

Beyond the bank app: How banks stay strategic when the interface moves

Nicolas de Genot de Nieukerken

Director of Product, Open Banking
& Digital Wallet at SBS



Content

01. The interface is moving, but the bank is not disappearing	p.4
02. Embedded finance redistributes experience, not accountability	p.5
03. PSD3 turns compliance into an operating-model decision	p.6
04. New interfaces create variations of the same control problem	p.7
05. Build the control model once and reuse it	p.9
06. From compliance to strategic readiness with SBS	p.10

Executive summary

Banks are increasingly providing financial services through customer journeys they do not fully control. The strategic risk is not simply reduced visibility in the customer interface, but retaining the cost and responsibility of regulated execution while losing customer context, distribution influence and a meaningful role in what happens next.

That creates a second challenge. As delivery stretches across merchants, platforms, software providers and other partners, banks remain responsible for areas such as identity, fraud controls, servicing, complaints, partner oversight and regulatory evidence, even when those activities span multiple organizations.

Europe's new payment-services framework brings many of these issues into immediate focus. PSD3 and PSR introduce requirements around permissions, third-party access, fraud prevention, interface performance and oversight.

Banks can treat those obligations as isolated compliance tasks, or use the investment to build capabilities that can be reused across future partners, interfaces and propositions.

That choice will matter as account-to-account payments, recurring payment authority, shared wallets, open finance and AI-assisted transactions expand the number of ways financial activity can begin and be managed. Banks that build a consistent control model will be better placed to reduce duplicated work, preserve strategic flexibility and remain differentiated. Those that do not risk carrying the obligations of regulated execution while becoming increasingly interchangeable behind someone else's customer relationship.

01. The interface is moving, but the bank is not disappearing

Today, financial services are increasingly accessed through channels outside the bank's direct control. Customers can arrange installment finance at the point of sale, take out insurance while booking travel or secure car finance through a dealership. A small business can pay suppliers from its accounting software, while marketplaces and wallets increasingly provide the interface through which payments are initiated and managed.

[Embedded finance](#) has accelerated this shift by **integrating financial products and services directly into non-bank customer journeys**. The

bank may still provide the underlying account, payment, credit or other regulated service, but the customer interaction, product distribution and surrounding data can increasingly sit with another organization.

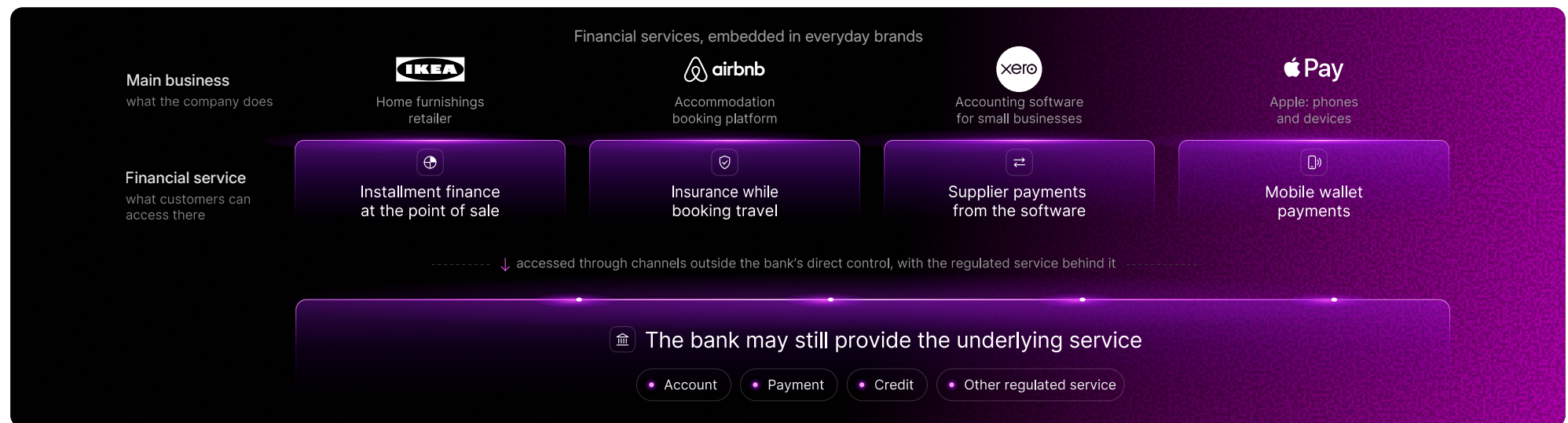
This is already an established part of the financial-services landscape. [BCG](#) estimates that the addressable **embedded finance market across Europe and North America is worth around \$185 billion**, compared with approximately \$32 billion in current penetration. The [European Banking Authority](#) (EBA) also found that 35% of surveyed banks were using white-label arrangements in 2025.

In these journeys, the bank often enters later in the customer decision process. By the time its service is called upon, the financial need may **already have been identified**, the product presented and the provider selected through another platform. The bank still processes or supports the underlying financial activity, but sees less of the decisions that led to it and has less influence over them.

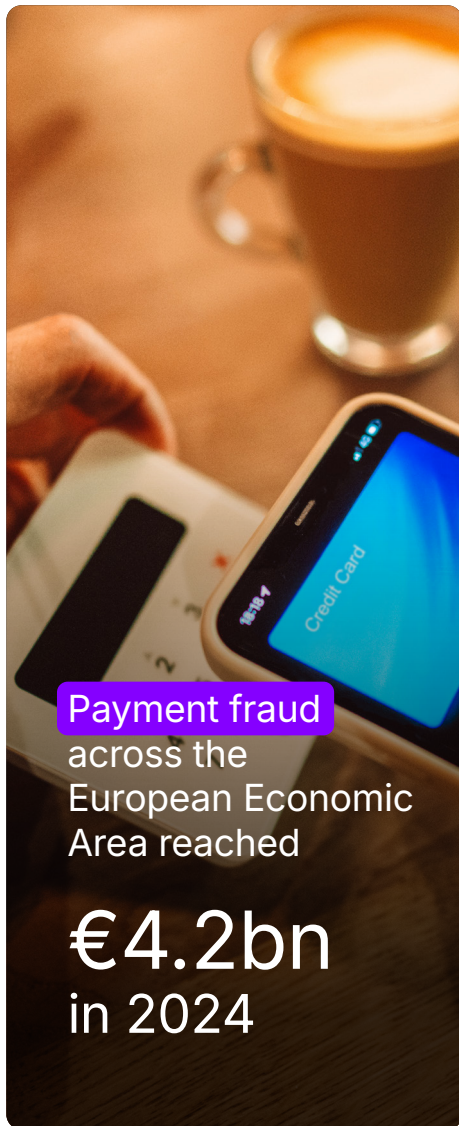
That matters because the **information surrounding the transaction can be as strategically important as the transaction itself**. Another party may understand why the customer needed the service, what alternatives were considered,

what shaped the choice and what financial need may follow. It may also have greater influence over which providers are presented at the point of need.

Over time, this can weaken the bank's ability to personalize services, develop new propositions, acquire customers efficiently and participate in future financial needs. The bank remains present in the execution chain, but risks moving further **outside the customer data** feedback loop that supports understanding, differentiation and future growth.



02. Embedded finance redistributes experience, not accountability



Losing influence does not mean losing responsibility. When financial services are delivered through merchants, platforms and software providers, the **customer experience** may move **outside the bank** while significant **regulatory accountability remains with it**.

That creates a more complex operating environment. Each additional partner introduces new handoffs across identity, onboarding, fraud controls, customer communications, servicing, complaints, partner oversight and regulatory evidence. With every handoff comes the potential for gaps in responsibility, visibility or control.

The EBA has already highlighted some of these risks in white-label banking. In particular, it points to a "lack of transparency about the roles and accountability" of providers and partners, which can make it harder for customers to understand which institution ultimately stands behind a product or **who is responsible when something goes wrong**. For supervisors, the model can also mean less direct visibility over the wider distribution chain.

The risks are not theoretical. Among competent authorities that currently assess the money laundering and terrorist financing risks associated with white labelling, **90% rate them as medium or high**. The EBA also points to the complexity of contractual arrangements, the involvement of entities that may not themselves be regulated and the cross-border nature of many services as contributing factors.

For banks, weaknesses across the wider chain can have consequences well beyond financial crime. Inconsistent customer communications, delayed investigations or complaints that fall between organizations can quickly become conduct, compliance and reputational issues. Fraud adds further pressure, with payment fraud across the European Economic Area reaching **€4.2 billion in 2024, up 17% from the previous year**.

The answer is not for banks to operate every component themselves. Instead, they must retain clear responsibilities, sufficient visibility, consistent controls and evidence across the

full partner chain. They also need the right to step in when a partner's performance, customer treatment or controls fall below the required standard.

As financial services are delivered across a wider range of partners and interfaces, accountability therefore becomes **less about controlling every part of the journey and more about governing the whole model consistently**.

03. PSD3 turns compliance into an operating-model decision

The governance challenge created by distributed financial journeys increasingly overlaps with the requirements of Europe's new payment-services framework. [PSD3](#) and [PSR](#) address different parts of that framework, but together they raise the bar around customer control, third-party access, fraud prevention, interface performance and regulatory oversight.

The distinction between the two is important. **PSR is a regulation**, directly applicable across EU member states, while **PSD3 is a directive** and must be transposed into national law. Under the April 2026 compromise texts, the implementation timetable spans roughly 18 to 21 months after entry into force, depending on the measure, with most PSR provisions applying after 21 months and member states given 21 months to transpose PSD3.

Under the PSR compromise text, specified breaches covering areas such as account access, payment initiation and account-information services, and fraud-prevention requirements can attract maximum administrative fines of **at least 10% of a payment service provider's total annual turnover**.

For banks, the practical requirements touch many of the same capabilities already needed to govern increasingly distributed financial journeys:

- **Permissions and customer control.** Consent dashboards, consent management and the ability to revoke access, with the same architecture potentially extending to AI agents or MCP-connected services acting on a customer's behalf within defined scopes and limits.
- **Partner access.** Stronger governance of TPP identity, onboarding and access to bank interfaces.
- **Fraud controls.** Enhanced fraud prevention, transaction monitoring and customer protection measures.
- **Interface performance and digital parity.** Dedicated interfaces must provide comparable data, functionality and services to the bank's own digital channels, alongside equivalent levels of availability and performance, with ongoing monitoring and reporting.
- **Evidence and oversight.** Clearer records of permissions, access, controls, performance and regulatory compliance.

Meeting the regulatory requirement is only one part of the decision for banks. They must also consider whether the underlying capabilities can support future partners, interfaces and services.

A consent dashboard, for example, can satisfy a defined requirement for customer control. But the **same investment can support a broader system** for managing permissions consistently across products and partners. Interface reporting can be delivered as a regulatory output, or underpinned by a common way of monitoring whether APIs are available and performing as expected. TPP access can be managed connection by connection, or through a scalable approach to identifying, approving and governing external providers. Required fraud controls can likewise sit within a broader framework for setting rules, monitoring activity and retaining evidence.

The strategic value lies in **how far those investments can be reused**. Capabilities built to meet today's requirements can also provide a foundation for future partners, interfaces and services. The proposed FIDA framework points in the same direction, extending permission-dashboard requirements beyond payment accounts to a broader range of financial data.

Designing permissions as a reusable capability therefore reduces the need to rebuild the same controls as the scope of data sharing expands.

PSD3 and PSR therefore create more than a compliance deadline. They give banks an **immediate reason to address operating questions** that will continue to matter as financial activity moves across a wider range of external channels.

04. New interfaces create variations of the same control problem

The operating challenges created by distributed financial journeys extend well beyond today's regulatory requirements. New payment models, shared interfaces and emerging forms of delegated authority are already creating similar questions around identity, access, permissions, monitoring and accountability.

PSD3 and PSR bring many of these issues into immediate focus, but the underlying capabilities will also matter across a wider range of services and customer journeys. As financial activity increasingly begins outside the bank, continues over time or operates within predefined permissions, banks will repeatedly face variations of the same control problem.

Taken together, these developments point to a broader shift. Financial initiation is becoming more distributed, authority can persist beyond a single transaction, and some activity can increasingly operate within predefined rules rather than requiring a fresh customer instruction each time.

For banks, this means the **control model cannot be designed around one regulation, one interface or one type of transaction**. The same fundamental questions will continue to recur around who is acting, what authority they have, which policies

apply, how risk and performance are monitored, what evidence is retained and who remains accountable.

That makes consistency increasingly important. As new interfaces and propositions emerge, banks will need a way to apply the same underlying principles of identity, authority, access and oversight across them rather than rebuilding the control model each time.



Different developments create variations of the same governance challenge

Development	What changes	Control question	Related stat
 Account-to-account payments	Bank services operate at growing scale through external interfaces.	How are access, performance, fraud and accountability governed when initiation happens elsewhere?	80 billion Brazil's Pix, an instant account-to-account payment system, processed almost 80 billion transactions in 2025
 EU Digital Identity Wallet (eIDAS 2.0)	Under eIDAS 2.0, customers will increasingly be able to use EUDI Wallets to identify themselves and authenticate payments across services and borders.	How does the bank integrate trusted external identity and authentication while retaining control over access, consent and payment authorization?	550 550 private companies and public authorities across 26 EU member states, plus Norway, Iceland and Ukraine, are participating in large-scale EUDI Wallet pilots covering more than 11 everyday use cases
 Commercial VRP	Customers can grant ongoing authority for payments within agreed rules and limits.	How are duration, limits, revocation, monitoring and evidence managed?	16% VRPs already account for around 16% of UK open banking transactions
 Wero	Banks participate in a common customer experience while continuing to provide underlying accounts and payment capabilities.	How does the bank maintain control and insight when the interface is shared?	54 million Wero served around 54 million users across Belgium, France and Germany in June 2026
 Open finance	The same model could extend beyond payment accounts into areas such as savings, lending, investment and insurance.	How can access and permissions be governed consistently across a wider range of financial data and products?	493 million India's open finance Account Aggregator ecosystem had fulfilled more than 493 million customer consents by June 2026, with 1,117 financial entities live on the network
 AI agents	A new actor can potentially initiate and execute activity on a customer's behalf.	Who does the agent represent, what authority has it been given, what limits apply and how are its actions evidenced?	1st Europe's first live end-to-end payment executed by an AI agent was completed in March 2026, followed by the first end-to-end European agentic payment in production in June

05. Build the control model once and reuse it

The underlying **requirements are remarkably consistent across regulations**, partners and customer journeys. Banks repeatedly need to manage identity, permissions, access, risk and evidence, and addressing each area separately adds complexity and makes every new connection harder to govern.

A reusable trust and orchestration layer offers a different approach, applying the same underlying controls consistently across interfaces and propositions. This does not mean bringing every component in-house. It means establishing a **common framework** for how the bank governs systems and partners, including who can act, what they are permitted to do, how activity is monitored and what evidence is retained.

A reusable control model can bring together:

- Identity, consent and permissions
- TPP and partner access
- Policy, authority and limits
- API performance, availability and readiness for future monetization
- Enhanced fraud and anomaly controls

- Monitoring and regulatory evidence
- Connections to the bank's underlying execution systems, with ongoing integration and updates to maintain digital parity as products, functionality and services evolve

Reusing these capabilities reduces the need to recreate integrations, controls and remediation processes for every new partner or proposition. It also protects engineering, risk and compliance capacity, while **giving the bank more consistent visibility** as financial journeys extend across external systems and interfaces.

The benefits extend beyond operational efficiency. A bank may want to lead the customer experience in one proposition, participate through a shared interface in another, support a partner-led journey elsewhere and provide regulated execution behind the scenes in another market.

A common control model makes those choices easier to base on commercial strategy and customer need. Without it, the range of viable options can be constrained by legacy systems, fragmented controls or the cost and complexity of supporting another connection.

Greater reuse therefore creates greater strategic flexibility. The same foundation can support new propositions, from repeatable account-to-account payments and partner-led lending to broader open finance services, without requiring the operating model to be reconstructed each time.

Reusable infrastructure is not a revenue engine in itself. Its value lies in giving banks the flexibility and partner readiness to support new propositions and develop stronger commercial models over time.

The banks best placed to remain differentiated will not necessarily be those with the most visible app or the largest number of APIs. They will be those that make their regulated capabilities easier to access, safer to operate and more valuable to reuse.

06. From compliance to strategic readiness with SBS

For banks, the opportunity is to ensure that investment in PSD3 and PSR does more than satisfy the next regulatory requirement. The same capabilities needed for compliance can provide the foundation for managing a growing range of partners, interfaces and propositions more consistently.

SBS helps banks make that transition. The [SBS PSD3 Compliance Solution](#) addresses the immediate requirements of the new payments framework, while the broader [SBS Open Banking Platform](#) provides capabilities that can be reused as the operating model evolves. Wero Connect offers one example of how those foundations can support participation in customer experiences beyond the bank's own applications.

Across consent and permissions, TPP and partner access, API performance, monitoring, security and integration, **SBS gives banks a consistent way to govern how external parties interact with regulated banking capabilities.** Rather than recreating controls for every regulatory change or new connection, banks can reuse them across different partners and services.

That has practical benefits. It can reduce duplicated remediation

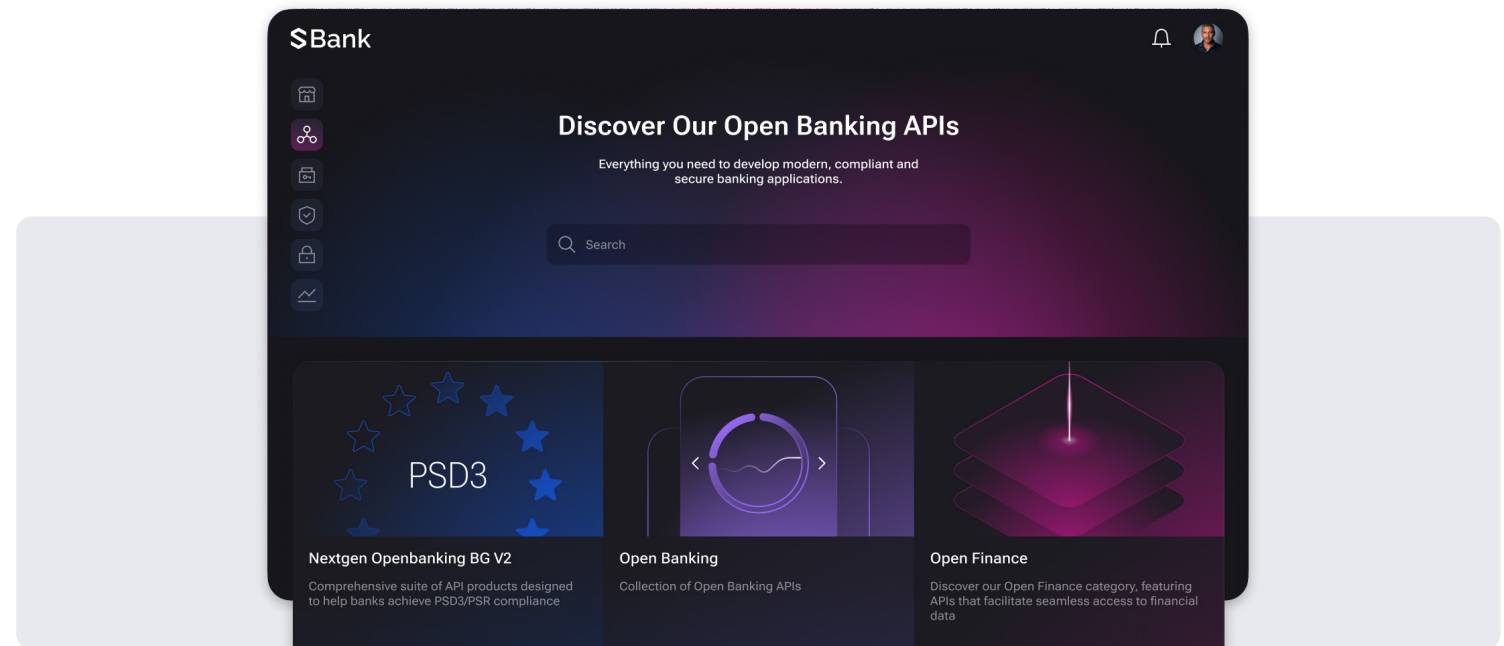
and integration work, protect engineering and compliance capacity, improve visibility across external journeys and shorten the path from a new requirement or partnership to a viable proposition.

More importantly, it preserves choice. A bank can decide where it wants to lead the customer experience, where it makes sense to participate through a shared interface, where to enable a partner-led proposition and where to

provide regulated execution behind the scenes. Those decisions can be driven by strategy rather than by the limitations of fragmented controls or legacy architecture.

The value is not simply more APIs, nor does reusable infrastructure automatically create new revenue. It creates the partner readiness, operating flexibility and strategic freedom from which stronger commercial models can be developed.

Banks may not control every interface. But they can **decide whether they remain differentiated** participants behind those interactions or become interchangeable providers of regulated execution.





SBS is a global software company helping banks and the financial services industry reimagine how to operate in an AI-driven world. Trusted partner to more than 1,500 financial institutions and large-scale lenders across 80 countries, including Santander, Société Générale, BNP Paribas, Groupe BPCE, Crédit Agricole, La Banque Postale, HSBC, Attijariwafa Bank, Nationwide, NextGear Capital, Mercedes-Benz, and Toyota FS, SBS combines 50+ years of banking domain expertise with a suite of award-winning solutions built for the AI era. SBS's composable architecture extends across core banking, lending, payments, compliance, open banking, and asset finance.

With 2,800 employees across 50 offices worldwide, SBS is recognized as a Top 8 Global Core Banking Technology Provider by Everest Group (2026), a Strong Performer in The Forrester Wave: Digital Banking Engagement Platforms (2026), a SPARK Matrix Leader in Digital Banking Platforms (2025), a Top 10 European Fintech by IDC (2025), a Leader in Omdia's Universe: Digital Banking Platforms (2024), and a Leader in Everest Group's Banking Customer Experience Orchestration PEAK Matrix (2024).

SBS is part of 74Software alongside Axway, forming an international software group. SBS is headquartered in Paris, France.

To find out how we can help your bank to create market-beating digital transformation strategies:

www.sbs-software.com

HELLO@SBS-SOFTWARE.COM

Nicolas de Genot de Nieukerken

Director of Product, Open Banking & Digital Wallet at SBS

Nicolas de Genot de Nieukerken is the Director of Product, Open Banking & Digital Wallet at SBS. He has been a Product Manager at SBS for over three years, leading the Open Banking platform and its strategic evolution across Europe and beyond. He oversees two main pillars: regulatory compliance (PSD2) through secure API exposure, and Wero Connect, connecting and orchestrating European Payments Initiative (EPI) central services to any bank core and instant payments engine through a single layer, including the integration of the Wero solution within EPI. His expertise includes API orchestration, core banking integration, consent management, regulatory compliance, and instant payment ecosystems. He plays a key role in positioning SBS as a trusted Open Banking partner by combining technological innovation, security, and scalable architecture.

