via white labelling

14. Based on the specific use cases reported by NCAs via the 2024 survey, the EBA has identified three core clusters of common financial products and services offered via white labelling: (i) account and payment services; (ii) credit provisioning (BNPL, and SME and corporate credit); and (iii) open banking services. Table A below further describes the use cases, the authorisation status of providers and partners, and the nature of the business model.

Table A. Core clusters of financial products and services offered via white labelling

	Account and payment services	Credit provisioning	Open banking
Use cases	(i) Payments, e-money and deposit account; (ii) card issuance; and (iii) acquiring services	(i) BNPL and consumer credit; (ii) SME and corporate credit	(i) API-aggregation services; (ii) account information and data enrichment services
Provider's status	Mostly credit institutions and e-money institutions	Mostly credit institutions	Account Information Service Providers and Payment Account Service Providers
Partner's status	Both financial and non-financial institutions (e.g. telcos, retail and software companies)	Mostly non-financial institutions (often tech companies)	Both financial and non-financial institutions
Nature of the distribution model	Depending on the individual provider	Generally ancillary nature	Generally core nature

D. Type of target customer

15. The target customer may vary depending on the concrete use case. In general, the 2024 survey results show that a large majority of products and services (such as deposit accounts, BNPL credit, card issuance, e-money and payment services, as well as account information services) are offered via white labelling to consumers and SMEs, while acquiring services, API-aggregation and data enrichment services, are mainly directed to SMEs and corporates.

E. Geographic distribution (Home Member State, cross-border)

16. Although white labelling is often used to distribute products and services in the same jurisdiction as the one in which the provider is established (i.e. the 'home' Member State), the results of the 2024 survey and the 2025 workshop identify that white labelling is being used increasingly to provide services cross-border (i.e. into 'host' Member States)[18]. One core rationale is that the provider may have no, or very limited, presence and/or brand visibility in a 'host Member State'. By leveraging the distribution channels/brand of a partner active in another Member State, it may be easier for the provider to expand its products/services into that market than building out its own infrastructure/embarking on costly advertising.

F. Roles of the provider and partner

17. In the context of a white labelling arrangement, providers and partners may perform a wide variety of tasks, which may also vary depending on their regulatory status and the specific use case.

18. In principle, providers, as the entity with whom the customer is ultimately contracting, bear the ultimate responsibility for regulatory compliance. As such, they typically carry out the AML/CFT checks (sometimes relying on preliminary screenings performed by partners, see Annex II for more details), receive and control customer funds, operate the 'back office' infrastructure for the purposes of important compliance functions such as record keeping and regulatory reporting, and ultimately handle customer complaints. Providers may also supply to the partner (to use at the 'front office' stage) documentation or information (e.g. regarding 'key facts') relating to the products and services. Moreover, during the 2025 workshop, participants indicated that providers typically perform *ex ante* checks on prospective partners (see Text box: Assessment of the ML/TF risks stemming from partners).

Text box: Assessment of the ML/TF risks stemming from partners

Pursuant to Article 8 of the AMLD, obliged entities need to identify and assess the ML/TF risks including those linked with distribution channels. For that purpose, the provider should obtain information and perform appropriate ex ante checks on partners. Where the ML/TF risk associated with the partner is increased, the provider should perform additional scrutiny and checks on the partner. These usually include, for instance, an analysis of the business, and of the individuals involved in its ownership. Participants in the 2025 workshop highlighted that providers may face challenges in obtaining additional information on prospective partners and in assessing the robustness of their business models. In such cases, providers may choose not to proceed with a white label arrangement with that entity.

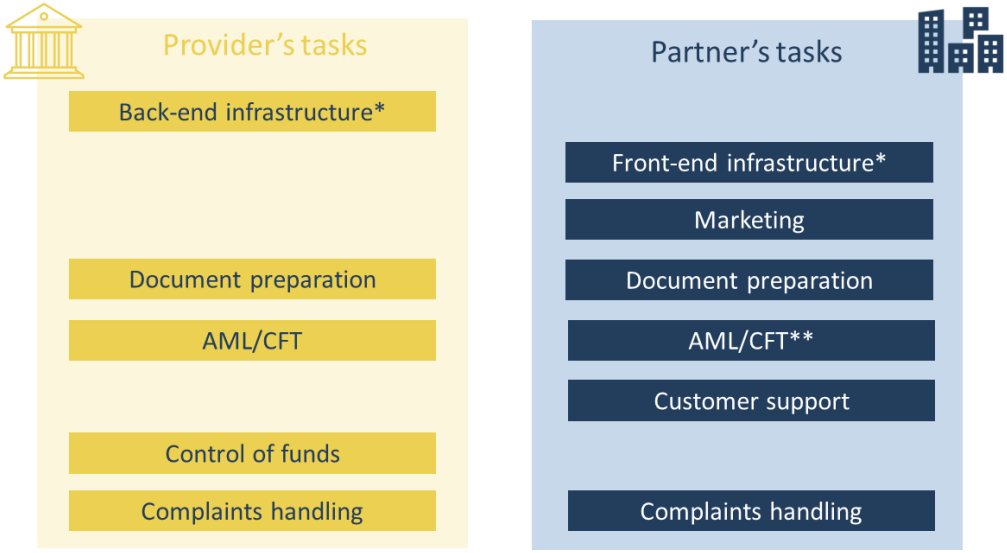
19. Partners may also perform a wide variety of tasks, typically 'front office' including operating the customer-facing infrastructure (e.g. a digital platform), collecting the information necessary for

[18] A total of 11 NCAs reported financial institutions established in their jurisdictions (i.e. as home Member State) offering products and services via white labelling to customers in other jurisdictions (host Member States). Conversely, 9 NCAs in host Member States observed financial institutions established in other jurisdictions providing products and services through white labelling to customers in their own territory.

onboarding customers, and complaints handling (albeit in most cases partners may refer complaints about retail banking products and services directly to the provider, partners may have to handle complaints concerning dissatisfaction of wrongdoings related to their activities). Notably, partners often perform a key role in the marketing of products and services, and disclosing the terms and conditions of products in customer-facing communications.

20. Based on the 2024 survey and 2025 workshop, Figure 3 summarises, to the extent possible, the tasks which are generally performed by providers and partners[19].

Figure 3. Tasks generally performed by, respectively, the provider and the partner



21. As such, in practice, the arrangements put in place between the white label provider and partner may involve a dependency on the other party. From a regulatory and supervisory perspective, white labelling arrangements may constitute 'third party dependencies'. The outcome of the 2024 survey and the 2025 workshop suggested that the same white labelling arrangement may be qualified differently in different Member States (for a discussion of the issues and some illustrative examples see Annex I: third party dependencies). Therefore, in case of cross-border offerings, there is a risk that providers and partners may have to implement multiple different compliance processes/operating models to conform to the different expectations from supervisors in different Member States, resulting in additional costs to business.

* This can also include maintenance and other back-end/front-end services.

** AML/CFT also includes customer onboarding, KYC/CDD, sanction screening, ongoing customer monitoring, etc. If the partner is an AML/CFT obliged entity, according to participants to the 2025 workshop, providers always perform the AML/CFT checks, but depending on the regulatory status of the partner, providers may rely on the information collected by the partner in line with Article 25 of the AMLD. See also Annex II.

[19] If the partner is an AML/CFT obliged entity, according to participants to the 2025 workshop, providers always perform the AML/CFT checks, but depending on the regulatory status of the partner, providers may rely on the information collected by the partner in line with Article 25 of the AMLD.

G. Fee model

22. The 2024 survey and 2025 workshop exposed that the fees charged by providers depend on the precise nature of the white labelling arrangement. However, generally, flat fees (e.g. set-up fees, and recurring fees) are imposed by providers on partners and, in connection with the service offered, additional per-use fees (e.g. fees per-transaction, fees per-API call, commissions on volumes, etc)[20] are also charged.

23. Partners can profit from expanding the products and services offered to customers and may charge fees to providers or to customers. For example, partners may charge to providers broker fees or fees to grant access to their platform or marketplace; partners may charge customers a fee to access the interface/platform, in addition to the fees for the specific service/product offered.

4. Potential opportunities

Opportunities for providers, partners and customers

24. When assessing potential opportunities for providers, partners and customers, the EBA has identified some that can bring benefits to all parties (see Annex III for the summary of the potential opportunities and risks per stakeholder type). These are:

a. **Cost efficiency**: providers can grow their market presence without expensive marketing campaigns by leveraging on partners' brand visibility and marketing. In addition, providers can optimise their overall costs by using a partner's front-office infrastructure for customer day-to-day interfaces, and customer relationship management, as well as certain AML/CFT tasks (depending on the qualification of the relationship between partner and provider). On the other hand, partners may achieve substantial cost savings by leveraging the license of the provider (thus avoiding costs relating to license applications and ongoing costs of compliance linked to that licence). Moreover, as partners may utilise the 'back office' infrastructure built and managed by the provider, they can avoid building their own IT systems from scratch while focussing on the customer-facing infrastructure (e.g. a digital platform) to distribute a broader product and service range. These cost savings may ultimately translate into more competitive pricing for customers.

b. **Expanded offer**: providers can offer their products and services via additional channels (e.g. digitally, in store, etc), thereby enhancing their market presence, while partners can broaden their offerings and provide a comprehensive range of financial products and services without

[20] It should be noted that some white labelling agreements involve a third party, i.e. a non-bank pure technical provider that offers back-office solutions, such as software development, data storage, APIs to connect the partner to the provider's infrastructure. In such cases, the technical provider also charges fees for the provision of its services.

necessarily holding the relevant license. In turn, this benefits customers who can access a wider range of products and services, potentially making financial services more accessible and convenient and reducing geographical disparities. Moreover, providers may use white labelling to develop and test the roll-out of innovative products, or enter new markets via selected partners.

c. **Better targeting of products and services to customers**: the provider may leverage the partner's customer database to better target and/or customise products and services to customers, ultimately ensuring access to personalised products and services.

d. **Increased customer base**: both providers and partners can reach new customers. The interface deployed by the partner can offer new opportunities to customers, including improved accessibility, convenience, and overall enhanced customer experience.

e. Finally, the integration of **new technologies and platforms** developed by partners can bring benefits when providers (due to reasons of legacy IT systems and/or cost) have constrained capacity to develop alternative solutions. This can enable more traditional providers to accelerate their digital transformation, moving away from legacy systems and embracing more efficient, scalable solutions from third parties. The use of advanced platforms can facilitate the provision of personalised financial products and services, enhancing customer engagement and satisfaction.

25. White labelling may also contribute to **enhancing financial inclusion** by improving the access to financial products and services for consumers in vulnerable circumstances, such as consumers excluded from traditional financial systems due to geographic or technological constraints (e.g. underserved consumers in rural areas where traditional financial institutions have no or limited physical presence). Providers may leverage on the infrastructure offered by the partner to offer user-friendly and more accessible (and potentially more affordable) financial products.

26. White labelling may also support the creation of **new revenue streams**: in addition to any revenue on the specific product or service (e.g. interest paid on a loan, fee for issuing a card, etc) both providers and partners can charge fees for the provision of their specific services and/or infrastructures. In addition, partners can profit from their own offering of financial products and services.

Text box: The potential impact of FIDAR on white labelling

The introduction of the proposal (as at the date of the publication of this report, under negotiation) for a Framework for Financial Data Access[21] (so-called FIDAR) has the potential to support the growth and scalability of white labelling by improving standardisation and fostering secure and reliable data sharing models across a broader range of products and services than the 'open banking' facilitated by PSD2. In addition, FIDAR introduces the concept of Financial Information Service Providers (FISPs), i.e. firms authorised to access certain customer data and provide financial information services, which, in the future, could act as white label providers.

[21] See the legislative proposal for a Framework for Financial Data Access.

FIDAR aims to enhance data accessibility and interoperability, which can streamline the integration of white label services across borders. By providing a standardised framework for data sharing, FIDAR can foster the distribution of white-labelled financial products and services, as it would make it easier for providers and partners to operate in multiple jurisdictions. Standardisation, paired with increased data transparency and accessibility, can also foster innovation, allowing partners to develop more tailored and efficient financial products and services. Additionally, the emphasis on data protection and security can help mitigate some of the risks associated with cross-border data transfers, thereby enhancing consumer trust and confidence in white-labelled financial products.

Other opportunities

27. Finally, white labelling has the potential to **foster competition**. The ability to benefit from the provider's licence reduces set up costs for partners thereby reducing entry barriers. As such, partners can test and grow their business model in a real market setting without seeking a license upfront[22]. By leveraging their own brand and platform to distribute financial products and services, partners can serve a broader range of customers (as compared to the customer base of the provider) without increasing operating costs. In turn, white labelling also plays a role towards a more dynamic and competitive market environment by facilitating customer access to a wider range of products and services at more competitive prices (e.g. lower fees) against a context of customers' prioritising simplicity and ease of access to financial services.

5. Potential challenges and risks

28. The involvement of multiple entities in the distribution of financial products and services via white labelling may fragment the value chain and create complex business models with potentially increased challenges and risks. For consumers, the main concern is generally represented by the lack of transparency regarding the roles and responsibilities of the different entities involved, which can lead to consumers facing difficulties in making complaints and seeking redress should things go wrong. Risks stemming from inadequate or misleading disclosures to customers and mis-selling practices may also be observed. For providers and partners, the primary concerns revolve around business model risk, regulatory compliance, operational, counterparty and reputational risks, and the management of customer relationships. Finally, for supervisors the main challenges revolve around the potential opacity of white labelling agreements, challenges in qualifying the arrangements from a regulatory perspective (outsourcing, agency, etc) and, potentially, a lack of direct supervision over partners.

Challenges and risks for consumers

[22] Sometimes, when the offering is successful, partners may choose to evolve their business model and acquire their own licence.

29. For consumers, as identified in the responses to the 2024 survey (see Figure 4, laying down potential risks for consumers as reported by NCAs) and during the 2025 workshop, white labelling can lead to:

    a. increased risks of **misleading/insufficient information and mis-selling practices,** which might occur due to:

        i. **lack of transparency about the roles and accountability** of providers and partners. With the involvement of multiple entities, consumers may struggle to correctly identify (i) the existence of the white labelling agreement[23]; (ii) the identity of the entity/entities with whom they are contracting; (iii) the licensing status of the provider and partner[24]; and (iv) the allocation of responsibilities between provider and partner. For example, the business model is not necessarily made clear on the partner's digital platform or in the contractual agreement, or customers are required to navigate multiple sets of terms and conditions for each service;

        ii. **the opacity of the cost structure or of the product/services features**, as consumers may receive inaccurate, incomplete, or contradictory information and the terms and conditions applicable might not be clear enough or even differ according to each service, which increases the complexity for consumers; and

        iii. **the setting in which products and services may be sold**, as these may be placed alongside other of the partner's products offered and may look attractive for the consumer, but may not be suitable taking into account the consumer's needs.

    b. risks of **fraudulent activities**, including the risk of being manipulated into making a payment to the fraudster that is impersonating the partner or the provider or pretend to be working with them[25]; sometimes fraudsters leverage (virtual) IBANs to impersonate others. A risk of fraud might arise due to the lack of transparency and consumers understanding of the roles and allocation of responsibilities between providers and partners. Weaknesses in partner CDD practices, and absent sufficient oversight by the provider, may also increase fraud risks. In cases of fraud, and especially when the allocation of responsibilities between provider and partner is not clear, consumers may not know which party should be liable[26];

[23] From the end customer's perspective, the information might not always appear sufficiently clearly in pre-contractual information (e.g. through the marketing material or the partner's website), or in the terms and conditions/contractual agreement. NCAs and consumer organisations reported that, in some circumstances, the customer may receive no clear information on the provider.

[24] Partners sometimes display the license of the providers on their websites, misleading consumers into believing they are directly interacting with a regulated financial entity.

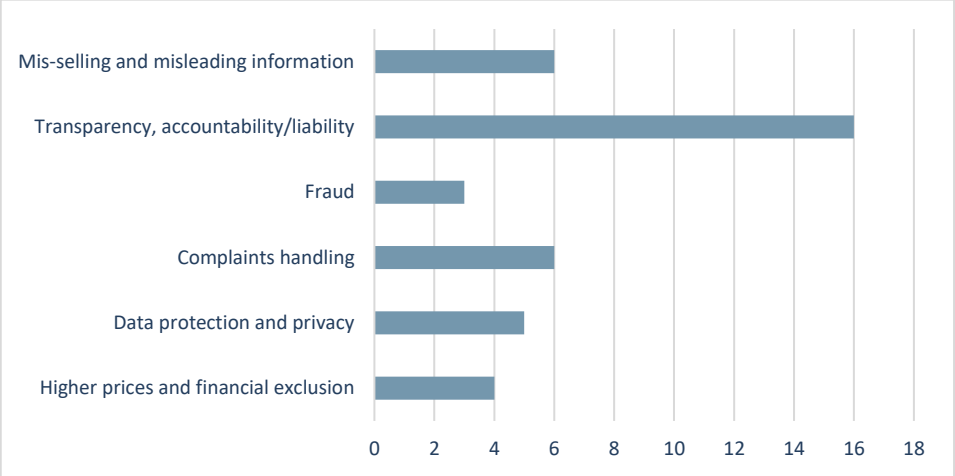
[25] Payment fraud is still the most significant issue for EU consumers as a result of new types of fraud such as "Authorised Push Payment" (APP) fraud, where the payer is manipulated into making a payment to the fraudster, see the EBA Consumer Trends Report 2024-2025.

[26] For example, a consumer falls victim to a phishing scam while using a white-labelled banking app that looks like it is owned by a popular ride-booking app. Although the app is branded with the ride service's name, the actual banking services are provided by a separate financial institution. When such fraud occurs, the consumer does not know who to contact or who is responsible—the ride app or the bank.

moreover, the consequences of the fraudulent activity may not be appropriately/timely managed, causing detriments to consumers.

c. challenges in **complaints handling**: consumers may face difficulties in identifying the relevant entity to whom a complaint should be addressed. For instance, if a Payment Service Provider relies on the partner to monitor transactions and a fraudulent transaction occurs, the consumer might not know whom to contact if their payment transaction is unduly blocked. While some partners have invested in streamlined procedures that prioritise quick dispute resolutions, others may lack the experience and knowledge to effectively support consumers and handle complaints. Complaints handling issues may be exacerbated in cases where the provider and the partner are located in different Member States.

Figure 4. Potential risks for consumers as reported by the 23 NCAs responding to the 2024 survey



30. Beyond consumer protection, **data protection and data privacy** concerns might arise regarding how consumer data is stored, shared, and protected by the provider and partner. Since providers and partners are sharing data with each other, the risk of data misuse, data breaches and unauthorised access to consumers personal data could increase due to the access by multiple entities. Moreover, the partner or the provider may have an incentive to use the personal data for other business purposes. In accordance with the General Data Protection Regulation (GDPR)[27], consent of the data subject must be obtained ahead of the processing of personal data and this consent must cover all purposes to which data may be processed. Moreover, some NCAs responding to the 2024 survey, underscored the importance of providers and partners providing published policies to ensure transparency about how they use and protect consumer data, including how they manage the risk of data loss or violations of data protection and consumer's rights.

31. Finally, during the 2025 workshop consumer organisations reported that white labelling can lead to **financial exclusion** of certain consumers. For instance, when white labelled services are delivered through digital platforms (e.g. mobile apps or websites), elderly consumers who are

[27] Regulation (EU) 2016/679.

not digitally savvy might be financially excluded, as they may not be able to access or navigate a digital interface (see also the Text box: Consumer financial education/literacy). Consumer representatives however explained that full compliance with regulations like the EU Accessibility Act[28] might contribute to ensuring white labelling arrangements do not exclude specific groups of consumers.

Text box: Consumer financial education/literacy

A higher level of digital and financial literacy would help consumers make effective use of financial services distributed via digital channels, including via white labelling, and make effective and responsible choices, identify and report suspicious products and service providers, increase their welfare, efficiently enforce their rights, and have confidence and trust in the digital financial system.

In this light, further actions at the national level could improve financial literacy of consumers, for example, by enhancing their understanding of opportunities, challenges and potential risks linked to financial innovation, in particular regarding the use of 'seamless' online financial services, including via multi-purpose platforms, and cybersecurity issues. Raising awareness of the risks that consumers may face when choosing online or mobile banking services should be further encouraged on a regular basis. Consideration should be also given to the existing OECD core competencies for adults and for youth[29] *and the ongoing work of the European Commission and the OECD International Network on Financial Education, which jointly developed a financial competence framework for the EU[30].*

Challenges and risks for providers and partners

32. The fragmentation of the value chain may also increase challenges and risks for providers and partners, as identified in the responses to the 2024 survey and during the 2025 workshop. Notably, white labelling has the potential to:

    a. Increase the **business model risk** for both providers and partners. For example, providers whose core activity comprises white labelling may become very dependent on partners, with consequences on the sustainability of their business model in the longer term should partners choose to exit the market, switch provider, substantially raise fees or provide directly the product or service. Similarly, partners may also face business model risks should a financial service become unavailable, for instance in case of a provider discontinuing a product offering, or in the event of the provider's failure or license withdrawal. These risks may increase further in case the provider is offering services to multiple partners. Negative consequences may also affect customers, especially in absence of adequate exit plans.

    b. Increase the **operational risk** for both providers and partners, as the complexity of the value chain can reduce transparency and create operational vulnerabilities. For example, the management of ICT infrastructure connections with multiple partners can be operationally challenging for providers. In addition, the possibility to use third-party interfaces and APIs

[28] Directive (EU) 2019/882.
[29] See Financial education | OECD.
[30] See Financial competence framework for adults in the European Union.

may result in adding multiple layers between the provider and the customer and increasing the risk of technical failures. Providers may also have insufficient control over partners' behaviour (e.g. marketing, distribution and sales strategies), which could lead them to face liability for failures attributable to partners but ultimately resulting in compliance/wider liabilities for providers. On the other hand, white labelling can expose partners to service disruptions and operational failures, with limited control over mitigating measures.

c. Have negative consequences in terms of **reputational risks**, which in turn can lead to a loss of customer trust and confidence. Both providers and partners can be indirectly affected by any failure, misconduct or poor practice carried out by the other party, as any incident or negative media report has the potential to negatively affect both parties[31]. In severe circumstances, the provider (or the partner, when it is a financial entity) may need to 'step-in' to support the other due to the risk faced (see Text box: 'Step-in' risk).

d. Result, in certain instances, in a **lack of direct customer relationship** for providers, with potential adverse effects in terms of: (i) not having the necessary information to effectively perform compliance tasks (e.g., credit worthiness assessment, customer onboarding, transaction monitoring); (ii) not having enough information to assess the suitability and appropriateness of the financial product(s) for the specific customer; and (iii) potentially losing the end-customer in case the white labelling agreement with the partner is terminated.

Text box: 'Step in' risk

'Step-in' involves a situation in which a financial institution, such as a credit institution, has to 'step-in' and provide financial support to an entity outside its group due to reputational or operational considerations. For example, during the Great Financial Crisis of 2008-2010, several banks had to provide such financial support (e.g. credit provision or liquidity) to funds to whom they had referred clients, due to reputational considerations. Similar forms of financial support were also provided to securitisation vehicles.

Post-crisis banks are subject to specific regulatory requirements to identify ex ante any potential step-in risks to ensure that these potential liabilities are properly taken into account in assessing the capital requirements of the bank[32]. However, other types of financial institution are not subject to such requirements, meaning any potential step-in risks, including from white labelling, are not systematically accounted for in the quantification of own funds.

Regulatory and compliance risks

33. Providers may face challenges in **securing adequate conformity with the relevant regulatory requirements**, including with the need to proactively ensure partners have a clear

[31] For instance, customers may run on the funds held by the provider in case of failures attributable to the partner or in case of issue in relation to other products and services offered by the partner. Negative consequences may then extend to other customers of the provider and to other partners.

[32] See BCBS guidelines on the identification and management of step-in risk (2017).

understanding of permissible activities and the relevant measures to take[33]. This may be more challenging when the partner is not a financial institution and/or when the provider distributes different products and services through multiple partners. Providers should make sure that partners successfully integrate these into their operating models, to ensure the provider can still demonstrate across the distribution model compliance with the requirements to which it is subject. For example, the provider will need to ensure any consumer-facing communications about financial products and services distributed by the partner conform to the regulatory expectations in the jurisdictions in which the products are being distributed. Similarly, providers may use partners for the performance of certain compliance tasks, such as identification and verification during customer onboarding (see also Annex II), but remain responsible for AML/CFT compliance.

34. The involvement of multiple parties, often established in different jurisdictions, results in the fragmentation of data and procedures, thereby increasing **compliance risk**, including with prudential requirements where applicable. Additionally, the dispersion of tasks between partner and provider can create gaps in compliance, leading to inconsistencies in risk assessment and reporting obligations. This structural challenge may increase the risk of financial crime, requiring service providers to implement robust oversight mechanisms to mitigate exposure and AML/CFT breaches. Moreover, providers and partners may encounter challenges in assessing whether the arrangement includes elements of outsourcing, agency and/or third-party reliance, particularly in cases where there is a cross-border element, and in cases where requirements are not fully harmonized in EU law (see Annex I).

35. Additional challenges may emerge due to **differences in national identification and verification requirements or other AML/CFT requirements**, which can create a complex compliance landscape for providers offering financial products and services cross-border. Additionally, partners and providers may have different ways to conduct risk assessments potentially resulting in different outcomes. The Anti-Money Laundering Regulation (AMLR)[34] introduces directly applicable and harmonised CDD rules across the EU, which should enhance regulatory clarity, operational efficiency, and supervisory convergence, ultimately strengthening the EU's overall AML/CFT framework.

36. Challenges may also arise in **accessing CDD data**: where CDD processes are assured by the partner, the provider has to be sure it has access to the information obtained by the partner so that the provider can meet its AML/CFT obligations. However, under outsourcing or reliance agreements, the provider may not have direct access to such information (e.g. KYC records, transaction data, monitoring results) because the underlying systems and processes were not designed to facilitate seamless data sharing between the partner and the provider. This presents a significant compliance risk as failure to establish appropriate data access arrangements or mechanisms may result in a breach of AML/CFT obligations. System upgrades to enable

[33] It should be noted that the use of white labelling of certain products and services may be limited or precluded by law in certain Member States.
[34] Regulation (EU) 2024/1624.

structured, secure, and privacy-compliant data sharing between providers and partners could reduce operational friction and mitigate regulatory risk.

Supervisory and system wide risks

37. As evidenced by the responses to the 2024 survey[35], the complexity introduced by white labelling, coupled with emerging trends such as digitisation and platformisation, can exacerbate challenges faced by supervisors in monitoring compliance at all points of the value chain. According to NCAs, the main challenges are represented by:

    a. The **opacity of the structure**, especially with regards to the relationship between providers and partners and their respective roles (including which tasks are carried out by the partner). The opacity is further exacerbated as these agreements often go unreported, as commercial partnerships, including white labelling, typically do not need to be notified to the NCAs, unless the partner can be qualified as agent under the PSD2, or the arrangement constitutes a material part of, or change to, the business model. Therefore, supervisors may not have visibility of how regulated services are delivered to end users, particularly when these services are bundled with non-regulated offerings or when services are offered cross-border.

    b. **Regulatory qualification of the arrangements and supervisory fragmentation**, due to potentially different visibility over, and regulatory qualification of, different parts of the distribution arrangement (e.g. as outsourcing and/or agency – see Annex I) and resulting supervisory expectations. This can pose particular challenges: to providers and partners, in terms of possible varying application of the regulatory framework across different Member States; and to supervisors, especially as regards white labelling arrangements on a cross-border basis, as they may not be aware of the offer of services/products via white labelling in their jurisdiction (see Text box: Home/Host notifications). In addition, the complexity of the agreement may increase the difficulty to supervise the different entities involved, especially when the partner has multiple agreements with different providers for the offer of different services and products. In such cases, different supervisors may be in charge, especially if the obliged entities are established in different countries.

    c. The **lack of direct supervision over partners**, especially when they are un-registered or un-authorised entities, or when they are located in a different jurisdiction. In the latter case, NCAs may be unaware that a licensed financial institution is offering services in their jurisdiction via white labelling and therefore might not have the opportunity to communicate with the competent authority in the home Member State regarding the arrangement and any applicable requirements under domestic frameworks, for instance relating to conduct of business considerations (see the Text box: Home/Host notifications).

[35] 16 NCAs and the ECB have observed supervisory issues or challenges arising from white labelling.

Text box: Home/Host notifications

When carrying out financial services activities, providers[36] can leverage their right to passport their services cross-border. Under EU law[37], the intention to provide financial services on this basis has to be notified to the 'home' NCA and then transmitted by that authority to the 'host' NCA. However, such notifications to host authorities can be unreliable as the initial notification to the home NCA may be completed on a generic basis (e.g. reporting a potential intent to carry out services in all Member States 'to be on the safe side', rather than in specific Member States)[38]. This issue, rather than limited to white labelling, is more widely observed across the financial sector. The unreliability of notifications can create challenges for home and host NCAs in terms of monitoring financial activities and ensuring compliance with the applicable requirements, particularly on conduct of business issues that varies across jurisdictions. Visibility over white labelling agreements could be even more challenging in cases of 'triangular passporting', i.e. cases where a provider authorised in a Member State A uses a partner located in a Member State B to provide financial services in a Member State C. In such cases, the notification should be sent by the 'home' NCA (Member State A) to the 'host' NCA (Member state C)[39].

38. To facilitate the identification and understanding of white labelling agreements and the concrete allocation of tasks between providers and partners, NCAs could use, on a voluntary basis, in the context of line supervision, a common template questionnaire developed by the EBA[40].

39. Responses to the 2024 survey suggest that white labelling may affect supervisors' ability to effectively monitor and assess potential risks, including those related to ML/TF (see Text box: ML/TF risks analysis), especially if the white labelling agreement does **not clearly define the tasks delegated to the partner**. For instance, if the partner is a regulated entity subject to its own AML/CFT obligation, the white labelling agreement does not always make clear whether the relationship is based on outsourcing (Article 29 AMLD) or third party reliance (Article 25 to 28 AMLD).

40. To mitigate these risks, it is essential to establish clear contractual agreements, well-defined compliance frameworks, and robust supervisory oversight to ensure that AML/CFT obligations are properly allocated and enforced. Indeed, the EBA underscores that all obliged entities shall have in place internal policies, procedures and controls in order to ensure compliance with

[36] And partners, if they are EU-regulated entities.
[37] For credit institutions, see Article 39 of the CRD; for payment institutions, see Article 28 of the PSD2, which also applies to e-money institution as per Article 3 of the EMD2.
[38] For instance, providers and/or partners could notify their home NCA about their intention to provide the same services in all Member States, eventually deciding to concretely provide services in only a limited number of Member States. On the other hand, services may be provided in more Member States than the original notification to the home NCA, highlighting poor notification practices.
[39] See also Q&A 2021_5726 on "Triangular" passporting.
[40] In the context of the yearly Union Strategic Supervisory Priorities (USSP), the EBA has identified the key topics for supervisory attention in 2026. As part of the key topic 2, i.e. technology integration and resilience, "attention should be given to technological integration as an enabler of value chain evolutions (e.g. white labelling) and their potential reputational and operational impacts". See Annex III of the EBA Work programme 2026.

AML/CFT obligations, including outsourcing and reliance on CDD performed by other obliged entities.

Text box: ML/TF risks analysis by AML/CFT authorities

The responses to the 2024 survey suggest that in half of the Member States, ML/TF risks associated with white labelling are currently assessed specifically. In the majority of these Member States, the risk is considered medium or high. Differences may be due to the extent to which white labelling is present in each Member State.

Considerations for a high-risk assessment include the complexity of the arrangements, potential lack of direct oversight, and the involvement of multiple parties—often across borders—which significantly increases exposure to ML/TF risks. When the provider engages with unregulated partners in high-risk jurisdictions, these challenges are further exacerbated, making it more difficult for the regulated financial institution to maintain effective transaction monitoring and ongoing compliance. Considerations for a medium-risk assessment include variations in the specifics of the business model, the nature of the products and services offered, and the degree of involvement of the partner. Considerations for a low-risk assessment include the limited scale of operations via white labelling and the inherently low risk associated with the services or products offered.

6. Conclusion

41. White labelling appears to be widely used in the EU banking and payments sector to distribute a broad range of financial products and services. While traditionally taking the form of agreements between financial institutions in both the role of provider and partner, the EBA finds that non-financial entities are emerging increasingly as partners (for example, some BigTechs are acting as partners to distribute financial products and services as a complement to their broader service offerings).

42. In practice, white labelling agreements differ based on 7 key features: the regulatory status (financial or non-financial) of providers and partners, the allocation of tasks, the core or ancillary nature of the business model, the product or service distributed, the target customer (retail or corporate), the geographic distribution (domestic or cross-border), and the fee model (flat, per use). The report finds that, depending on variations in these features and the specificities of each white labelling arrangement, potential benefits and risks for customers, providers and partners may arise. The report also finds potential challenges for supervisors.

43. White labelling can benefit partners and providers, by improving cost efficiency, broadening the offer of financial products and services, and supporting the creation of new revenue streams. In turn, this can benefit consumers who may enjoy access to a wider range of products and services at potentially lower costs. However, the involvement of multiple entities implies a fragmentation of the value chain and may create complex business models, which in turn can increase challenges and risks for consumers, providers, partners, and supervisors.

44. For consumers, particular challenges can arise in terms of navigating and understanding the roles of the provider and partner, including in the context of complaints handling and redress. Concerns and risks can also arise in the context of data protection and data privacy. The risk of mis-selling practices may increase in the context of product placement via white labelling. The risks of fraud may also be elevated in the event of weaknesses in partner CDD practices, and absent sufficient oversight by the provider.

45. Challenges for providers and partners mainly arise in terms of business model risk, operational and reputational risks. Providers and partners may also face challenges in demonstrating and ensuring compliance with the AML/CFT framework, for instance due to possible differences in national identification and verification requirements, or as a result of the fragmentation of data and procedures among different entities. Providers may face difficulties in ensuring that partners, especially when they are not a financial institution, act in full conformity with expectations regarding measures to conform to regulatory requirements. Moreover, providers and partners may encounter challenges in qualifying the regulatory classification of the arrangement (i.e. in terms of outsourcing, agency and/or third party reliance). Particularly in cases where there is a cross-border element, challenges may increase in terms of identifying and aligning with the relevant supervisory expectations.

46. Supervisors face challenges in identifying when, how and where white labelling is being used to distribute financial products and services due to gaps or limitations in notification practices. Additionally, supervisors may lack supervision powers over (certain) partners (e.g. where the partner is not an authorised financial institution, or where the supervisor of the provider is not the same as the supervisor of the partner).

47. More generally, absent clear information about the concrete white labelling agreement, it can be challenging not only for providers and partners, but also for supervisors to qualify the arrangement from a regulatory perspective (outsourcing, agency, other). In cases where the requirements are not fully harmonised by EU law, the regulatory qualification and regulatory obligations consequent on that qualification can vary from Member State to Member State. As such, additional efforts are needed to enhance knowledge sharing about business models and promote convergence in classification. In this context, the revision of the EBA GL on outsourcing will introduce a broader concept of third party risk management and will help promote convergence in the regulatory classification and expectations toward these arrangements.

48. The EBA has not identified areas of EU law that require amendments. However, the EBA has identified a need for supervisory convergence in promoting common understanding among NCAs about potential opportunities and risks, the regulatory qualification of the arrangements between the parties, and ensuring the information conveyed to consumers is clear. Inter alia, the EBA has noticed that supervisors rarely focus on white labelling business models in the context of line supervision. To this end, the EBA will take forward in 2026 actions to facilitate supervisory dialogue, including discussing individual case studies, with a focus on the regulatory qualification of the arrangements between the provider and partner. The EBA will also continue to monitor banks' engagement in white labelling via the annual Risk Assessment Questionnaire.

49. The integration of white labelling in NCAs' supervisory priorities and activities in line with the key topics for supervisory attention set in the 2026 Union Strategic Supervisory Priorities (USSP) will further enhance supervisory attention on the issue. This report can support NCAs in identifying the key features of while labelling and the potential risks that could arise, including for consumers. A questionnaire developed by the EBA will also help NCAs in the context of their day-to-day supervisory activities.

50. As regards consumer protection, going forward the EBA will focus on consumer-facing disclosures and discussion among NCAs about appropriate measures to facilitate awareness by consumers of key elements, including with whom they are ultimately contracting and how/to whom they can submit complaints.

Annex I: Third party dependencies

In practice, the arrangements put in place between the white label provider and partner may imply a dependency on the other party. The regulatory qualification of this dependency will be informed by the precise arrangements[41].

By way of examples:

Third party risk management (including outsourcing) for AML/CFT purposes

The provider may outsource to the partner the performance of certain tasks relating to customer due diligence (CDD) for AML/CFT purposes, while remaining responsible for compliance with the AML/CFT requirements. This is a classic 'outsourcing' scenario. This must be clearly documented, with roles and responsibilities unambiguously defined to ensure regulatory alignment. In some cases, the partner may also rely on the provider for the performance of certain operational functions such as record-keeping.

Third party dependency more generally

The EBA Guidelines on outsourcing arrangements apply to a broad range of financial institutions, including credit institutions, payment institutions and electronic money institutions, and ensure the effective oversight and risk management of the outsourcing of processes, services or activities that would otherwise be undertaken by the institution. These Guidelines are currently subject to revision to encompass a broader range of third-party dependencies and, accordingly, are proposed to be re-named 'Guidelines on the sound management of third-party risk'[42].

Use of agents in the context of payment services

In some cases, the white labelling arrangements may involve the partner acting as an agent of the provider. For example, the use of agents is commonly the case in the context of the provision by payment institutions of payment services (see Article 19 PSD2) where agents may not only perform operational functions for the payment institution (e.g. the outsourcing scenario outlined above) but may provide the payment service itself on behalf of the payment institution (such as money remittance). In cases where the partner acts as an agent, specific obligations may apply (where the partner is also an outsourcee, any obligations applicable in its capacity as an agent will apply in addition to any measures under the outsourcing framework). The precise nature of the obligations depends on two core elements (a) the activities undertaken by the agent, and (b) the location of the agent (and the provider).

[41] For example, a partner may be performing functions which engage specific requirements (e.g. in cases where the partner is determined to be a PSP agent, a service provider, an ICT service provider, a tied agent, an account information service provider, a credit intermediary).
[42] See EBA/CP/2025/12.

In cases where the requirements are not fully harmonised by EU law, the nature of the obligations can vary from Member State to Member State. For example, in some Member States, agents, may be required to hold certain qualifications or attestations, and may be subject to specific conduct of business obligations, including regarding the ability to carry out 'suitability assessments' of financial products for consumers, and record-keeping. For industry, variations between Member States about when a partner may be considered to be acting as an agent, and any resulting requirements, can pose challenges in scaling activities cross-border.

From the perspective of the competent authorities challenges may also arise. For instance, for the competent authority in the home Member State of the provider, there may be challenges in understanding the full range of controls and risk mitigation absent a clear understanding of the local expectations attached to the partner. For the NCA in the host Member State there may be challenges in understanding if there is reliance by a provider on a local partner for the distribution of a financial product or service, resulting in the supervisor being unable to ensure conformity with any supplemental local requirements applicable to agents. These problems can be compounded where any supervisor appointed for the purposes of any local requirements applicable to agents is not the same as the 'host competent authority' notified by the home competent authority with regard to the provision of the financial service. Finally, risks of regulatory arbitrage may arise in cases where partners may seek to rely on agents, including in so-called 'three-way' passporting arrangements, where an agent in Member State A leverages the licence from the provider (in Member State B) to carry out financial services in Member State C, with a view to circumventing any supplemental requirements in Member State C.

Third party introduction/reliance for Articles 25 and 26 AMLD5

For completeness it is noted that, in very specific cases where the partner is an authorised entity, the provider may be able to rely on the partner for CDD (see further Annex II).

Annex II: Additional AML/CFT considerations associated with white labelling

The nature of the relationship between providers and partners in AML/CFT

In white labelling models, the nature of the relationship between the provider and the partner is usually an outsourcing arrangement or maybe qualified as third party introduction/reliance arrangement[43]. In the latter case, where the partner is an obliged entity for AML/CFT purposes, the provider will be able to rely on it pursuant to Articles 25 and 26 of AMLD5. This means that the provider will rely on the partner's own AML/CFT measures, provided that adequate information is obtained, and appropriate risk-based oversight is maintained. In this case, the third party (the partner) has their own business relationship with the customer, which is independent from the business relationship the relying institution has with the customer. Equally, the partner applies CDD measures to the customer in line with its own processes in compliance with its own AML/CFT obligations.

Alternatively, the arrangement may be an outsourcing arrangement under third party risk management. In this case, the partner will apply AML/CFT measures on the provider's behalf as specified by the provider, while the provider remains fully responsible for ensuring compliance with all AML/CFT obligations. This includes establishing clear contractual terms, conducting regular reviews and audits, and ensuring that the outsourced activities are subject to the same standards as if they were performed in-house. Depending on the jurisdictional approaches, outsourcing arrangements are, in principle, possible irrespective of whether the partner is an obliged entity for AML/CFT purposes itself.

In cases where the partner is itself a financial institution and where the arrangement amounts to a correspondent relationship (e.g. access to accounts or payment services on behalf of the provider), Article 19 of AMLD5 will apply. In such cases, the provider must apply enhanced customer due diligence on the relationship. This will include gathering sufficient information on the partner's AML/CFT controls and obtaining senior management approval.

Regardless of the specific model, providers must ensure that roles and responsibilities are clearly defined, risk assessments are regularly updated, and effective mechanisms are in place to monitor the partner's compliance. All reliance or outsourcing arrangements should be supported by robust documentation and be auditable for supervisory purposes.

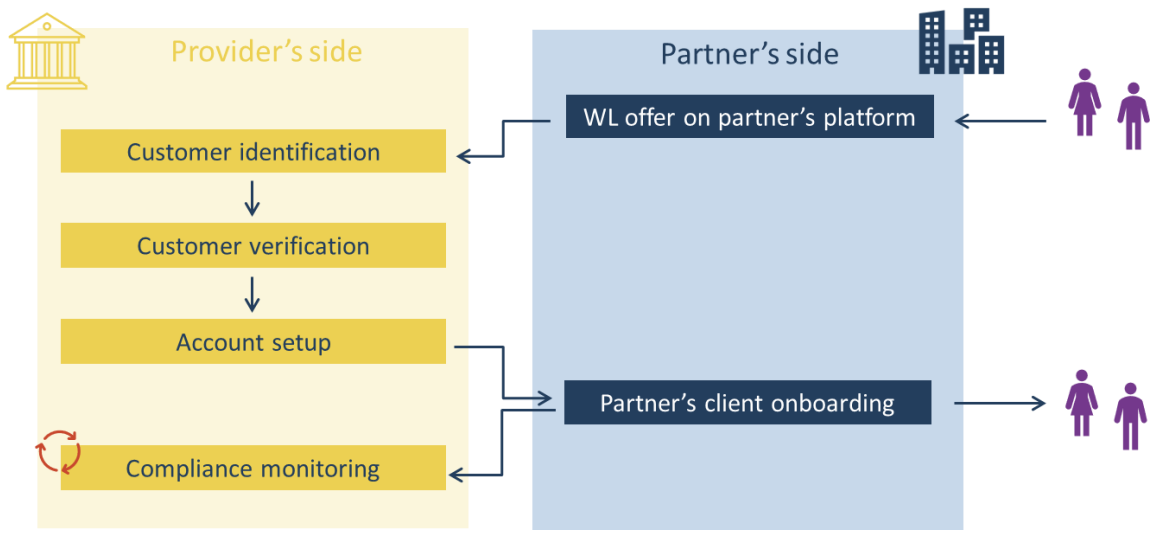
[43] The differences between outsourcing and third party reliance in the context of AML/CFT are explained in Q&A 2020_5100.

Examples of customer due diligence tasks

Customer identification and verification (KYC/KYB) performed by the provider: This model enables partners to onboard customers through an interface that is fully developed, hosted, and managed by the provider (see Figure 4 below).

In some models, the provider offers a standard interface with predefined fields for essential customer information. The extent of required information varies significantly among different providers and depends on the ML/TF risk profile associated with the business. Other models provide a fully customisable solution, allowing partners to tailor the data collection process to a risk-based approach (of the party responsible for the identification and verification tasks according to the contractual arrangements). Customer information may be collected directly from the partner's clients via a dedicated link or provided by the partner itself through an outsourcing arrangement.

Figure 5. Customer identification and verification (KYC/KYB) performed by the provider: steps performed by each entity.



The onboarding interface can either be 'white labelled' to align with a partner's brand or kept in the provider's original format. Typically, there is no need for additional interface development, as partner's clients are redirected to the provider's platform.

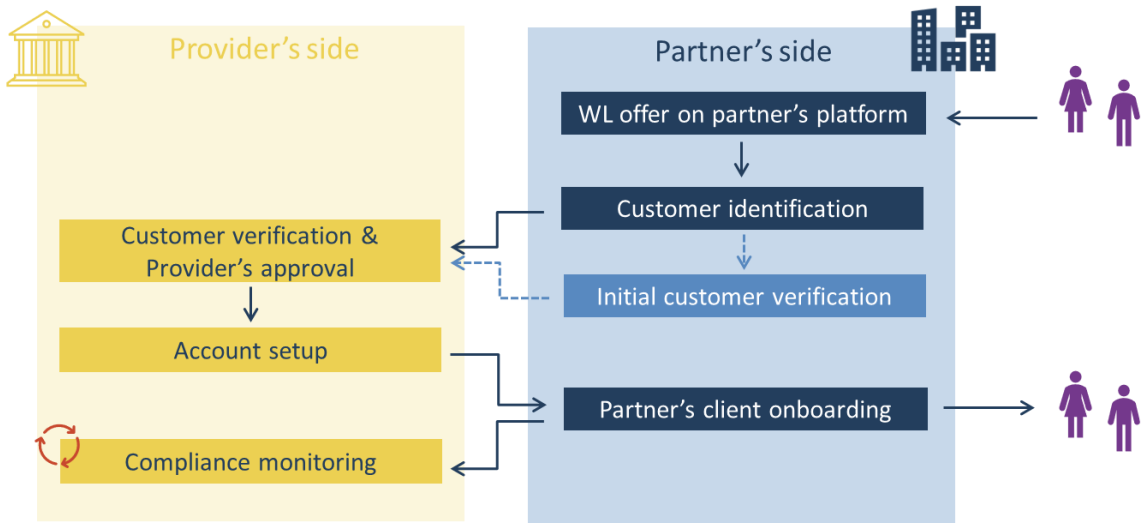
Once all required information and documents are submitted, the provider conducts (often automated) verification checks and, if necessary, may request additional information—either from the partner or directly from the partner's customers (depending on contractual arrangements in place).

The partner's customer is only onboarded once the provider grants approval.

Customer identification and verification (KYC/KYB) performed by the partner, supporting the provider: In this model, the partner may collect the necessary customer information for identification (see Figure 5 below). In some cases, the partner may also conduct initial verification checks. Once the application process is completed, the partner submits it to the provider for approval.

The customer becomes active only once all checks are satisfactorily completed and approval has been granted by the provider.

Figure 6. Customer identification and verification (KYC/KYB) performed by the partner: steps performed by each entity.



Risk monitoring. Providers usually perform monitoring tasks themselves using tools for real-time risk monitoring to detect potential ML/TF. For instance, risks are calculated using a customisable risk model, with early warning alerts that cover amounts, number of transactions, specific patterns, the consideration of clients' historical patterns, calculating individual thresholds per partner's customer or account, considering the risk of a customer/account etc. These monitoring systems are often integrated with the provider's infrastructure via APIs (Application Programming Interfaces), which allow for the automated and secure exchange of data between the core transaction systems and the monitoring engine.

Annex III: Summary of potential opportunities and risks per type of stakeholder

Table B. Summary of opportunities and risks per type of stakeholder.

Opportunities	*Customer*	*Provider*	*Partner*
Cost efficiency	✓	✓	✓
Expanded offer	✓	✓	✓
Better targeting of products/services	✓	✓	✓
Increased customer base		✓	✓
Enhancing financial inclusion	✓		
New revenue streams		✓	✓
Development of new technologies and platforms	✓	✓	✓
Foster competition	✓		✓
Risks	*Customer*	*Provider*	*Partner*
Misleading/insufficient information, mis-selling	✓		
Fraud	✓		
Difficulties in complaints handling	✓	✓	✓
Data protection concerns	✓		
Financial exclusion	✓		
Business model risk		✓	✓
Operational risk		✓	✓
Reputational risk		✓	✓
Lack of direct customer relationship		✓	
Regulatory and compliance risk (including with AML/CFT and prudential requirements)		✓	✓
Step-in risk		✓	

Tour Europlaza, 20 avenue André Prothin CS 30154
92927 Paris La Défense CEDEX, FRANCE
Tel. +33 1 86 52 70 00

E-mail: info@eba.europa.eu

https://eba.europa.eu