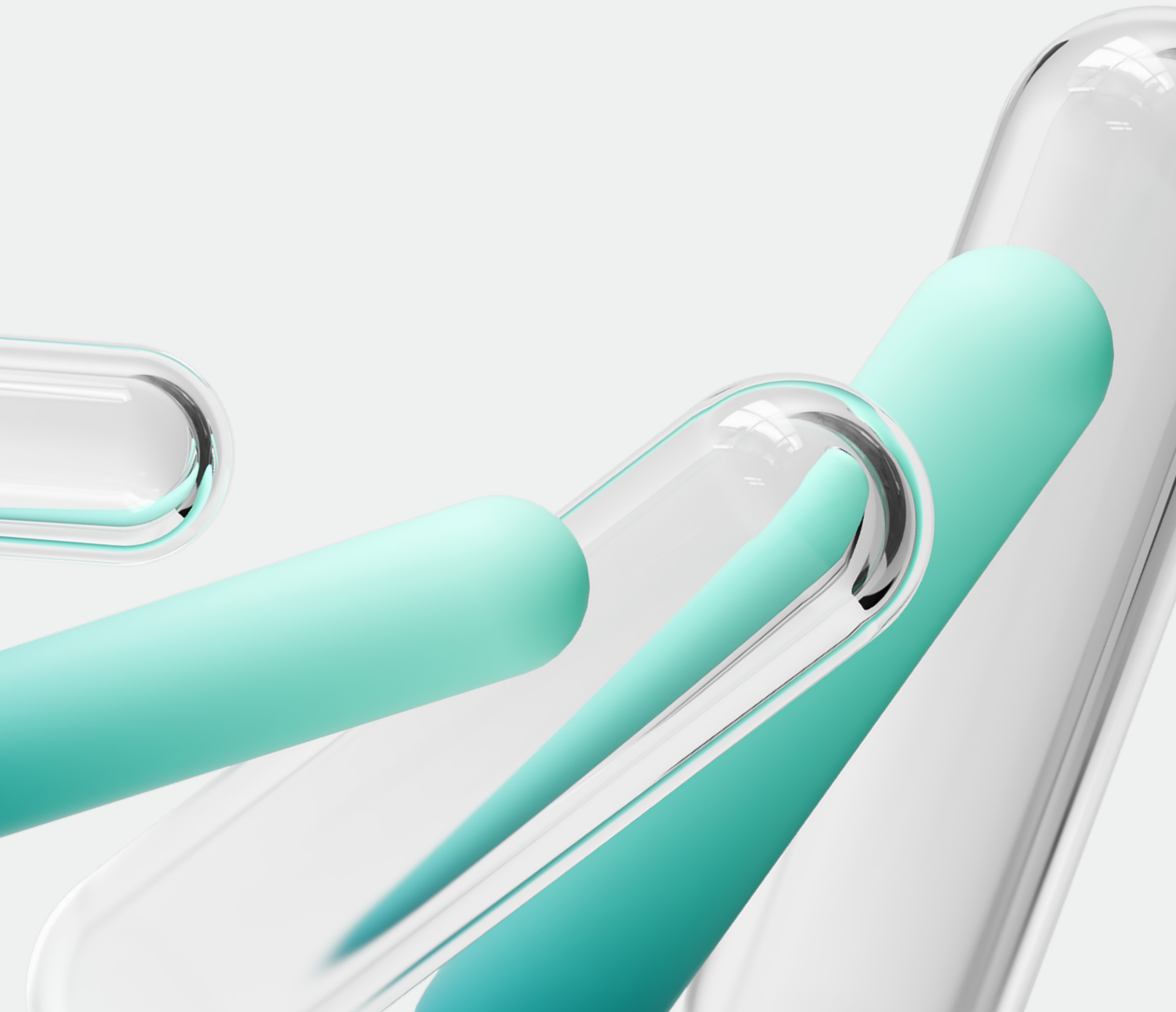


Clear.Bank | CELENT

# UK and European banks and EMIs: friends or foes?

Capturing the embedded finance opportunity



# The market is changing – are you prepared?

The line between bank and non-bank provision of financial services is becoming increasingly blurred due to the significant growth in the number and use of electronic money and payment institutions (EMIs and EPIs).

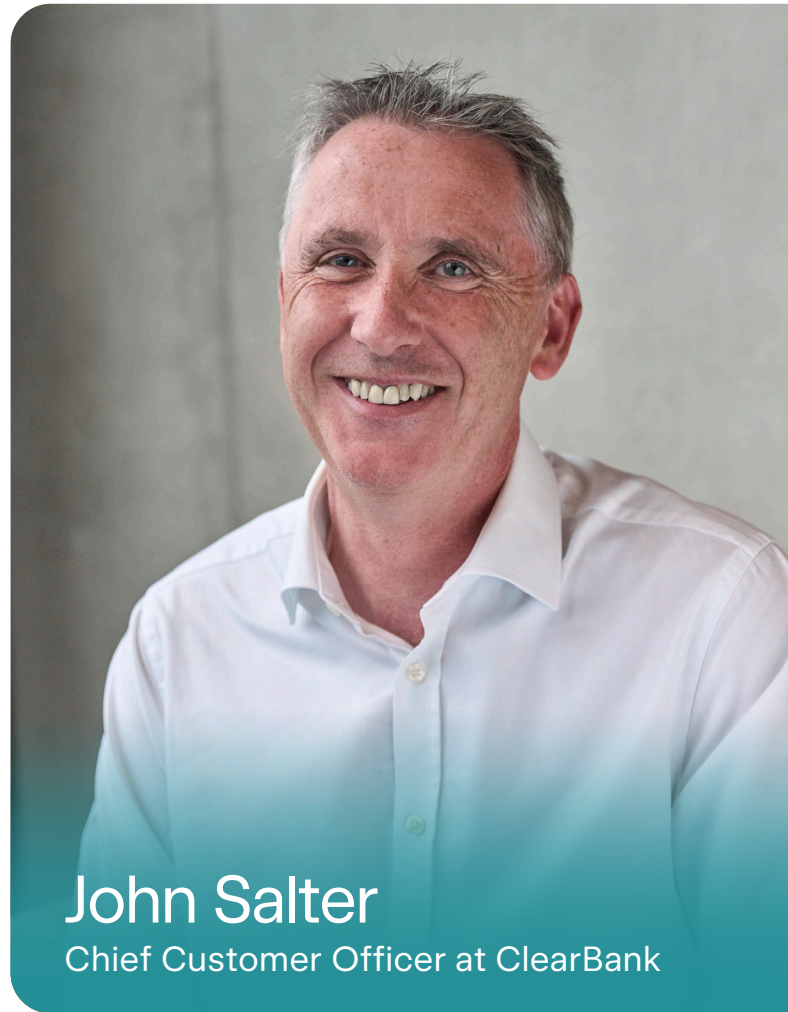
These firms have filled the gap left by incumbent banks who were unwilling or unable to support the fintech sector and now play a significant role in how financial services are delivered across the UK and EU. However, while a more relaxed regulatory framework for EMIs is often viewed as a benefit to delivering greater agility, recent market issues have suggested that the model has potential downsides.

To explore this and other key industry issues, we partnered with Celent – a leading research and advisory firm specialising in Financial Services – to conduct a research study examining the expansion of EMIs. The research looks at the key criteria firms use when evaluating partners and whether those criteria have evolved considering recent market events.

Finally, the report considers whether a new model is emerging where banks should view EMIs as collaborative partners to capture burgeoning embedded finance opportunities.

The findings reinforce that, traditionally, many firms had no option but to work with or even become EMI. Incumbent banks either viewed these firms as too small or too risky to service or were unwilling to support them as they could cannibalise their own service offerings.

At the same time, and partly in response to recent failings, firms are demanding more detail of how their client funds are safeguarded, forcing EMIs to improve their practices and reconsider their safeguarding partners. Regulators, too, are putting a renewed emphasis on ensuring that all market participants have robust operational resiliency, fraud and AML controls, and safeguarding of customer funds as the industry focus shifts to include APP fraud and Consumer Duty requirements.



**John Salter**

Chief Customer Officer at ClearBank

At ClearBank, we're excited by what the future holds.

We were built with a different purpose: to address the gap in the market between the stability of a fully regulated bank and the agility and technology-first model of EMIs for firms to deliver innovative services without the cost and complexity of acquiring a banking licence.

We work with other banks to support their services. We work with EMIs, too, because our core belief, as revealed in this research, is that cooperation and collaboration provide more options and, ultimately, better services for consumers and businesses.

**Enjoy the report.**

# **UK AND EUROPEAN BANKS AND EMIS: FRIENDS OR FOES?**

Capturing the Embedded Finance Opportunity

Zil Bareisis, Kieran Hines, Daniel Mayo

23 January 2024

This is an authorised reprint of an independent  
Celent report granted to ClearBank.  
For more information, please contact Celent  
([www.celent.com](http://www.celent.com) or [info@celent.com](mailto:info@celent.com)).

## CONTENTS

<b>Executive Summary .....</b>	<b>3</b>
<b>EMIs in Europe: The Catalyst for Innovation.....</b>	<b>7</b>
Electronic Money Institutions Defined .....	7
Key Differences Between EMIs and Banks.....	8
Introducing Safeguarding.....	10
Safeguarded Deposits: Sizeable and Growing Market.....	12
<b>The Turbulence in the Sector Driving Increased Regulatory Scrutiny.....</b>	<b>14</b>
Tighten Your Seatbelts .....	14
Regulators Sharpen Focus on Safety and Resilience .....	16
<b>Selecting and Managing Partners in Turbulent Times .....</b>	<b>19</b>
The Complexity of Ecosystem Relationships .....	19
Celent’s Hierarchy of Partner Selection Criteria .....	21
Product and Risk Appetite Alignment Dominate Partner Selection Criteria .....	22
Technical and Support Capabilities: Important but Secondary .....	23
Pricing: Decreasing in Importance .....	24
Relationships: Plan for Long-term, Prepare to Change .....	25
Safeguarding Is Getting Increasingly More Attention.....	26
EMIs Vs. Banks as Partners .....	28
Reactions to Changing Regulatory Environment .....	29
<b>Path Forward: Consider EMIs as Key Clients and Partners .....</b>	<b>30</b>
<b>Leveraging Celent’s Expertise.....</b>	<b>31</b>
Support for Financial Institutions .....	31
Support for Vendors.....	31
<b>Related Celent Research .....</b>	<b>32</b>

# EXECUTIVE SUMMARY

---

Electronic Money Institutions (EMIs) have played a key role in the growth of the fintech sector in Europe and are now becoming systemically important. As banks are looking to capture embedded finance opportunities, should they be viewing EMIs as competitors or collaborative partners, or perhaps both? What really matters to fintechs, EMIs, and banks when they are looking for a partner? Have those criteria changed in recent turbulent months?

It has been over 20 years since the Electronic Money Directive (EMD) formalised the concept of Electronic Money Institutions (EMIs) in Europe. Since then, EMIs have played a hugely important role in catalysing competition and product innovation across the region.

**EMIs hold €35 billion of client funds that need to be safeguarded**

There are just under 600 EMIs across Europe, including 250 in the UK and around 80 in Lithuania, which has emerged as a major regulatory hub for EMIs within the EU. Celent estimates that in 2022 those EMIs collectively held over €35 billion of client funds, a number that doubled in the last four years. While EMIs support significantly larger fund flows, the customer deposits need to be safeguarded as they are not covered by any deposit protection schemes, such as the Financial Services Compensation Scheme (FSCS) in the UK.

Also, until relatively recently, the fintech sector in Europe was extremely buoyant. However, the market has faced several challenges in the past 18 months or so, and conditions are now far tighter. Regulators are putting increased pressure on EMIs and their clients to demonstrate safety and resilience.

Regulatory concerns are understandable: the financial ecosystem has become increasingly open and interconnected, and problems in a single node can ripple through multiple other providers (remember Wirecard?) Players across the industry are evaluating whether their networks of partners and service providers have the necessary stability and resilience to survive this period of turbulence.

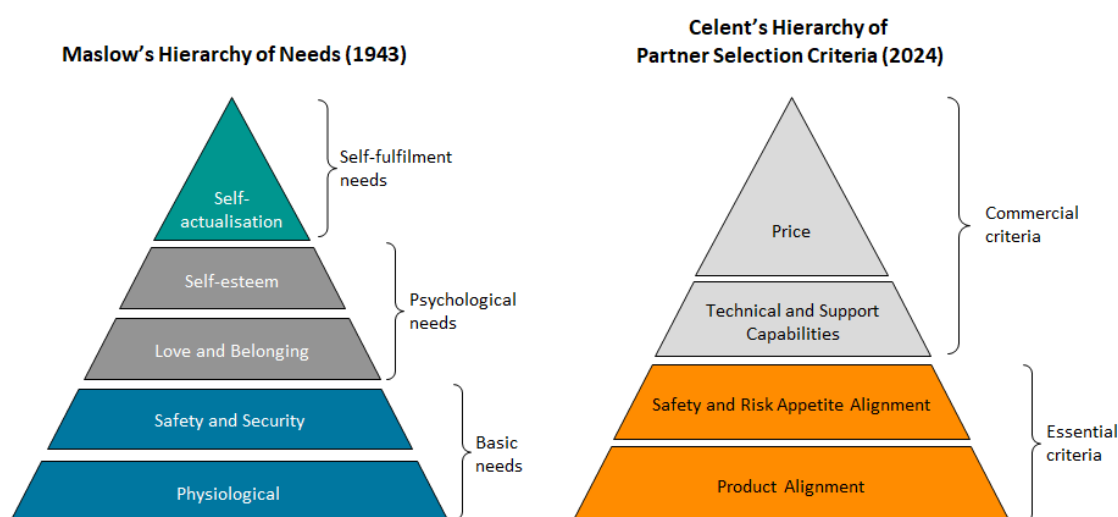
Celent kicked off this research seeking to better understand the risk posed by e-money across Europe and explore questions around how various players—fintechs, EMIs, banks—select and manage partners, such as:

- What are the key criteria when evaluating partners? Have those criteria changed in recent times?
- What is their partner selection horizon? Do players typically select partners on a short-term, medium-term, or long-term basis to start with? How often

- do they review partners? Do the current market conditions and potential risk of contagion change their attitudes?
- How do EMIs approach safeguarding? How do they and their customers view safeguarding—as a hurdle barrier in selection (i.e., needs to be demonstrated, but a risk tick box), or as a strategic element for them (i.e., used as part of customer value proposition)? How important is deposit insurance, such as FSCS protection?
  - What are pros and cons of EMIs? How much of an issue is the inability of EMIs to offer interest-bearing accounts?

Based on the research findings and inspired by Maslow’s hierarchy of needs, we developed Celent’s hierarchy of partner selection criteria (see Figure 1). Product and risk alignment are essential criteria—they must be met first, before technical and commercial discussions can take place.

**Figure 1: Maslow’s Hierarchy of Needs and Celent’s Hierarchy of Partner Selection Criteria**



Source: Celent

Other key findings include:

- As the number of EMIs increases and individual EMIs grow larger, as a sector EMIs are becoming more systemically important, posing an increasing risk.
- Ease of integration and quality of APIs matters the most when considering technical capabilities.
- The ability to provide local IBANs (International Bank Account Numbers) and avoid a practice called “IBAN discrimination” is particularly high on the list of functional requirements of many fintechs.
- EMIs earn yield on safeguarded funds but cannot pass that back as interest to their clients. Now that interest rates are relatively high, this makes banks more attractive, particularly to those partners that want to offer savings accounts to end customers.

- This also has another effect: on one hand, it reduces the importance of pricing for EMIs when negotiating deals with bank partners, as the revenue from client funds outweighs the cost. On the other hand, if EMIs attempt to pass that revenue to their clients, e.g., through rebates, they risk setting a precedent and creating a race to the bottom, which might hurt when interest rates do come down.
- The relationships that fintechs and their partners strike tend to be long-term; both sides acknowledge the disruption to the business if they have to change partners. However, both sides regularly review the partners that they work with and assess whether anything has changed.
- Many fintechs and EMIs are looking to add new partners. In some cases, the intention is to enhance the product range, but often it is to provide redundancy, mitigate against potential risk, and improve resilience.
- Safeguarding is receiving increasingly more attention. In recent years, EMI clients have started to care more about how their client funds are safeguarded, forcing EMIs to improve their practices and reconsider their safeguarding partners. However, EMIs are not spoilt for choices, as not all banks offer safeguarding services.
- The degree to which FSCS (and similar) protection matters depends on the end customer and the product. If it is a consumer account, and especially, for savings accounts, it is perceived as important. However, for payments accounts that might see a large volume of transactions but relatively low balances, or for business accounts where balances regularly exceed the £85k limit, the protection scheme is much less relevant. Of course, if EMIs manage their business risks and safeguard customers' money well—admittedly, big “if’s”—then safeguarding arguably can offer more protection as it does not have any limits.
- Finally, many providers expect the regulatory landscape in Europe to tighten in response to recent failings of market participants, and they welcome the change: “Anything that increases credibility in the industry in general is great.”

As the market continues to evolve, we expect more collaboration between EMIs and banks:

- EMIs can help align with risk appetite by insulating banks from unregulated entities. By teaming up with the EMIs, banks can deploy their advantages of a superior funding model, especially for lending, while at the same time significantly reduce their exposure to the scrutiny of onboarding and overseeing individual customers, as they ultimately belong to the EMI.
- EMIs can bring relevant technology capabilities—especially solutions that are tailored for specific industries.
- EMIs need banks for safeguarding, offering the opportunity—albeit not for all banks—to capture a share of those €35 billion deposits across the UK and EU.

We live in an age of cooptation, with the same entities competing in one area, while cooperating in another. This is true for the UK and European banks and EMIs, which can be both competitors and partners when capturing the embedded finance opportunity.

**A note on methodology**

The research study that underpins the findings discussed in this report was commissioned by ClearBank. The report was written independently by Celent. As part of the research for this report, Celent interviewed over a dozen players in the industry, including banks, EMIs, and fintechs / EMI clients, who collectively offer a range of consumer products or target businesses / commercial customers. We are grateful to all participants for their time and insights. We also kept the individual discussions confidential and did not attribute anything to specific identifiable interviewees.



# EMIs IN EUROPE: THE CATALYST FOR INNOVATION

It has been over 20 years since the Electronic Money Directive (EMD) formalised the concept of Electronic Money Institutions (EMIs) in Europe. Since then, EMIs have played a hugely important role in catalysing competition and product innovation across the region.

## Electronic Money Institutions Defined

EMIs are a well-established part of the financial services ecosystem in Europe, but the role they play in the market is often misunderstood. A more specific definition is provided in the box below, but EMIs are best considered as a class of regulated financial institution that provide digital (electronic money) payment services to their clients. While EMIs are not banks, their services can be bank-like in many respects; EMIs today support a wide range of different products and services to customers. Examples include corporate payment services, merchant accounts, and funding for third party wallets.

In some cases, EMIs serve their end customers directly, and there are many examples of providers with direct B2B or B2C propositions. In other cases, EMIs sit upstream and provide the technical capabilities for fintechs, challengers, and other providers to serve their customers. As a result, EMIs have been fundamental in shaping product innovation and change across the region.

### Defining Electronic Money Institutions (EMIs) and Electronic Money (e-money)

#### Electronic Money Institutions (EMIs)

The original Electronic Money Directive defined EMIs as “A legal person that has been granted authorisation to issue electronic money”. In other words, an EMI is a form of financial institution with the regulatory authority to facilitate e-money transactions (electronic payments) on behalf of its clients. EMIs are licensed to issue e-money up to the value of the funds deposited by clients. This can then be used for transactions.

#### Electronic Money (e-money)

The European Central Bank defines e-money as “An electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions”. E-money products can be hardware-based (with the value stored on something like a plastic card) or software-based (such as a digital wallet or other stored value account).

## A Brief History of EMIs

The concept of EMIs in Europe was first formalised in the Electronic Money Directive (EMD) in 2000. This was largely a response to the range of new payment products and electronic purses that were developed through the 1990s,

as well as the rapid growth of the Internet and digital commerce. While it was initially thought that only fully licensed credit institutions (i.e., banks) should issue these products, discussion grew around the merits of creating a narrower licence aimed at smaller providers who could specialise in issuing e-money products.

The EMD was designed to provide a harmonised regulatory framework across EU member states. As well as setting a level playing field to stimulate competition, it outlined the licencing requirements and safeguards for consumer protection. At the time, the scope of e-money was quite limited and was restricted to value stored on physical devices, mostly smart cards.

In 2009, the Second EMD (2EMD) was introduced to improve on the original EMD and help to further develop the e-money sector. The most important changes to the regulatory framework were:

- The definition of electronic money was expanded to include monetary value stored remotely, and not just on a physical device, such as a card.
- The scope of e-money services was expanded to include electronic money issued in any form, including digital or virtual currencies.
- Tighter authorisation requirements were introduced, including changes to the requirements for the regulation and supervision of EMIs.
- To safeguard customer funds, the 2EMD required that customer funds were kept fully separate from the EMIs own funds.
- Passporting was introduced to enable an EMI licensed in one EU member state to offer services in others.
- Anti-Money Laundering (AML) and Counter-Terrorise Financing (CTF) requirements were introduced for EMIs, introducing obligations for customer due diligence, record-keeping, and reporting suspicious activity.

The guiding aim for the 2EMD was to support further product innovation and competition in the e-money space. This has ultimately underpinned the growth of fintechs and challengers by providing them with a mechanism for offering payment services without having to become fully licensed banks or to partner with a bank.

EMIs are licensed and monitored by the relevant national authority in a given jurisdiction. In the EU, passporting rules mean that an EMI licensed by the national regulator in any member state can offer services across the EU-27 markets. EMIs also exist in the UK and are regulated by the Financial Conduct Authority (FCA).

## Key Differences Between EMIs and Banks

One of the reasons for the growth of the EMI sector is that they can offer—or enable partners to offer—propositions that are functionally very similar to bank accounts. These include holding customer funds; initiating and receiving payments, including direct debits and cross-border transactions; and issuing payment cards. However, the licencing of EMIs is very different to that of a bank, and there are important differences in the services that each can offer.

EMI licences are less onerous to obtain and come with lighter capital and reporting requirements than for a bank. As an example, the capital requirements for an EMI start at around €350,000, while a full banking licence requires capital of at least €5 million.

And while both banks and EMIs have regulatory reporting requirements, the ongoing supervision differs. For example, in the UK, banks are regulated by the Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA). The PRA has examiners who look closely at the banks' operations and records and make it difficult for a bank to take certain types of risks. This type of bank examiner regime does not exist for EMIs that are supervised by the FCA. As one of the interviewees told us:



The UK banks effectively have two regulators breathing down their necks, and the PRA has the reputation of being much stricter than the FCA on innovative models such as Banking-as-a-Service. So, while banks can claim they are under higher level of scrutiny and therefore less likely to become unstable, their risk appetite is also likely to be more conservative. Under FCA, EMIs have more freedom to debate the trade-offs of risk exposure and try out new models.

CEO of an EMI

EMIs are also narrower in terms of the range of services that they can provide. The intent is to align the regulatory requirements with the risk that an EMI can pose to customer funds and the wider ecosystem. The 2EMD is clear that issuing e-money does not constitute a deposit-taking activity. The rationale behind this is that e-money is designed to be a surrogate for cash, and any funds held by an EMI should therefore only be for the purpose of making payments. In other words, customers should not be using EMIs to 'save' or build deposits.

As a result, EMIs are explicitly prevented from offering any form of return on the funds held on behalf of customers. This is a clear distinction from a bank, which can pay interest on balances in credit.

Another significant difference between the institutions is that banks can perform maturity transformation by using their deposits base to offer loans to their customers. EMIs cannot extend credit to customers themselves, although they can partner with a credit institution or a marketplace if they want to offer credit products.

Figure 2 provides a comparison of selected similarities and differences between EMIs and banks.

**Figure 2: Selected Similarities and Differences Between EMIs and Banks**

		EMIs	Banks
<b>1</b>	Difficulty of obtaining licence and ongoing regulatory supervision	Lower	Higher
<b>2</b>	Capital requirements	Lower	Higher
<b>3</b>	Holding customer funds	✓	✓
<b>4</b>	Issuing payment cards	✓	✓
<b>5</b>	Receiving payments (domestic and cross-border)	✓	✓
<b>6</b>	Making payments (domestic and cross-border)	✓	✓
<b>7</b>	Paying interest on deposits	✗	✓
<b>8</b>	Offering credit and investment products	✗	✓
<b>9</b>	Government-backed deposit protection	✗	✓
<b>10</b>	The need to safeguard customer funds	✓	✗

Source: Celent

## Introducing Safeguarding

One of the important differences between banks and EMIs is that, unlike with banks, customer funds held by EMIs are not covered by regulator-backed deposit protection schemes. For example, should a UK-authorized bank, building society, or credit union fail, the Financial Services Compensation Scheme (FSCS) covers each customer for the first £85,000 of any loss per institution (rising to £170,000 for joint accounts). Equivalent protection is offered across the EU under national deposit guarantee schemes (DGS), under which customer funds are protected up to a value of €100,000 (or local currency equivalent). This protection is provided automatically and immediately in the event of a bank failure, with no requirement for a customer to make a claim. In both cases, these schemes are funded by an annual levy on the banks themselves.

These protection schemes do not extend to funds held with EMIs. Instead, the regulators require that all customer funds kept with EMIs must be safeguarded. That means there must be a mechanism which would ensure that should an EMI (or fintech client of an EMI) fail, customer funds should be returned in full.

The regulatory principle behind safeguarding is to balance the relatively light regulatory regime for EMIs by having tighter requirements around the protection of customer funds. Safeguarding reduces the risks for customers and has therefore been important in driving the growth of new entrants and product innovation in Europe. At heart, this comes back to the design of EMIs, which is to enable greater competition in the market for payment services.

## Safeguarding in Practice

There are two primary ways that an EMI can perform safeguarding. The first is the **segregation method**, under which client funds are held separately from the assets of the business. This cannot be a virtual exercise, and even cash must be kept physically separate from the banknotes and coins under the ownership of the EMI. This separation must take place through the business day, and no co-mingling of funds is allowed overnight. Detailed records must be kept of the holdings for each individual customer, and some EMIs use virtual account structures for this purpose. Also, an additional capital buffer is often required (typically 2%) to cover the administrative costs of winding down a failed EMI.

The most common approach taken under the segregation method is to use a client money account at a licensed credit institution (i.e., a bank) or a central bank, where this is available. EMIs are free to hold these accounts with multiple banks and this is becoming more common, particularly in those cases where the funds received are from customers in different countries and currencies. In addition, some national regulators require that EMIs active in their jurisdiction maintain customer safeguarding accounts with a bank also in that country. Others (such as De Nederlandsche Bank) go further, and mandate that client money accounts are held under a trust structure with a separate legal foundation.

Alternatively, safeguarded funds can be invested in secure liquid assets placed in a separate account with a licensed credit institution. The choice of assets open to an EMI is typically guided by the national regulator but would likely include bonds and money market funds.

The second approach that can be taken to safeguarding is the **insurance or guarantee method**. Rather than holding funds on deposit, the EMI can take appropriate cover from an authorised insurer or credit institution for the full value of the relevant client funds to be safeguarded. In the event of the failure of an EMI or a fintech/challenger that an EMI provides services to, the proceeds from the insurance policy or guarantee would cover the value of customer funds at risk.

The insurance policies must also contain sufficient headroom to allow for variation in the value of safeguarded funds. As a result, this method may not be suitable for EMIs that see large fluctuations in the value of customer funds held.

All EMIs are required to have an independent annual audit of their safeguarding provisions, and national competent authorities must be informed of any material change to the approach taken (including changing or adding new providers). In addition, the responsibility for safeguarding rests with the EMI, even where they are providing the capabilities for partners to offer payment services to customers.

## Safeguarded Deposits: Sizeable and Growing Market

As the EMI sector has grown and matured, the value of safeguarded funds is now considerable.

**Celent estimates that the customer funds safeguarded by EMIs in the EU and the UK almost doubled in the last four years to over €35 billion in 2022.**

The second half of the 2010s saw a strong acceleration in the number of EMIs operating in Europe, with the UK and Lithuania witnessing a particularly high number of new EMI authorisations, and Ireland, Malta, and the Netherlands also notable in recent years. There are now just under 600 EMIs across Europe; the UK is the largest market with just under 250 EMIs, although Brexit forced dual registration for EMIs active in the EU and the UK. Also, there are around 80 EMIs in Lithuania, which has emerged as a major regulatory hub for EMIs within the EU.

However, the number of new EMIs itself is not a strong indicator of relative size of the sector in terms of market share. While new authorisations have been high in recent years, the number of EMIs closing (through acquisition, administration, or suspension) is also notable—78 EMIs had authorisation withdrawn across Europe (UK and EU) over the last five years.

Additionally, the largest players in the sector demonstrated the strongest growth in terms of customer numbers, payment volumes, and assets. While not as concentrated as the more mature banking industry, for example, the top 10 EMIs in the UK have over 70% of the sector's assets—with a long tail of much smaller EMIs, which increases the risk of a single point of failure. Even within the larger EMIs, individual growth has often been highly volatile on a year-over-year basis.

While the growth in registered EMIs is telling, we believe the value of customer funds safeguarded by EMIs would be a better metric to reflect the growing size and impact of EMIs across Europe. There is some reported data on this, such as by the European Central Bank as well as some national Central Banks; Bank of Lithuania is the exemplar here. However, detailed and recent data is relatively sparse, despite significant reporting requirements for EMIs to local regulators.

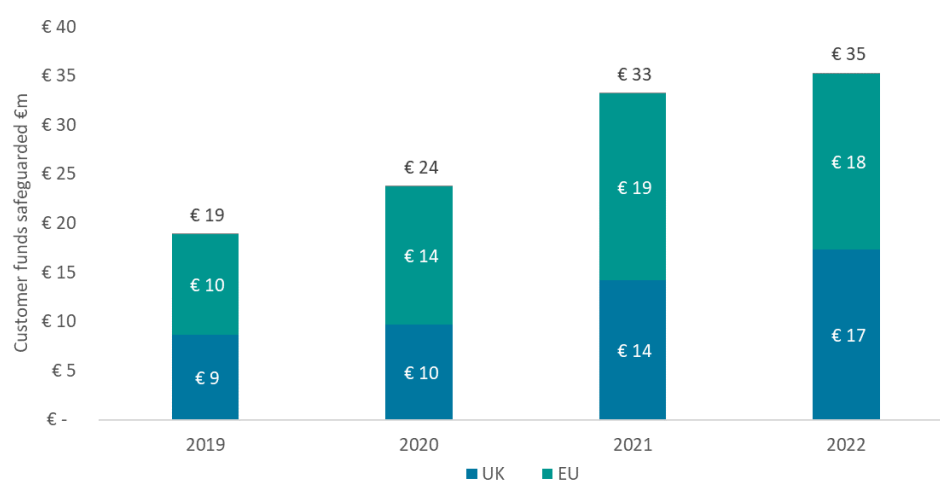
Therefore, to estimate the value of customer funds safeguarded by EMIs, Celent has analysed the reported regulator/central bank data, where available, and the financial reports of the top EMIs across Europe, which have driven the market in recent years. Based on this, we have modelled growth of safeguarded customer funds by EMIs, reconciling differences between national and EU-level reporting, and calculating 2022 figures, leveraging latest financial data from the EMIs themselves.

Given many customers will primarily use EMIs for transactions rather than balance holding, the value of payment transactions conducted by EMIs is typically many multiples higher than the end-of-day balances of outstanding customer electronic money. Ratios here vary significantly by EMI, depending on services offered as well as the customer base targeted (such as consumer or SME).

Conversely, the total amount of customer funds to be safeguarded is generally slightly higher than average outstanding balances, as EMIs need to protect funds in transit as well as funds received, plus make an allowance (typically 2%) to cover potential unwinding costs, should they go into administration.

Considering these factors, Celent calculations for customer funds safeguarded by European EMIs in recent years is shown in Figure 3. We break out differences in growth between the UK and EU given the size of the UK EMI market and the fact that these are now separate regulatory areas. The UK figures are based on a constant 2022 exchange rate to illustrate underlying growth.

**Figure 3: Safeguarded Customer Funds in UK and Europe, 2019–2022**



Source: Celent

Overall, customer funds have grown strongly in recent years, with the European total increasing from close to €19bn in 2019 to reach just over €35bn in 2022, a 17% CAGR, with the market almost doubling in only four years. That said, while this recent performance continues a longer-term trend extending back to 2010, sector growth is often volatile on a year-on-year basis, particularly at an individual country level. This reflects both economic conditions, but perhaps more significantly developments within the EMI and banking sectors, as the wider industry and regulatory environment has evolved.

A good example here is evident in the decline with EU EMI customer funds in 2022 over 2021. This is primarily driven by the shift in Revolut Payments' regulatory status from an EMI to banking licence, which took place at the end of 2021 (for Revolut's EU rather than UK regulatory entity). Given the prominence of Revolut, the EMI customer funds in Lithuania declined from €5.6bn in 2021 to €1.9bn in 2022, even though the remaining EMIs in this market saw average outstanding electronic money levels expand by around 24%. What will happen in 2023 and beyond will depend on how the sector matures and deals with setbacks and tightening regulatory scrutiny.

# THE TURBULENCE IN THE SECTOR DRIVING INCREASED REGULATORY SCRUTINY

---

Until relatively recently, the fintech sector in Europe was extremely buoyant. However, the market has faced several challenges in the past 18 months or so, and conditions are now far tighter. Regulators are putting increased pressure on EMIs and their clients to demonstrate safety and resilience, including approaches to safeguarding.

## Tighten Your Seatbelts

Until relatively recently, there seemed to be a steady flow of fintech startups in Europe looking to enter the value chain and make use of investor funding. Readily available investment accelerated the growth in the number and variety of fintechs in the market and helped create several new 'unicorns'.






However, the market has faced several challenges in the past year, and conditions are now far tighter. The impact of the pandemic and more recent political challenges in Europe have caused many difficulties for this sector, but arguably the most damaging has been the impact on the availability of funding. To illustrate the scale of the challenge, Finch Capital estimated that fintech funding in Europe in the first half of 2023 had fallen by 70% compared to the same period in 2022. M&A valuations and deals were also down, as investors took a more wary approach to this sector.

Investor expectations over the timeline and scale of returns, coupled with rising interest rates, have put significant stress on many business models. EMIs, Banking-as-a-Service (Baas), and fintech players have been heavily affected in some cases, which has caused a ripple effect across the market. Some have been forced to adjust their business plans to prioritise revenue over customer growth, while others have had more difficult challenges to overcome.

However, it is not just fintechs and EMIs that can run into trouble; the last 12 months also saw several bank failures in both the US and Europe, further shaking confidence in the sector. Table 1 on page 15 summarises a few examples of players that recently had to face challenges, with all information coming from reports in the public domain.



**Table 1: Examples of FI Players Facing Challenges**

Company	Description
	In April 2023, Central Bank of Ireland imposed “nil growth cap” on PFS Card Services Ireland, the Irish subsidiary of EML Payments, an Australian company. This was followed by the UK FCA also raising concerns and requesting Prepaid Financial Services Limited (PFS UK), the EML’s UK subsidiary, to “temporarily cease onboarding new customers, agents and distributors” in November 2023. At the end of November, the EML stock price lost nearly a third of its value after the company’s strategic review revealed that “its remediation efforts had been unable to satisfy the regulator” in Ireland.
	In October 2023, the UK FCA asked Modulr, the UK-based EMI and embedded payments platform, not to onboard any <i>new agent and/or distributor</i> without its prior written consent. The company was reported saying that after a period of growth it had to ensure its “governance, systems and controls reflect the scale of the business and regulatory requirements”. However, this restriction does not impact any of the existing partners, the onboarding of <i>new direct customers</i> , or growth of the company’s European business.
	In March 2023, Banking-as-a-Service (BaaS) provider Railsr, formerly known as Railsbank, had been acquired by a shareholder consortium and went into administration. This followed a period of instability in which Railsr faced several financial and regulatory challenges, including being ordered by the Bank of Lithuania to stop onboarding new clients and return to customers funds held in its Lithuanian-regulated entity (PayrNet). In July, the PayrNet EMI licence in Lithuania was revoked. However, since the acquisition and re-capitalisation, Railsr has emerged as a more stable entity and announced \$24 million in new funding in October 2023.
	Another BaaS provider, Solaris, formerly Solarisbank, which services many fintechs in Europe, ran into problems in late 2022. In December, BaFin, the competent authority in Germany, imposed a ban on Solaris onboarding new customers without its approval. In September 2023, the FT reported that a large client was considering new providers for its co-branded credit card proposition due to concerns around Solaris capitalisation. Most recently, in November 2023, Contis, the UK-based EMI that was acquired by Solaris, was fined €840,000 by the Bank of Lithuania and was requested to improve its anti-money laundering procedures.
	Also in March 2023, Silicon Valley Bank (SVB) became the largest US bank to fail since the 2008 financial crisis. As a specialist provider to the fintech sector, it was heavily exposed to the success of that ecosystem, and the same was true in reverse. Rumours over a lack of liquidity at the bank led many depositors to withdraw their funds in the US, which quickly led to the collapse of the institution. In Europe, the impact was most keenly felt by customers of SVB’s UK arm, which was swiftly acquired by HSBC under the direction of the Bank of England. Former SVB customers in higher risk business areas were widely expected to look for new banking partners.

Sources: public announcements and press coverage

## Regulators Sharpen Focus on Safety and Resilience

These challenges have brought the issues of safety and operational resilience to the top of the agenda not just for EMIs, fintechs, and banks, but also for regulators. They are putting a renewed emphasis on ensuring that all market participants have robust operational resiliency, fraud and AML controls, safeguarding of customer funds, and if it comes to that, the plans to be unwound efficiently.

### The UK FCA's 'Dear CEO' Letter

In March 2023, the UK's FCA wrote to the chief executives of payments firms under its jurisdiction one of its 'Dear CEO' letters to draw their attention to several concerns, given the turbulence in the sector.

The letter highlighted the need to ensure the safety of customers' money, maintain financial system integrity through increased fraud and AML controls, as well as compliance with customer duty provisions.

Safeguarding was addressed at length, and the letter identified several common failings, which it stressed needed to be put right:

- A lack of documented processes for identifying which funds needed to be safeguarded.
- Inadequate processes around reconciliation to ensure the correct sums were being safeguarded.
- A lack of due diligence and acknowledgement of segregation from the credit institutions providing safeguarding accounts.

In addition, the FCA also highlighted the importance of EMIs having clear policies and plans in place to wind down businesses if they were unable to continue trading.

### FSCS Protection Extension to Safeguarded Funds

Also in March, there was a further change to the UK's rules around safeguarding. Following the collapse of Silicon Valley Bank and Credit Suisse, the Prudential Regulation Authority (PRA), which regulates credit institutions, announced that the rules around depositor protection would be extended to cover authorised payment institutions, including EMIs. Therefore, should a bank that is safeguarding customer funds for an EMI fail, the customers of that EMI will each be protected up to the value of £85,000.

While a welcome step, there are some limitations. Firstly, FSCS protection only applies when there is a failure of *a safeguarding bank, but not if an EMI or its fintech clients fail*.

More significantly, this change may drive the need for full transparency in the way EMIs handle safeguarding. Today, this is becoming an increasingly complex issue, as an EMI may have multiple safeguarding partners across different jurisdictions, while FSCS protection only covers deposits at UK banks. An EMI may also use insurance or investments to cover some or all of its safeguarding obligations.

Given this, it may be difficult for an EMI to track exactly which funds benefit from FSCS protection. Furthermore, should a bank fail, the customer-level cap on FSCS protection will still apply, irrespective of whether the funds were deposited by the customer directly with the bank or safeguarded via an EMI. Therefore, to fully understand their risks and protection, a customer would need to know exactly how each EMI with which they have a relationship safeguards its funds. Given that a single customer may have multiple accounts with several EMIs or fintechs, all of which may be using the same bank to safeguard their funds, this could be a considerable challenge.

### Further Potential Changes on the Horizon in the UK...

In January 2023, the UK government announced a review into the Payment Service Regulations (PSRs) and opened a period of consultation into potential improvements. This phase concluded in April 2023.

#### What is a Payment Institution?

In the second payment services directive (PSD2), Payment Institutions were defined as “A legal person that has been granted authorization to provide and execute payment services throughout the European Union”. These payments are drawn on a payment account held at a licensed entity.

Pis and EMIs have many similarities, but the latter is the only entity that is licensed to issue electronic money.

Safeguarding was highlighted as an important issue to be addressed, and it acknowledged that recent experience shows there is room for improvement. There have been cases in the UK where court proceedings have been required for customers to have their funds returned following an insolvency. In these instances, refunds have taken long periods to be resolved and customers have been forced to shoulder losses, due to the costs of administration not being covered by the remaining assets of the company.

While the UK government did legislate in 2021 to establish the Payment and E-Money Special Administration Regime to accelerate the distribution of funds, this has not fully addressed the needs of customers and insolvency practitioners. The review will therefore examine whether

the FCA should develop a more stringent framework for safeguarding the winding up of insolvent firms.

#### ... And in the EU with PSD3 Looming

In the meantime, regulators in the European Union are also actively looking to strengthen the frameworks around both safeguarding and what happens when an EMI becomes insolvent.

The regulatory framework around EMIs is expected to see some changes as part of the new Payment Services Directive (PSD3). The draft text was published in June 2023, and includes several changes to the regulatory frameworks for Payment Institutions (Pis) and EMIs.

One of the biggest shifts will be the incorporation of 2EMD into PSD3, which will see the repeal of the 2009 regulation. In a move designed to streamline the regulation of payment services in Europe, EMIs will be classified as a sub-category of Payment Institution. Those Pis and EMIs already authorised will need to obtain a new licence under PSD3, and it's expected they will have 18 months from the implementation of PSD3 to submit their application to the respective National Competent Authority (NCA).

The scope of the proposed PSD3 is broad, but there are several aspects that are particularly relevant to the theme of EMI stability and resilience. There will be new requirements for EMIs (and PIs) in at least four areas:

- **Winding up plans** – Detailed plans must be provided to the national competent authority to outline how the EMI could fail in an orderly manner if the situation arises. This must be appropriate to the size and business model of the PI.
- **Business continuity** – Plans to withstand and recover from a range of technology-related disruptions and threats need to be in place and be fully compliant with the Digital Operational Resilience Act (DORA).
- **Security** – EMIs must undertake a detailed risk assessment covering the risk of fraud and the misuse of sensitive and personal data.
- **Other applications** – An EMI must also alert the competent authority of any plans or submissions for authorisations to other regulators in other EU states.

The rules around safeguarding will remain largely unchanged. It is expected, however, that the EBA (Euro Banking Association) will develop regulatory technical standards on safeguarding requirements.

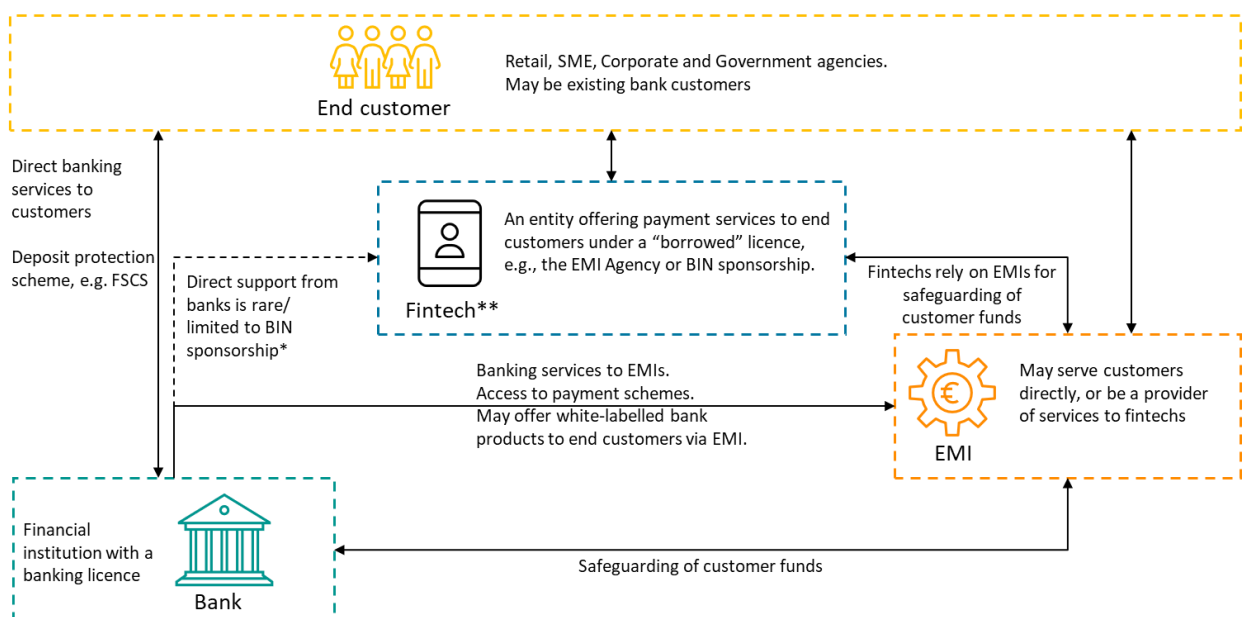
# SELECTING AND MANAGING PARTNERS IN TURBULENT TIMES

The financial ecosystem has become increasingly open and interconnected, and problems in a single node can ripple through multiple other providers. Players across the industry are evaluating whether their networks of partners and service providers have the necessary stability and resilience to survive this period of turbulence.

## The Complexity of Ecosystem Relationships

While it may appear that banks, EMIs, and various fintechs are direct competitors, the reality is more nuanced. On the one hand, these providers often do compete for customers and engagement. However, this is also a highly connected ecosystem in which the services provided by banks are fundamental to the ability of EMIs, fintechs, and other challengers to operate. Indeed, from the bank perspective, as the segment continues to mature, it represents a growing opportunity to increase revenues and exposure to what is a dynamic market.

**Figure 4: Relationships Between Banks, EMIs, and EMI Customers**



\* BIN sponsorship enables fintechs to offer cards by leveraging the issuing banks' direct membership with the major schemes, such as Mastercard and Visa  
 \*\* Fintechs that provide technology solutions to banks are excluded from this chart

Source: Celent

As Figure 4 demonstrates, there are few cases in which a fintech or EMI can offer services without there being a bank involved somewhere in the value chain. In addition to providing safeguarding services to EMIs, banks also provide credit and banking services to the ecosystem. In some cases, banks also act as sponsors or agents for access to the account-to-account payment schemes in a country.

In other cases, banks provide these scheme-access services to payment service providers (PSPs), which then provide these services in turn to the EMI or fintech. In all these examples, existing banks are already closely involved in supporting the services offered by these providers.

However, not all banks are as directly involved in this ecosystem as others. Those that are active in supporting EMIs and fintechs are typically those with the risk appetite to work with this market segment. Even then, the pool of banks that want to work with EMIs that have exposure to certain business areas, such as cryptocurrencies and digital assets, is smaller still.

It should also not be forgotten that some fintechs underpinned by EMIs also count banks as their customers. Just to pick one example, Barclays announced a partnership with TransferMate in May 2023 to distribute the EMI's cross-border payment services to its customers. For the purposes of this research, we focused on the services that banks provide to EMIs and fintechs rather than the other way around.



How well the ecosystem will function depends on how diligent people are on their risk mitigation. There can be a domino effect as the ecosystem is so interconnected.

A pan-European EMI

We kicked off this research seeking to understand a series of questions about how various players select and manage partners, such as:

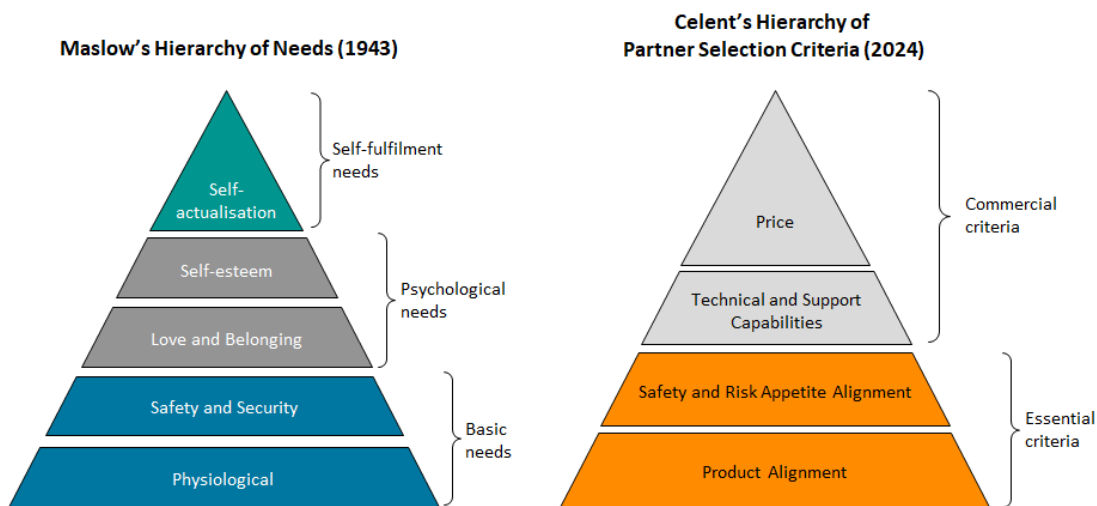
- What are the key criteria when evaluating partners? Have those criteria changed in recent times?
- What is their partner selection horizon? Do players typically select partners on a short-term, medium-term, or long-term basis to start with? How often do they review partners? Do the current market conditions and potential risk of contagion change their attitudes?
- How do EMIs approach safeguarding? How do they and their customers view safeguarding—as a hurdle barrier in selection (i.e., needs to be demonstrated, but a risk tick box), or as a strategic element for them (i.e., used as part of customer value proposition)? How important is deposit insurance, such as FSCS protection?
- What are pros and cons of EMIs? How much of an issue is the inability of EMIs to offer interest-bearing accounts?

As part of the research for this report, Celent interviewed over a dozen players in the industry, including banks, EMLs, and fintechs/EMI clients, who collectively offer a range of consumer products or target businesses/commercial customers. We promised that the individual discussions would remain confidential, and nothing would be attributed to specific identifiable interviewees. The rest of this section summarises the research findings.

### Celent’s Hierarchy of Partner Selection Criteria

Anyone who remembers their Psychology 101 will be familiar with Maslow’s hierarchy of needs. In 1943, American psychologist Abraham Maslow published a paper suggesting that human needs can be arranged in a hierarchy. The basic needs—physiological, such as food, water, sleep, and safety and security—lie at the base of the pyramid, while the need for self-actualisation and fulfilment is at the top. Over the years, more layers were introduced, but the key point is that the basic needs at the bottom need to be met first, before the person becomes motivated by other concerns.

**Figure 5: Maslow’s Hierarchy of Needs and Celent’s Hierarchy of Partner Selection Criteria**



Source: Celent

Our research suggests that criteria the financial players use when selecting partners can also be arranged in a hierarchy. As with Maslow’s hierarchy of needs, the layers of Celent’s hierarchy of partner selection criteria are not strictly fixed in order and may vary in importance depending on a specific situation or over time. However, we found that two **essential criteria** typically must be met first, before the **commercial** discussions can take place.

## Product and Risk Appetite Alignment Dominate Partner Selection Criteria

Before engaging in more detailed discussions, the two entities must align around the product required and being offered and be comfortable with the level of risk that the relationship would represent. Product alignment is key—if the fintech is looking for a bank-like account and the provider can only support card issuing, or if the client wants to offer savings accounts, but the provider is focused on payments, the conversations will not go any further. Product alignment matters especially in a relatively young market because not everyone offers everything; as the market matures, we would expect the importance of product alignment to decrease somewhat.

Of course, product requirements go deeper, with partners looking to align around specific needs and breadth of coverage. For example, clients want to explore questions such as:

- Can this provider offer us accounts in multiple currencies (e.g., Sterling, Euro, non-Euro currencies, such as Polish Zloty, Norwegian Krona, and others)?
- Could we get access to multiple settlement rails (e.g., Faster Payments, CHAPS, SEPA Instant Payments, non-SEPA)?
- Would supporting the expansion beyond Europe (e.g., the US) be an option?

Sometimes, early discussions about product requirements reveal lack of alignment around the risk appetite. Some banks and even EMIs have clear rules against supporting fintechs in certain industries, such as gambling or crypto. As one fintech said, “When a startup begins its journey, there are some BaaS providers who won’t want to work with you depending on the target audience and who you want to go after. So, if you want to build a crypto on/off ramp, you immediately lose a bunch of BaaS providers because of this.” Also, few if any banks are willing to engage with unregulated fintechs; most prefer to work with EMIs or PIs.



We would have loved to work with a bank, but they wouldn’t have us.

A fintech with a direct-to-consumer proposition

Other points tend to be more nuanced, and while it’s unlikely that the risk appetite between partners will be completely aligned, getting as close to parity as possible is key. For example, the onboarding model is often a bone of contention. Fintechs want to manage and offer a seamless onboarding process, even though they are not the account issuer from the licencing perspective. They don’t want to hand over the client to another process over which they have no control and ask them to negotiate another contract to access the service. From their perspective, it must be an extension of the service, not a completely new relationship: “Our clients don’t want to do brand new onboarding again if they’ve already onboarded with us.”



Furthermore, risk appetite can't be a static view. It is important for partners to understand each other's growth ambitions and road map. Understandably, fintechs change and evolve their strategies, but they must take their partners along on that journey: "If I start doing something slightly risky—for example, go after migrant workers with no credit history or electoral roll status—providers will be concerned that I would expose them to money laundering risks, etc." One of the EMIs shared with us their approach with managing risk, where they set expected minimum volumes for clients and monitor them over time. If the clients can't meet those minimums, the EMI challenges their forecasts and adjusts the risk profile.

On the other hand, fintechs might not be best equipped to assess the risk of their potential partner. As one of them said, "We try looking at it as part of our due diligence process, but it's hard. Sometimes it comes down to their size and reputation—if it's a large provider, you assume they will be around for the next few years. With smaller players, we need to be more careful—do they have a track record, can they scale, will they have enough funding?"

## Technical and Support Capabilities: Important but Secondary

Of course, other key considerations include technical capabilities and breadth of functionality, with ease of integration and quality of APIs at the top of the list of requirements. According to several providers, the importance of end-to-end functionality depends on the client. Some large corporate clients favour end-to-end functionality, "because it's only one throat to strangle if anything does go pear shaped", while more nimble companies and more price-sensitive fintechs may want to choose the components themselves.

Recent challenges faced by several providers are also causing a shift in thinking here. One way to increase resiliency for a fintech is to take on more of the operational activities themselves. For example, one fintech reminisced about the time when they outsourced all of card issuing completely to Wirecard. Then, when Wirecard collapsed, they decided to take many aspects of card issuing back in house—such as KYC/KYB processes and the contracts with card manufacturers—and partnered with the issuer processor only for transaction processing.

One key functionality that is particularly important for fintechs looking to operate across Europe is the ability to provide local IBANs (International Bank Account Numbers). The IBANs issued by banks and EMIs in some countries are considered less trustworthy than others, leading to transactions being declined, a practice known as "IBAN discrimination". In other words, if a French resident has an account with a Lithuanian IBAN, their energy company might refuse to process their direct debit because it's not coming from a local account with a French IBAN. This is against the spirit of the single payments market and is illegal under SEPA. The European Commission encourages individuals to file a complaint with the national competent authority in the country where they have encountered IBAN discrimination. However, in practice, a local IBAN today improves the chances of transaction success and is, therefore, an important criterion when choosing a partner.

## Pricing: Decreasing in Importance

Few would want to admit that price doesn't matter in commercial transactions, but ultimately it becomes a secondary consideration.



Price is important, but you can always negotiate around price and try to squeeze the providers. If they don't have the right product, technical capabilities, or don't look safe, price becomes meaningless.

A fintech with a direct-to-consumer proposition



Price is always mid-to-low in importance, because by then you either qualified yourself or not. And if the client can offer volumes, we will look after them.

A pan-European EMI

Typical arrangements between providers and clients involve a monthly fee and a unit price (transaction fee). Some providers charge higher monthly fees (e.g., £5–10k) and lower transaction fees (e.g., £0.05–0.10), while others may be charging smaller monthly fees (e.g., £200) but higher transaction fees (£0.20–30 per payment). Unit price matters especially for those that build propositions which compete with other well-known alternatives, e.g., open banking-enabled payments versus cards. However, if a provider has developed a specialised proposition, some clients value that more than a similar but generic proposition and are prepared to pay more.

One of the recent changes in the macroeconomic environment has been **higher interest rates**. EMIs typically get a yield on their safeguarding accounts from the bank partner but cannot pass that on as interest on funds to their clients. This has an effect of reducing the importance of pricing for some EMIs when negotiating deals with their bank partners: "We could try and haggle around monthly fees or transaction fees, but the reality is that the revenue we get from client funds outweighs our costs."

We would have expected to see EMIs getting questions from their clients about their inability to pay interest on funds stored with them. However, some EMIs said the opposite was true: clients were concerned in the past whether they would be charged a negative interest, but have not been asking for interest payments now that the rates are high: "We've seen maybe a couple of questions in all the RFPs over the last few years. It's not a day-to-day request." On the other hand, others did say they were trying to compensate their clients by offering rebates on the unit price and other incentives. At the same time, they

are wary of establishing dangerous precedents for when interest rates do come down.

## Relationships: Plan for Long-term, Prepare to Change

The relationships that fintechs and their partners strike tend to be long-term; both sides acknowledge the disruption to the business if they have to change partners. However, both sides regularly review the partners that they work with and assess whether anything has changed—such as the partner risks or commercial logic—that could merit reassessing the relationship.

Having said that, several fintechs told us that they are either planning or already in the process of adding more partners for several reasons. One reason to add a new partner is to increase coverage (e.g., new currencies, new functionality) or add new products (e.g., card issuing in addition to bank accounts). Another reason is redundancy: considering recent challenges by some of the large providers in the market, fintech clients are keen to ensure they have backup. “We don’t want to be over-reliant on any single partner, no matter who they are—an EMI, an investment broker, and so on.”

Of course, additional partnerships come at a cost in terms of managing those relationships, so the number of partners tends to remain small. Also, fintechs are committed to not expose any additional complexity on the back end to their clients and would seek to “abstract the service on our end, so that for the client, it doesn’t matter if the account comes from provider A or B, or both”.



We want to have no more but also no fewer than two safeguarding partners.

An EMI

Even when fintechs are unhappy with their current providers and add new partners, they tend to keep the relationship with the existing provider open but minimise business with them. Banks and EMIs should watch out for any reduction in their volumes with fintech clients, as it may indicate a sign of trouble in their relationship, rather than necessarily the fintech’s health.

Another reason why relationships might be terminated or curtailed is when EMIs try to get a better grip on their risk management and client safeguarding processes. It is not uncommon for an EMI to be partnering with another EMI, creating a nested relationship, where EMI One might be relying on EMI Two, which is the one that safeguards the clients’ funds with the bank. That means that EMI One is relying on the processes and controls of EMI Two to fulfil their obligations to the regulators.

Conversely, EMI Two is relying on EMI One’s onboarding practices and judgement when signing up customers: “There’s always a danger here that there’s money laundering, so we need to be comfortable in the risk processes they have, as well as our ability to onboard the nested flows.”



You don't know how many times the flow is nested. You want to know the end customer, as your licence is at risk. The question is whether what you do puts your licence at risk.

Large pan-European EMI

An agency model—when the EMI is “lending its licence” to a fintech for them to “piggyback on”—is even riskier. Given the sharpened focus of regulators on risk management, some EMIs are finding such practices increasingly harder to justify.

By the way, that interconnectedness of the system means that competitor failures are not celebrated. While some might think reduced competition is good and any competitor failure means an opportunity to cherry pick some of their clients, the reality is that a competitor having troubles casts the dark cloud on the entire market and raises doubts about all EMIs. Also, some EMIs have suffered because of their clients, which is why others are not always rushing to onboard them—while it might represent an increased revenue in the short-term, it might also bring a heightened risk.

## Safeguarding Is Getting Increasingly More Attention

### **Clients Care More about Safeguarding, Forcing EMIs to Act**

Overall, the topic of safeguarding has certainly increased in importance in recent years. In the past, many told us it was treated as a perfunctory task, something that had to be done at the end of the day for the outstanding balances. Now, EMIs are keen to improve their safeguarding practices, aiming to cover the balances throughout the day and protect the funds in real time, as soon as they come in. One of the banks we spoke to during our research said, “We’ve been responding to RFPs with explicit questions on how we can help the client improve their safeguarding approaches. It just wouldn’t have been there a few years ago.”

Understanding how their partners perform safeguarding is also critical for fintechs. All of them said that during the due diligence they pay close attention to safeguarding practices of their partner, seeking to understand exactly how they do it, with what banks. Auditor reports can be helpful to further validate those details.

Some fintechs and clients go a step further and seek to influence their EMIs’ partners, requesting that they work with specific banks. Larger commercial clients especially are increasingly asking EMIs questions about where their funds are, with some demanding that EMIs demonstrate that they can partner with large Tier 1 banks. This in turn is even starting to influence the EMI’s licencing decisions. As one EMI explained: “We currently have a European licence in Lithuania, which we passport into Europe. However, several Tier 1 banks are happy to work with our UK licence, but not the Lithuanian one. In our opinion, this is a bit unfair, as Lithuania has a strict regulator, but we have now applied for and expect to have a Dutch licence from the end of this year.”

Many fintechs that work with EMIs who safeguard with commercial banks view it as a key part of due diligence and establishing trust with partners, but not as a differentiator with customers. Others, while offering a financial product, lead with software; as a result, their clients tend to focus more on the software product rather than the nuances of the financial product and funds safety. On the other hand, those whose partners can demonstrate that their client funds are stored at the central bank, such as the Bank of England, do emphasise that point to customers and view it as a strategic differentiator.

### **Safeguarding Vs. Deposit Protection Schemes**

The degree to which FSCS (and similar) protection matters depends on the end customer and the product. If it is a consumer account, and especially, for savings accounts, it is perceived as important.



We constantly have a debate internally to what degree our customers understand and care about FSCS protection, but we know if we could add that badge to our website, we would do it in an instant, as we think it matters.

A consumer-oriented fintech

However, for payments accounts which might see a large volume of transactions but relatively low balances, or for business accounts where balances regularly exceed the £85k limit, the protection scheme is much less relevant.

Also, it is important to remember that the reason schemes like FSCS exist is because banks lend the customers' money and take risks, which EMIs can't do. If EMIs manage their business risks and safeguard customers' money well—admittedly, big “if's”—then safeguarding arguably can offer more protection as it does not have any limits.



The education piece hasn't been done successfully. If your funds are safeguarded, you have more protection than under the FSCS agreement, which is £85k. If you're safeguarded with an EMI, 100% is ringfenced regardless of the amount. Customers think that holding with a fintech is less protected than with a bank, but it's not the case as you get it all back.

A consumer-oriented fintech

## Finding Safeguarding Partners

We also asked EMIs how they select their safeguarding partners. Turns out, they are not spoiled for choice—the options are somewhat limited, as not every commercial bank offers designated client money accounts needed to ringfence safeguarded funds. The banks with client money accounts that are able to offer safeguarding services include large global banks like Barclays, JP Morgan, Citi, and HSBC, or specialist institutions with a banking licence, such as ClearBank in the UK or LHV in Estonia.

As one EMI described to us:

“We went with what is recognised as a good solution in the market. There are not that many providers who are tech friendly, with good APIs, willing to work with EMIs, and where you can easily get onboarded early on. The conversations with larger global banks tend to be slower, and their onboarding is more challenging<sup>1</sup>; some of them currently simply don’t work with EMIs licensed in certain European countries. Some banks have a very siloed approach. For example, the European team of a pan-European bank could not comment at all about what they could offer in the UK, while we wanted a partner that could support us in both the UK and the European Union. Others have been scolded by the regulators too many times in the past and have scaled down their risk appetite so much that they couldn’t support some of our payment flows. They suggested we use them for safeguarding, but work with others for payments clearing, which for us again means dealing with multiple partners.”

## EMIs Vs. Banks as Partners

Similarly, we asked fintechs and other EMIs why they chose to work with an EMI rather than a bank. Once again, flexibility and willingness to take more risk dominated the responses. (See Table 2.)

**Table 2: Interviewee Responses on Why They Prefer EMIs over Banks**

EMI Advantages	Comments
<b>Risk Appetite/ Tolerance</b>	EMIs are often willing to take more risk than banks, enabling them to serve a broader range of customers. Risk appetite/tolerance varies not only by individual players, but also by the underlying regulators. For example, the Bank of Lithuania is perceived by many to be more tolerant to risk-taking, than say BAFIN in Germany.
<b>Nimbleness of the licence</b>	The European EMI licence allows providers to passport across Europe faster, whereas the banking licence might be more restricted. For example, one provider told us that with their German banking licence, they can support clients in Germany, France, Spain, and Italy, but not some of the other markets, as the regulators might require the bank to have local presence or impose other criteria. The main reason is that banks are allowed

<sup>1</sup> Another EMI said it took them three years to get onboarded with a Tier 1 bank, and they have a large team internally dedicated to deal with the bank’s compliance requirements.

	to do maturity transformation by taking on risk, whereas EMIs can't do that, so the systemic risk of an EMI or a PI is lower than that of a bank.
<b>KYC optionality</b>	When working with an EMI, clients have the option of who does KYC. They can either use the service provided by the EMI, or if they already have an internal compliance function and a connection to the KYC solution provider, they can choose to use those. In that case, the EMI would audit the clients on a regular basis, e.g., every 6-12 months. Conversely, most bank regulators insist on banks doing KYC themselves on behalf of their clients.
<b>Lack of product and technical fit, organisational silos</b>	<p>"We don't see many banks offering good virtual accounts functionality. Also, incumbent banks can be very inflexible in their processes and technology and find it very hard to keep up." (Open Banking provider)</p> <p>"The reason we built this business is because, in the past, we wanted to build our own solutions but couldn't get access to tech-enabled payment services in a coordinated way through a bank. Even in large banks you have a siloed mentality. For example, the corporate cards department is nowhere near the transaction banking part of the bank, and you can't bring that together. So, before you even get to the conversation about the tech, you can't get people together organisationally. We can help clients break down these barriers." (CEO of a large UK-based EMI)</p>

## Reactions to Changing Regulatory Environment

Finally, many providers we spoke to expect the regulatory landscape in Europe to get tighter in response to recent failings of market participants. They expect that as a result, their own "due diligence questionnaire will get tightened and will become a lot more thorough", which means that the providers might want to concentrate on bigger and more established organisations, prioritising quality over quantity.

Overall, the players welcome the expected regulatory changes. In fact, some felt that regulators could also do more by providing them more specific guidance: "Sometimes we go and present [to the regulators] and all we get is, 'no further questions at this moment in time,' and you leave feeling if not quite like a criminal, then certainly questioning if you are doing the right thing here."



Anything that increases credibility in the industry in general is great. While [some proposed changes] may not make much of a difference for our clients on an individual basis, on a macro level, it will be beneficial.

A large EMI

# PATH FORWARD: CONSIDER EMIs AS KEY CLIENTS AND PARTNERS

---

We live in an age of coopetition, with the same entities competing in one area while cooperating in another. This is true for UK and European banks and EMIs, which can be both competitors and partners when capturing the embedded finance opportunity.

Banks should consider EMIs as key clients and partners in offering embedded finance:

- EMIs can help align with risk appetite by insulating banks from unregulated entities. By teaming up with EMIs, banks can deploy their advantages of a superior funding model, especially for lending, while at the same time significantly reducing their exposure to the scrutiny of onboarding and overseeing individual customers, as they ultimately belong to the EMI.
- EMIs can bring relevant technology capabilities and, especially, solutions that are tailored for specific industries.
- EMIs need banks for safeguarding, offering the opportunity—albeit not for all banks—to capture a share of those €35 billion deposits across the UK and EU.

However, as the discussion at the end of the previous section highlighted, fintechs often prefer EMIs not just because of their risk appetite. For banks to be successful in this space, they need investment and new thinking across several dimensions:

- Beefing up partner oversight, management, and ongoing monitoring capabilities. Even if EMIs assume the risk of individual customers, the portfolio exposure remains and must be carefully monitored.
- Building or acquiring the necessary technical capabilities.
- Reducing organisational silos and investing in new skills/staff in critical areas, including compliance, customer care, and technical support.



# LEVERAGING CELENT'S EXPERTISE

---

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

## Support for Financial Institutions

Typical projects we support include:

**Vendor short listing and selection.** We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

**Business practice evaluations.** We spend time evaluating your business processes and requirements. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

**IT and business strategy creation.** We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyse your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

## Support for Vendors

We provide services that help you refine your product and service offerings. Examples include:

**Product and service strategy evaluation.** We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

**Market messaging and collateral review.** Based on our extensive experience with your potential clients, we assess your marketing and sales materials—including your website and any collateral.

# RELATED CELENT RESEARCH

---

[Technology Trends Previsory: Retail Banking, 2024 Edition: Taking Agility to the Next Level with GenAI and Other Tools](#)  
November 2023

[Demystifying Virtual Accounts: New Opportunities to Drive Adoption](#)  
September 2023

[BaaS, PaaS, CBDCs, and PSD3: Decoding the Banking Buzzwords from EBAday 2023](#)  
July 2023

[Practical Advice on Maximizing Value in an Increasingly Complex Technology Ecosystem](#)  
April 2023

[What's in a Name? Unpacking Digital Wallets, Superapps, and Embedded Finance: Don't Let the Terminology Become a Distraction](#)  
January 2023

[A Primer on Variable Recurring Payments: The Next Big Thing in Open Banking?](#)  
December 2022

[The Payments Processing Opportunity for Banks: Moving Account-Based Payments from Cost Centre to Revenue Stream](#)  
December 2022

[Demystifying Embedded Finance: Promise and Peril for Banks](#)  
April 2021

## **COPYRIGHT NOTICE**

Copyright 2024 Celent, a division of Oliver Wyman, Inc., which is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. All rights reserved. This report may not be reproduced, copied or redistributed, in whole or in part, in any form or by any means, without the written permission of Celent, a division of Oliver Wyman ("Celent") and Celent accepts no liability whatsoever for the actions of third parties in this respect. Celent and any third party content providers whose content is included in this report are the sole copyright owners of the content in this report. Any third party content in this report has been included by Celent with the permission of the relevant content owner. Any use of this report by any third party is strictly prohibited without a license expressly granted by Celent. Any use of third party content included in this report is strictly prohibited without the express permission of the relevant content owner. This report is not intended for general circulation, nor is it to be used, reproduced, copied, quoted or distributed by third parties for any purpose other than those that may be set forth herein without the prior written permission of Celent. Neither all nor any part of the contents of this report, or any opinions expressed herein, shall be disseminated to the public through advertising media, public relations, news media, sales media, mail, direct transmittal, or any other public means of communications, without the prior written consent of Celent. Any violation of Celent's rights in this report will be enforced to the fullest extent of the law, including the pursuit of monetary damages and injunctive relief in the event of any breach of the foregoing restrictions.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

For more information please contact [info@celent.com](mailto:info@celent.com) or:

Zil Bareisis [zbareisis@celent.com](mailto:zbareisis@celent.com)  
Kieran Hines [khines@celent.com](mailto:khines@celent.com)  
Daniel Mayo [dmayo@celent.com](mailto:dmayo@celent.com)

#### Americas

##### USA

99 High Street, 32<sup>nd</sup> Floor  
Boston, MA 02110-2320

[+1.617.424.3200](tel:+1.617.424.3200)

##### USA

1166 Avenue of the Americas  
New York, NY 10036

[+1.212.345.8000](tel:+1.212.345.8000)

##### USA

Four Embarcadero Center  
Suite 1100  
San Francisco, CA 94111

[+1.415.743.7800](tel:+1.415.743.7800)

##### Brazil

Rua Arquiteto Olavo Redig  
de Campos, 105  
Edifício EZ Tower – Torre B – 26<sup>º</sup> andar  
04711-904 – São Paulo

[+55 11 3878 2000](tel:+55.11.3878.2000)

#### EMEA

##### Switzerland

Tessinerplatz 5  
Zurich 8027

[+41.44.5533.333](tel:+41.44.5533.333)

##### France

1 Rue Euler  
Paris 75008

[+33 1 45 02 30 00](tel:+33.1.45.02.30.00)

##### Italy

Galleria San Babila 4B  
Milan 20122

[+39.02.305.771](tel:+39.02.305.771)

##### United Kingdom

55 Baker Street  
London W1U 8EW

[+44.20.7333.8333](tel:+44.20.7333.8333)

#### Asia-Pacific

##### Japan

Midtown Tower 16F  
9-7-1, Akasaka  
Minato-ku, Tokyo 107-6216

[+81.3.6871.7008](tel:+81.3.6871.7008)

##### Hong Kong

Unit 04, 9<sup>th</sup> Floor  
Central Plaza  
18 Harbour Road  
Wanchai

[+852 2301 7500](tel:+852.2301.7500)

##### Singapore

8 Marina View  
Asia Square Tower 1  
#09-07  
Singapore 018960

[+65 6510 9700](tel:+65.6510.9700)

# Thank you for reading.

---

If you want to learn more about how ClearBank can support your business to innovate, differentiate and grow, contact us at [apply@clear.bank](mailto:apply@clear.bank).

Get in touch

