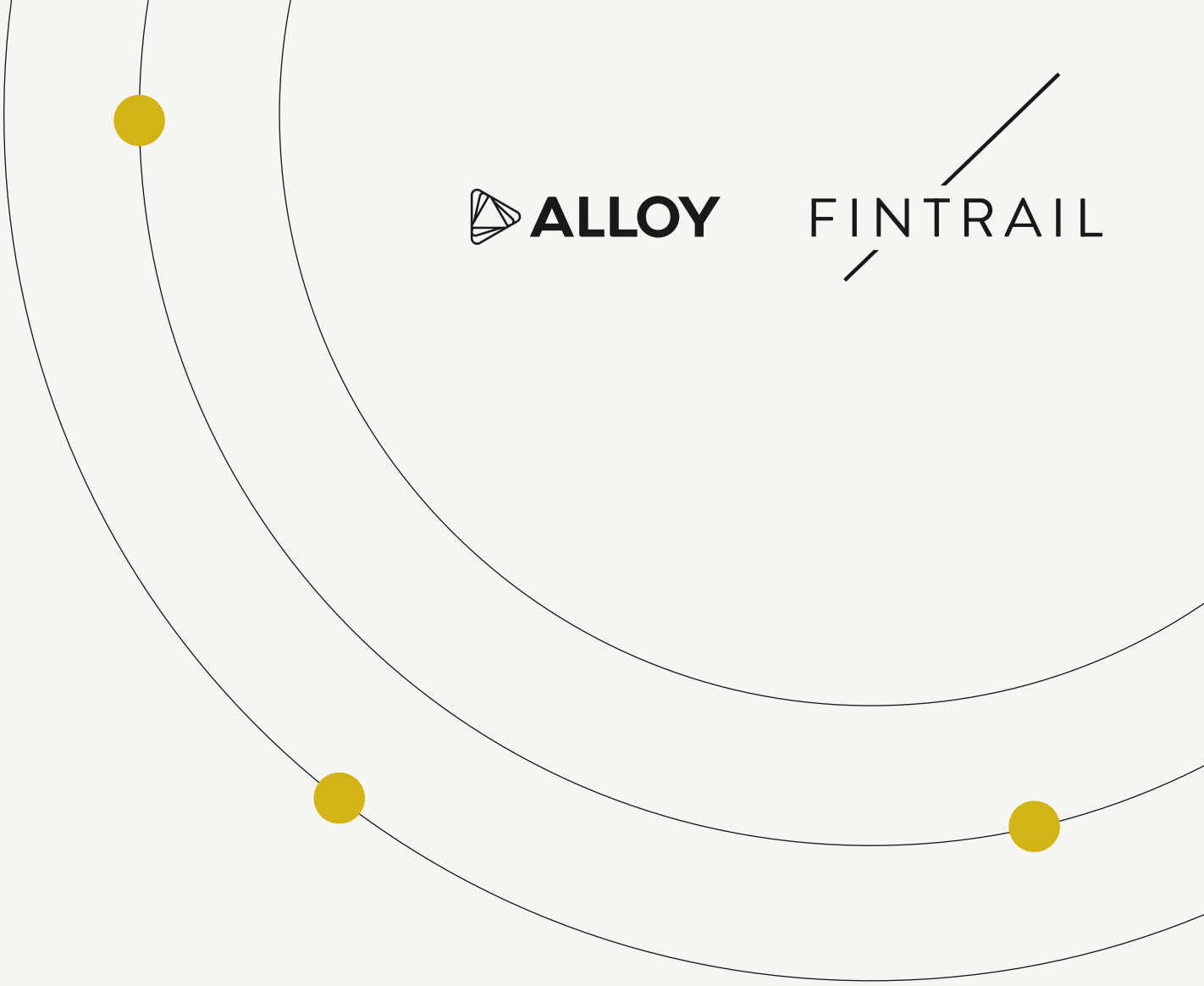

ALLOY FINTRAIL

White Paper

Embedded finance: Navigating risks and seizing opportunities

Embedded finance — Transforming the future of financial services

Embedded finance — the integration of financial products into non-financial offerings — is shaking up the financial landscape and drastically changing how people interact with financial services. The sector is growing fast and creating massive economic opportunities, with a total predicted market size of $35 billion by 2029.[1]

Embedded finance products have been around for years — think of your store credit card or an auto loan arranged at the car dealership. Once you start looking out for them, you'll spot them everywhere you spend money. Ecommerce retailers can now offer banking services through their apps without making customers onboard via a banking platform, and payment firms can go live in a fraction of the time by using a banking partner's license. The scale of offerings has surged with the explosive growth of digital payments, aided by the development of open banking, and driven by an increasing focus on frictionless customer experiences. A recent study by EY revealed that global fintech leaders believe the key to successful financial products is the ability to address customers' needs in real time.[2] Embedded finance provides opportunities for consumers to access financial services instantly, making their journey with financial and non-financial providers more seamless than ever.

In the banking-as-a-service (BaaS) space, fintechs are coming to market at an unprecedented pace as the BaaS model allows them a faster, simpler way to offer financial services without having to incur the costs of a payments license. The rise of challenger banks (also referred to as neobanks) has demonstrated that consumers are hungry for improved digital experiences and convenient services. This is often something that traditional banks have struggled with — think long account opening processes, visiting branches with physical documents, and even undergoing a separate account opening process to take out a second financial product. The BaaS model allows businesses to focus on customer experience and design, with the more complex regulatory tasks taking place behind the scenes managed by the BaaS provider.

What is embedded finance?

The term 'embedded finance' essentially refers to the integration of financial services into non-financial offerings, allowing non-regulated firms to provide financial products to customers without having to build their own financial infrastructure and obtain their own regulatory licenses. It encompasses a range of products and services, including embedded banking (also known as Banking-as-a-Service or BaaS), embedded lending (also known as "buy-now-pay-later"), embedded payments, and branded credit cards.

[1] Embedded Finance Sector: Business Models, Regional Forecast 2023-2029
[2] EY: How banks are staking a claim in the embedded finance ecosystem

Glossary

Here is a handy glossary of terms for embedded finance — your go-to guide for understanding all the jargon and terms for the various business models floating around in this ever-growing space!

Principal

The licensed financial institution providing the underlying embedded finance products and services. They could be a regulated bank, payment service provider, or e-money institution. In the UK, under the FCA regulatory framework and authorisation, principals are the firms which hold the regulatory license and enter into a business relationship with agents. Also known as the '**parent**' organization, '**sponsor bank**,' or '**partner bank**' in the US.

Agent

An agent is a business which acts on behalf of, or under the license of, a licensed financial institution (the principal). They are usually customers of the principal, but could be a subsidiary or associated business. Also referred to as a '**distributor**', '**program**', or sometimes '**child account**', especially in the US.

End user

An end user of an embedded finance product is the agent's customers — i.e. the individual or company using the agent's services, for example, an individual using Uber, or a company whose website accepts online payments. While this user is not a direct customer of the embedded finance provider, they are using its services indirectly.

Use cases for embedded finance

Embedded finance can refer to any case of integrating financial services into non-financial platforms, products or services, or non-regulated entities. Here is a non-exclusive list of some popular use cases — there are many others!

Banking-as-a-Service

BaaS refers to the provision of banking services, such as payments, lending, and account management, by banks or licensed financial institutions, such as Railsr and Modulr, to non-licensed institutions through APIs and other infrastructure. BaaS is very popular with fintech startups and challenger banks that lack their own regulatory licenses and use BaaS as a quicker way to market.

BaaS also covers so-called 'white label banking' where banks or other BaaS providers offer their digital banking platforms and services to other financial institutions or businesses that use their own branding.

Within the BaaS space, the concept of compliance-as-a-service has also grown in popularity. BaaS providers provide their banking license and infrastructure, and can also provide their compliance capabilities to their customers. Compliance services can range across the control areas, including due diligence, compliance monitoring, training, and awareness.

Payment-as-a-service

Payment processors — such as Square, PayPal, and Alipay — offer cloud-based payment services and access to payment schemes to B2B and B2C companies. They allow their customers to use and pay for specific parts of the payments stack, like cross-border transactions, payments clearing, card issuing, or ecommerce gateways. Their product suites can also include services like revenue management, transaction reporting, and risk management services.

Ecommerce platforms

The array of options available to consumers paying for goods and services online has multiplied in a very short space of time. Embedding financial services within ecommerce platforms streamlines the buying process and allows customers access to financial products like loans or insurance without being routed via another platform. For example, customers can access instant loans from buy-now-pay-later providers such as Klarna, or purchase insurance directly from Insurtech firms when making online purchases.

Marketplaces

Embedding financial services like escrow accounts or financing options within online marketplaces such as eBay and Facebook Marketplace ensures secure transactions and expands purchasing power for buyers. Sellers can benefit from streamlined payment processing and access to financing for inventory or expansion.

Embedded finance in Internet-of-Things (IoT) devices

IoT devices, such as smart appliances and connected cars, can leverage embedded finance to offer financial services directly to consumers. For example, a smart refrigerator could automatically reorder groceries and make payments using integrated banking functionalities.

Ride-sharing and delivery services

Integrating payment services directly into ride-sharing or delivery apps like Uber and Deliveroo simplifies transactions for both customers and service providers. Additionally, offering services like micro-insurance for drivers or goods during transit enhances user experience and safety.

Real estate

Financial services such as mortgages, escrow services, or property insurance can be embedded into listing platforms, simplifying the buying process for homebuyers and sellers. This integration can facilitate faster transactions and reduce paperwork.

Understanding the risks and challenges of embedded finance

The opportunities offered by embedded finance seem pretty clear. However, the model also poses a unique set of challenges in relation to risk and compliance.

> It's hugely important to understand that embedded finance providers are liable for any breaches of regulations by other firms using their license. It's their license, their regulatory responsibility.

However, these providers often have limited oversight over the end users and their activities, making it hard for them to adequately assess and monitor the risks they're taking on. There can also be confusion around the roles played by providers (i.e. the principal firm or sponsor bank) and their customers (i.e. the agent or program) and their respective responsibilities in terms of compliance. It is important to note, however, that while the legal responsibility sits with the embedded finance providers, there are still contractual obligations the embedded finance agents need to fulfill.

Embedded finance has flourished in the current regulatory framework, although arguably, the regulations have not been designed with some newer, more complex embedded finance models in mind, often leading to murky regulatory guidance that is not prescriptive enough for these business models. The regulatory frameworks are evolving, however, with increased scrutiny on banks and EMIs to ensure they stay on top of compliance obligations and implement effective Know Your Customer (KYC) and anti-money laundering (AML) controls.

An inherent risk faced by embedded finance providers and users, particularly new firms or those launching new products, is being marked out by criminals who perceive new offerings as having weaker, less sophisticated fraud and AML controls. Money laundering and fraud syndicates will often deliberately target banks and fintechs with new embedded finance products, trying to permeate them at inception or go-live. This can result in these firms having to stop new customer sign-ups to tackle fraud spikes and enhance their controls before opening up again. This is a key financial crime risk for embedded finance providers to be aware of, given their regulatory responsibility for the firms being targeted.

There has recently been significant regulatory attention on the BaaS space. In 2023, two key players in the European BaaS market — Solaris and Railsr — were found by their respective regulators to have serious failings in their compliance controls and were forbidden from onboarding new customers without prior consent from the regulators. On the other side of the Atlantic, in 2022 and again in 2024, the Office of the Comptroller of the Currency (OCC) issued two consent orders to Virginia-based community bank Blue Ridge Bank, instructing it to make serious reforms to its compliance practices, and not to enter any new business relationships with fintechs without prior approval.

CASE STUDY

Examining risks and failures

In 2023, the Bank of Lithuania revoked the license of UAB Payrnet, the European arm of UK embedded finance provider Railsr, for committing "serious, systematic and multiple violations of legal acts".[3] This included:

- Not properly identifying agents or their representatives, not verifying or checking information about agents' ultimate beneficiaries, and not identifying the intended nature of agents' business relationships
- Conducting improper due diligence and inadequate assessments of its agents' suitability, reputation and risk
- Not controlling how and to whom agents provided their services or how they performed their delegated AML/CTF functions
- Failing to provide the required training to agents
- Not detecting suspicious transactions or reporting them to the Financial Crime Investigation Service in a timely manner
- Not being able to tell whether transactions and operations carried out by agents violated international sanctions
- Failing to properly verify whether agents, beneficiaries or agents' representatives were sanctioned or were dealing with sanctioned parties

In June 2023, the main US regulators — the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency — issued guidelines to help banks manage the risks associated with third-party relationships.[4] The guidance said, "such relationships may introduce new or increase existing risks to a banking organization" while also recognizing both the benefits and risks of bank-fintech partnerships.

In March 2023, the UK's Financial Conduct Authority (FCA) issued a "Dear CEO" letter which said it had seen increasing evidence of financial crime in the payments space. It issued a clear reminder that parent firms are responsible for ensuring agents are registered with the FCA and that they comply with the relevant regulations. Parent firms must also have appropriate systems and controls in place to effectively oversee their agents' activities. The letter added that with "bank-like services willing to service high-risk customers and [with] weaknesses in some firms' systems and controls, it has made payment institutions and EMIs a target for bad actors".

Given the regulatory attention in this space, it is important for embedded finance providers to take seriously the consequences of getting things wrong. Ending up on the wrong side of the regulator can mean a suspension of licenses or restrictions on new business, as seen with the cases of Solaris, Railsr, and Blue Ridge Bank. Firms also run the risk of serious fines, which can result in both large financial losses and reputational damage.

[3] Bank of Lithuania: Licence revocation notice
[4] Interagency Guidance on Third-Party Relationships: Risk Management

Why it's worth getting it right

Despite these challenges, embedded finance is here to stay. It's already existed in some form for a long time and has many valuable use cases; the genie cannot be put back in the bottle. However, there is no doubt firms need to fully grasp the nature of the risks the model poses, and stay on top of new regulatory measures and compliance obligations. There are clear advantages to working out how to do this — with some market incumbents struggling with regulator-imposed restrictions and some new entrants discouraged by the compliance burden, the potential rewards for those providers who can get it right and stay in the game are considerable.

With the growing market share of embedded finance products but also the heightened regulatory attention, there is a real need for both principals and agents to have proper risk management frameworks in place to seize market opportunities while managing their risk responsibly. Compliance, including AML and fraud, must be at the forefront of the embedded finance agenda and must be baked into a firm's business model from the start. This entails a holistic risk management approach that identifies and assesses specific risks associated with embedded finance and implements mitigation strategies designed with these risks in mind.

How to make it work

Recent regulatory messages and enforcement actions give a clear idea of what regulators are looking for, and offer valuable advice for embedded finance providers. For instance, the FCA's Dear CEO letter reminded payment firms of the importance of:

- Having sufficiently knowledgeable and experienced staff to perform compliance role
- Having governance arrangements, risk procedures, and controls that are comprehensive and proportionate to the nature, scale, and complexity of the business
- Conducting meaningful due diligence before onboarding agents and distributors and performing ongoing monitoring

Building on this, here are the key things for embedded finance providers to think about which can help them manage their risks and keep their operations running smoothly:

1. Avoid a one-size-fits-all approach

All good risk management frameworks need to be tailored to a specific business model, and this is definitely true for embedded finance. Your products, your customers, your customers' products, and your customers' customers will all affect your risk — it's a complex model! For example, a travel company offering embedded loans poses different risks to a cash savings app, and some of your customers may have much higher risk appetites than others and be happier taking on riskier end customers. Embedded finance providers need to design appropriate controls specific to the risks posed by particular customers or agents. This could involve categorizing customers by product type or overall risk level, or it could mean having a bespoke control and oversight framework for each customer. As such, there may be instances where a more controlled agent relationship is required (i.e. stricter oversight of the agents' financial crime and fraud control framework, or more processes carried out by the provider directly) versus a more autonomous agent relationship (i.e. where there is less oversight required given the maturity of the agent). Embedded finance providers should be mindful that often having a one-size-fits-all approach in the name of compliance can result in a detrimental user experience. By customizing controls at the customer level, the principal firm and the agent can arrive at a mutually beneficial solution.

2. Clearly defined roles and responsibilities

There are many players involved in an embedded finance model — principals, their customers (i.e. agents, programs), and end users (i.e. the customers' customers) — so it must be clear from the outset who is doing what.

> Poorly defined roles or misaligned assumptions may result in things going wrong or being missed, allowing criminals to take advantage.

For instance, who is responsible for writing and then updating policies and procedures, defining risk appetite, designing or approving customer risk methodologies, designing screening and transaction monitoring systems and handling the resultant alerts, monitoring fraud and associated refunds, and for conducting quality assurance? Some providers might want to do more of these activities themselves, others will hand them over to agents, and others may take a nuanced approach and perform these tasks for less experienced or new agents while being happy to delegate to others with more experience.

It is vital to have clearly defined and documented roles and responsibilities across the framework, and establish regular check-ins to ensure responsibilities are being upheld. This can be supported through the constant provision of reliable management information, regular check-in calls, or ongoing testing or quality assurance activities.

3. Scalability and adaptability

Anti-financial crime models need to be flexible for both the principal firm and the agent. Clearly, business models may change over time with providers or customers changing their offerings, expanding to new markets, or targeting different customers. Similarly, the balance of who does what on the compliance and fraud side may change.

> Fintech clients are likely to improve their internal capabilities and be able to meet more of their own compliance needs over time, by improving senior management's understanding of financial crime, hiring dedicated teams, or building out their own control areas, such as onboarding or transaction monitoring.

Principals may also want more oversight over agents when they first onboard them, but become comfortable delegating more procedures to them over time as they gain reassurance while still maintaining oversight. A good model allows controls, roles, and responsibilities to change over time.

4. Ongoing oversight and scrutiny

Financial crime and fraud risks, regulatory requirements, and business models all change over time, and embedded finance firms need to ensure that they maintain an up-to-date picture of their clients' activities, customers, risks, and anti-financial crime controls. They should build a system that facilitates this through clearly defined policies and procedures, regular management information, and reliable data to facilitate quality assurance and auditing. One key area is risk assessment — providers must make sure they not only assess their clients' risk levels thoroughly at onboarding, but that they adopt a dynamic risk assessment methodology to reflect ongoing changes. This should then inform the degree of oversight applied, and potentially how the control framework is implemented — for instance, stepping up assurance processes or rewriting policies and procedures if the risk level goes up.

5. Use of automation and technology

Insufficient resourcing is a major challenge for embedded finance firms. Since their customers are often relatively small and lack specialist anti-financial crime staff (you often find people double-hatting, for instance, the CEO wearing the hat of Chief Compliance Officer), principals take on a huge strain on resources with each new client program, as they must conduct many compliance tasks themselves or double-check what the agents are doing. This is compounded by the more agents they take on, limiting their ability to scale. The solution is automation, whether building in-house tools and systems or using third-party solutions.

> Automation can free up resources from menial, repetitive tasks to focus on other, more complex compliance priorities.

It also helps close potential blind spots that manual processes may open up (for example, a policy change not being implemented in all applicable areas through a manual process).

6. Building a streamlined toolbox

The process of selecting a third-party provider, or of building a new tool in-house, is a major project and requires a lot of spare capacity on top of business as usual (BAU) operations. Using a tool with multiple capabilities across the anti-financial crime framework (e.g. ID verification, credit checks, ongoing monitoring, and case management) reduces the operational burden of selecting and maintaining multiple tools. It also reduces the likelihood of silos and disparate systems that don't talk to each other, and future-proofs firms' programs for any new use cases and needs that may arise as the firm scales. Having a single system of record is also beneficial for regulatory reporting and audit purposes.

7. Data, data, data

Data is essential to assess the risks faced and determine whether controls are working effectively. Embedded finance providers must make full use of all their own internal data, and ensure access to as much of their clients' data as possible. Siloed information split between the principal and agent limits the extent to which either party can successfully manage financial crime risk. External data sources also have an important role to play — covering everything from fraud databases, corporate records, adverse media, watchlists, and credit databases.

> As providers take on new partners with different business models or needs, and as they seek to respond to evolving threats and regulatory requirements, it is also useful to be able to swap data sources in and out.

Screening against a UK fraud database may be really useful for some client programs, for instance, but for others, it may not be relevant and instead just generate burdensome false positives. Having access to a wide variety of data sources and the agility to plug and play them helps providers manage their risks more effectively.

Final thoughts

Embedded finance solutions have gone through a rapid transformation in the digital payments era. We have seen more and more providers come to market, and subsectors like buy-now-pay-later evolve, bringing with them both new opportunities and new challenges. Firms offering embedded solutions and banking-as-a-service must fully understand the risks of operating these business models, and their responsibilities in the regulatory context. It is imperative they can strike a balance between rigorous oversight of their partner programs, and the ability to scale and develop. Automation and technology can help firms manage this, by simplifying and consolidating anti-financial crime controls across multiple programs, whilst ensuring flexibility and customizability, and maintaining clear visibility of both customers and end users.

About FINTRAIL

FINTRAIL is a global financial crime consultancy. We've worked with over 100 leading global banks, fintechs, other regulated financial institutions, regtechs, venture capital firms and governments to implement industry-leading approaches to combatting money laundering and other financial crimes. With significant hands-on experience, we can help you build, strengthen and assure your financial crime programme to meet evolving regulatory requirements, use technology effectively, and stay competitive. Visit fintrail.com to learn more.

About Alloy

Alloy solves the identity risk problem for companies that offer financial products. Nearly 600 banks and fintechs turn to Alloy's end-to-end identity risk management platform to take control of fraud, credit, and compliance risks, and grow with confidence. Founded in 2015, Alloy is powering the delivery of great financial products to more customers around the world. Learn more at alloy.com.