EU RegCORE Client Alert

Financial Services

August 2026

Bafin raises the bar on virtual IBAN compliance

QuickTake

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

Mariya Atanasova-Rigas
Tel: +49 151 42669964
mariya.atanasova-rigas@pwc.com

EU RegCORE Team
de_regcore@pwc.com

On 27 July 2026, the German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* – **Bafin**) published Supervisory Communication *("Aufsichtsmitteilung")* 06/2026[1] together with an accompanying interview explaining its supervisory concerns regarding the use of virtual IBANs (**vIBANs**) in connection with underground banking and money laundering.[2] The supervisory communication applies immediately and will remain in force until the EU Anti-Money Laundering Regulation (**AMLR**) becomes applicable on 10 July 2027.

The publication is significant not because Bafin questions the legitimacy of vIBANs themselves, but because it recognises that certain complex implementation models may create opacity over the identity of end customers, beneficial ownership and payment flows. Bafin's message is nuanced: vIBANs are legitimate payment infrastructure that underpin many modern financial services business models, but where they reduce transparency, they require correspondingly stronger Anti-Money-Laundering (**AML**)/Combating the Financing of Terrorism (**CFT**) controls. This supervisory communication should therefore be viewed as

[1] Available only in German: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Aufsichtsmitteilung/dl_2026_07_27_Aufsichtsmitteilung_06_virtuelleIBAN.html?nn=149494.
[2] See details, available at the time of writing, only in German here.

a governance and operating model challenge rather than a restriction on innovation. It should also be read in conjunction but also in contrast with the European Banking Authority's (**EBA**) ongoing work on vIBANs.[3]

Bafin's publication is particularly relevant for banks providing master accounts, payment institutions, electronic money institutions, Banking-as-a-Service providers, embedded finance platforms, treasury providers and firms operating cross-border payment infrastructures.

Bottom line: *Bafin's supervisory communication does not restrict the use of vIBANs. It requires firms to demonstrate that governance, customer transparency and monitoring arrangements have evolved at the same pace as the payment infrastructure itself. Innovation is welcome. Opacity is not. At the same time Bafin's communication marks a wider shift in supervisory tone as well as new principles[4] that the EBA and/or other national competent authorities (**NCAs**) may follow.*

Background and context

Why this matters

vIBANs have become an essential component of modern payments architecture. They support a wide range of entirely legitimate business models, including:

- Banking-as-a-Service platforms
- Embedded finance arrangements
- Marketplace settlement models
- Corporate treasury and cash management
- Payment orchestration
- Merchant acquiring
- Safeguarding structures for payment and e-money institutions
- Automated reconciliation and straight-through processing
- Customer-specific payment routing without separate payment accounts

Without vIBANs, many digital payment providers would lose much of the scalability and operational efficiency characteristic of modern payments infrastructure. Bafin expressly acknowledges these operational benefits, while observing that some multi-layered vIBAN arrangements may create material transparency gaps where the account-servicing institution knows only the intermediary payment institution rather than the

[3] See in particular also our coverage here.
[4] Key concepts and classification principles introduced in this Client Alert include:

- ***Information Architecture Principle*** – effective supervision increasingly depends on the quality of the information architecture connecting financial institutions.
- ***Information-Centric Regulation*** – regulation is progressively focused on transparency, traceability, explainability and accountability across financial ecosystems.
- ***Supervisory Allocation*** – extending the concept from allocating supervisory competences to allocating informational responsibilities across regulated ecosystems.
- ***Transparency by Architecture*** – the idea that transparency should be designed into financial infrastructure rather than reconstructed through compliance after transactions occur.

underlying end customer. These information asymmetries may, in certain circumstances, facilitate money laundering or underground banking. The supervisory focus is not on the technology itself but on the governance surrounding its use.

What Bafin is concerned about

Bafin identifies structural vulnerabilities arising where vIBANs are deployed through complex cross-border payment chains. These include:

- Reduced visibility of underlying customers and beneficial owners;
- Master account structures operated through intermediary payment institutions;
- International payment chains involving multiple intermediaries;
- Foreign master accounts linked to German ("DE") vIBANs;
- Fragmented payment flows;
- Reduced traceability of economic purpose; and
- Exploitation of these transparency gaps by underground banking networks.

The Supervisory Communication refers to supervisory findings involving large international payment flows routed through intermediary payment service providers, including structures connected with Hong Kong and China, illustrating that Bafin is increasingly analysing payment infrastructure through an AML risk lens rather than purely a payments regulatory perspective. Bafin's accompanying interview describes vIBANs as potentially "Trojan horses" where transparency is insufficient, while emphasising that the supervisory objective is to prevent criminal misuse rather than inhibit legitimate innovation.

Bafin's risk indicators

Bafin identifies the following indicators of elevated money-laundering risk in connection with vIBAN structures:

- Use of numerous vIBANs for a single master account of a foreign payment service provider (particularly from a third country)
- Indications of incomplete capture of end-customer details, address data or beneficial owners by the payment service provider
- High transaction volumes without recognisable economic activity
- High payment receipts from possible shell companies (newly founded companies, identical or unusual business addresses, no or generic web presence)
- Indications of shell-company characteristics on the payee side
- Generic or unclear payment references (e.g. "saldo invoice", "saldo fattura", "payment for goods")
- Short usage duration of vIBANs or unusually rapid account turnover
- Complex international payment routes
- Interposition of multiple payment service providers
- Fragmented payment structures and economically implausible transaction patterns
- Combination of trading activity and payment flows without recognisable economic plausibility

These indicators are unlikely to be unfamiliar to firms operating mature transaction monitoring systems, but Bafin has now expressly contextualised them within vIBAN structures and expects firms to calibrate their monitoring systems accordingly.

Supervisory expectations

Bafin expects firms to apply existing AML requirements more rigorously where vIBAN structures create elevated transparency risks. Specifically, firms should ensure:

- Enhanced understanding of underlying end customers and identification of beneficial owners;
- Greater transparency regarding intermediary payment providers and all parties involved in vIBAN structures;
- Strengthened customer due diligence, with enhanced due diligence (Section 15 GwG) where appropriate;
- Improved documentation and regular updating of information on the business model, functioning and control mechanisms of involved payment service providers;
- Risk-based transaction monitoring calibrated to detect fragmented, multi-tier or cross-border payment structures and atypical transaction patterns;
- Assessment of payment service providers' governance and controls, including their access to end-customer and beneficial-owner information;
- Proper registration of end customers and ultimate beneficial natural persons in the German account retrieval system (*Kontenabrufdatei*); and
- Staff training focused specifically on vIBAN-related risks as part of internal safeguards.

Measures should remain risk-based and proportionate to the complexity of the relevant vIBAN structure. The type, scope and intensity of measures should reflect the number of payment service providers involved and the degree of transparency over end customers and their beneficial owners.

Enforcement considerations

Firms that fail to meet Bafin's expectations face a range of potential supervisory consequences. While the supervisory communication does not create new legal obligations, it articulates how Bafin interprets existing requirements under the German Anti-Money Laundering Act *Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten* –**GwG**) and the German Banking Act (*Gesetz über das Kreditwesen* - **KWG**). Non-compliance may result in:

- **Supervisory measures.** Bafin may impose specific instructions, require remediation plans, conduct on-site inspections focused on vIBAN governance, or require enhanced reporting on transaction monitoring effectiveness.

- **Administrative fines.** Under Section 56 GwG), administrative fines of up to EUR 1 million (or EUR 5 million for credit institutions) may be imposed for AML compliance failures. In cases of serious, repeated or systematic violations, fines may reach up to 10% of annual turnover or twice the benefit derived from the breach

- **Licence conditions.** Bafin may attach conditions to authorisations, require changes to business models, or — in severe cases — restrict or withdraw licences where AML deficiencies are deemed material.

- **Personal liability.** Senior managers and MLROs may face personal fines, public naming, or disqualification from management positions where failures are attributable to inadequate governance or oversight.

- **SAR/STR obligations.** Where vIBAN-related transactions meet suspicious activity thresholds, firms must file Suspicious Activity Reports with Germany's FIU. Failure to file, or late filing, creates additional enforcement exposure.

- **Reputational consequences.** Bafin publishes enforcement actions under certain circumstances. For payment institutions and BaaS providers, reputational damage may also affect relationships with partner banks and institutional clients.

The practical message is clear: while the Supervisory Communication is guidance rather than binding regulation, firms should treat it as an indication of how Bafin will assess compliance with existing obligations. Deficiencies identified in future examinations are likely to be measured against these expectations.

Bafin vs EBA: Aligned or divergent?

- **Common ground**. Both Bafin and the EBA recognise that vIBANs are legitimate payment infrastructure but may create transparency gaps where customer information becomes fragmented across multiple institutions. Both emphasise the importance of understanding beneficial ownership and reconstructing payment chains.

- **Where Bafin goes further**. Bafin's communication is more operationally specific, identifying concrete risk indicators (e.g., generic payment references, rapid vIBAN turnover, shell-company characteristics) and linking vIBAN risks explicitly to underground banking and Hong Kong/China payment chains. The EBA's approach has been more principles-based.

- **Timing and legal status**. Bafin's communication applies immediately and will remain in force until the AMLR becomes applicable (10 July 2027). The EBA's work feeds into the broader AMLR/ Authority for Anti-Money Laundering and Countering the Financing of Terrorism (**AMLA**) framework. Firms operating cross-border should expect Bafin's approach to influence other NCAs and potentially shape AMLA supervisory practice.

- **Practical implication**. For firms operating in Germany or with German payment relationships, Bafin's expectations represent the current supervisory standard. For firms operating across multiple EU jurisdictions, the prudent approach is to treat Bafin's communication as an indication of the direction of travel and prepare for similar expectations from other NCAs.

Our observations on Bafin's expectations

Bafin's publication is best understood as part of a broader supervisory trend. Across Europe, regulators increasingly distinguish between digital infrastructure that enables innovation and governance that ensures transparency. The regulatory question is no longer whether innovative payment architectures should be permitted — they already are — but whether firms can demonstrate sufficient visibility over the economic reality behind increasingly sophisticated payment chains.

For many firms, the practical challenge is organisational rather than technological: banks, payment institutions and embedded finance providers need contractual arrangements, data sharing, customer due diligence, transaction monitoring and governance frameworks that collectively give supervisors confidence that complex payment infrastructures do not become AML/CFT blind spots.

For firms using vIBANs, the question is not whether the business model remains permissible, but whether governance, customer transparency and monitoring arrangements evolve at the same pace as the payment infrastructure itself.

Beyond the Guidance: Information Architecture, Supervisory Allocation and the future of AML supervision

What Bafin actually says

Drawing on supervisory experience and intelligence developed jointly with Germany's FIU, Bafin identifies significant money-laundering risks where vIBAN structures are used within complex payment chains or informal value transfer systems ("**underground banking"**). The objective is not to introduce new legal obligations but to raise awareness of existing AML/CFT risks and encourage appropriately calibrated controls.

vIBANs are identifiers allocated to individual customers or transactions without each identifier necessarily corresponding to a separate payment account. Incoming payments are credited to an underlying master or omnibus account, with payment service providers allocating individual vIBANs to their own customers for operational purposes. This model delivers significant operational efficiencies, but also alters the distribution of information across the payment chain.

Where the master-account institution knows only the intermediary payment institution — not the underlying end customer or beneficial owner — transparency gaps arise that make customer due diligence, transaction monitoring and reconstruction of payment flows materially more difficult. The communication does not question whether vIBANs should exist; it asks whether institutions retain sufficient information to satisfy existing obligations as payment architectures become more complex.

The three-regulated-entity problem

vIBAN structures frequently involve multiple regulated entities, each possessing different information and subject to different obligations. The following simplified structure illustrates the information chain:

Stage	**Entity**
1	End Customer
2	Payment Institution / EMI / FinTech
3	Credit Institution (Master Account)
4	Supervisory Authorities

Historically, supervisory models assumed the account-providing institution possessed a sufficiently complete understanding of the customer relationship. Modern payment ecosystems increasingly separate these

functions: one institution may hold safeguarded funds, a second may onboard the customer, another may provide payment initiation, a further provider may perform transaction monitoring, with cloud, fraud-detection and identity-verification specialists contributing further components. The result is a regulated ecosystem where information becomes distributed rather than centralised and no single participant necessarily has a complete picture. Bafin's communication shows supervisors increasingly regard this fragmentation of information — not just of legal responsibility — as a potential source of financial crime risk.

The correspondent banking analogy

Historical AML supervision devoted considerable attention to correspondent banking, asking whether the correspondent institution could rely on another institution's due diligence while maintaining adequate visibility over underlying activity. vIBAN structures raise a remarkably similar question: can institutions collectively identify the customer, understand the commercial purpose and reconstruct the payment chain if required?

vIBANs represent less a new category of AML risk than the latest manifestation of a long-standing supervisory concern about information asymmetry in increasingly complex financial networks.

Worked example: Information fragmentation in a typical Banking-as-a-Service (BaaS) model

Consider a typical BaaS arrangement where an e-commerce platform offers payment accounts to its merchants:

- **Stage 1 — Customer onboarding.** A merchant signs up through the e-commerce platform's interface. The platform collects basic business information but does not perform AML due diligence itself.

- **Stage 2 — Payment institution.** The platform's embedded finance partner (a licensed payment institution) receives the merchant's details and performs KYC/KYB checks. The payment institution allocates a vIBAN to the merchant for receiving payments.

- **Stage 3 — Master account.** The vIBAN routes to a master account held by the payment institution at a German credit institution. The credit institution knows the payment institution as its customer but has no direct relationship with the underlying merchant.

- **Stage 4 — Transaction flow.** A buyer in another EU Member State pays the merchant using the vIBAN. The payment arrives at the master account. The credit institution sees an incoming payment to a vIBAN but may not know the merchant's identity, beneficial ownership or the nature of the underlying transaction.

Information fragmentation. At this point, information is distributed across four entities: (i) the e-commerce platform holds commercial data on the merchant's trading activity; (ii) the payment institution holds KYC/KYB records and beneficial ownership information; (iii) the credit institution holds transaction data but limited customer context; and (iv) an outsourced transaction monitoring provider may hold pattern-detection algorithms but no direct customer relationship.

The supervisory question. If Bafin or the FIU requests information on a specific payment, can the credit institution reconstruct the payment chain, identify the merchant, confirm beneficial ownership and explain

the economic purpose? Bafin's supervisory communication asks whether the contractual, technical and governance arrangements across this ecosystem are sufficient to provide that transparency.

The Information Architecture Principle

> *"As financial services become increasingly modular, distributed and platform-based, effective supervision depends not only upon the regulation of individual institutions but also upon whether the underlying information architecture permits end-to-end transparency, traceability and accountability across the financial ecosystem."*

Historically, financial regulation concentrated on legal entities: who is regulated, which activities require authorisation, which regulator is responsible. Increasingly, supervisors also ask: who possesses information on the underlying customer? Who can identify the beneficial owner? Who can reconstruct the payment chain? Who understands the economic purpose? Who can explain how the payment architecture works in practice?

The object of supervision expands beyond institutions to the quality of information generated by interconnected ecosystems. vIBANs are one example; the same framework increasingly applies across operational resilience, digital finance, AI and data governance.

From institution-based regulation to information-centric regulation

Supervisory philosophy has evolved over three decades:

Period	**Supervisory Focus**
1990s	Institution-based supervision
2000s	Risk-based supervision
2010s	Group-wide supervision
2020s	Data-driven supervision
Emerging	Information-centric supervision

Under the emerging model, regulators continue to supervise legal entities but increasingly evaluate whether information flows across complex ecosystems are sufficiently complete, reliable and transparent to permit effective supervision. This is evident beyond AML: The Digital Operational Resilience Act (**DORA**)[5] requires understanding of critical ICT dependencies through supply chains; the Artificial Intelligence Act (**AI Act**)[6] emphasises transparency, explainability, human oversight and accountability; Payment Services Directive

[5] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

(**PSD3**)[7] and the proposed Payment Services Regulation (**PSR**)[8] strengthen governance across distributed payment ecosystems; the AML Regulation and AMLA seek improved transparency and consistency across integrated European markets.

Supervisory allocation in practice

Traditionally, supervisory allocation concerned dividing regulatory competence between authorities (e.g. ECB/NCA prudential allocation, banking/securities/insurance divisions, home/host allocation). Bafin's communication suggests supervisory allocation increasingly concerns the allocation of information: regulatory responsibilities remain divided between institutions, but the information necessary to supervise those responsibilities is distributed across banks, payment institutions, technology providers, embedded finance platforms and outsourced providers.

The challenge becomes ensuring those distributed information sets collectively provide an accurate, transparent understanding of customer relationships and payment activity. Supervisory allocation is evolving from an allocation of institutional competence towards an allocation of informational responsibility, with implications extending across digital finance, embedded finance, open finance and AI.

Why Bafin's guidance extends beyond AML

Viewed through this lens, the communication is a broader statement on governance of distributed financial ecosystems: as payment infrastructures become more sophisticated, transparency, accountability and governance expectations rise proportionately. Innovation remains compatible with effective regulation provided institutions can demonstrate governance and information management have kept pace.

PSD3 and the Payment Services Regulation: Reinforcing vIBAN governance

Bafin's supervisory expectations should be read in the context of the proposed PSD3 and Payment Services Regulation (**PSR**), which will reshape the governance framework for payment institutions and their relationships with credit institutions. Several provisions are directly relevant to vIBAN structures:

[7] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC.

[8] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010.

- **Strengthened authorisation and governance.** PSD3 proposes enhanced authorisation requirements and ongoing governance obligations for payment institutions, including more rigorous assessment of beneficial ownership structures and business models involving master account arrangements.

- **Agent and distributor oversight.** The PSR strengthens requirements for payment institutions to oversee agents and distributors, with implications for BaaS and embedded finance models where customer-facing activities are distributed across multiple entities.

- **Access to payment accounts.** PSD3 addresses the relationship between payment institutions and credit institutions providing master accounts, with provisions designed to ensure continued access to payment infrastructure while preserving AML controls.

- **Convergence with AML framework.** Both PSD3 and the AMLR emphasise the need for consistent governance across payment ecosystems. Firms that address Bafin's current expectations are likely to be better positioned for the combined PSD3/AMLR framework when it enters into force.

The practical implication is that vIBAN governance is not solely an AML compliance matter; it intersects with payment services authorisation, operational resilience (DORA) and the broader regulatory architecture for distributed payment ecosystems.

Governance, business model implications and preparing for the next phase of AML supervision

Bafin's risk indicators — looking beyond individual transactions

The risk indicators identified in the Supervisory Communication — from the use of numerous vIBANs by foreign payment service providers, through generic payment references and rapid account turnover, to economically implausible transaction patterns — will not surprise experienced AML practitioners. However, Bafin has expressly contextualised them within modern payment architectures.

The supervisory focus is evolving beyond identifying suspicious transactions towards understanding whether the overall payment ecosystem permits those transactions to be understood at all. This represents a shift from transaction-level monitoring to ecosystem-level governance.

Governance rather than technology

The communication does not require firms to redesign payment infrastructure. It requires firms to demonstrate that governance has evolved alongside innovation. This includes:

- Transparency regarding identity of end customers and beneficial ownership
- Contractual relationships between participating institutions
- Allocation of AML responsibilities
- Transaction monitoring
- Information-sharing arrangements
- Documentation

- Ongoing due diligence
- Escalation procedures where transparency becomes insufficient

The central question is not whether vIBANs are used but whether firms continue to understand the customers and payment activity behind them.

Outsourcing does not outsource transparency

Modern payment ecosystems often involve specialist providers for onboarding, eID, sanctions screening, fraud detection, transaction monitoring, cloud infrastructure, payment processing, safeguarding, customer support and data analytics. While operationally efficient, these arrangements distribute information across multiple organisations.

The principle is clear: institutions may outsource operational processes; they cannot outsource regulatory accountability for transparency. Outsourcing arrangements and commercial contracts should provide timely access to customer information, transaction data and supporting documentation when required for supervisory or AML purposes. This aligns with DORA, the EBA Guidelines on Outsourcing Arrangements and the forthcoming AML Regulation.

Implications by business model

The following summarises the key considerations for different categories of affected firms:

Credit Institutions

- Assess visibility over underlying customers, beneficial ownership and transaction activity where payment institutions allocate vIBANs to their own customers
- Focus on contractual rights to obtain customer information and oversight of intermediary institutions

Payment Institutions

- Evaluate whether due diligence, onboarding and monitoring remain appropriate as payment flows become more international and multi-intermediary
- Consider information-sharing arrangements with account-servicing institutions

Electronic Money Institutions

- Review governance of safeguarding accounts, customer identification and transparency of fund flows
- Consider the interaction between safeguarding obligations and AML obligations

Banking-as-a-Service Providers

- Most directly affected — many BaaS models depend on the combination of master accounts, vIBANs and distributed customer relationships
- Review governance, contractual responsibilities, customer due diligence, information-sharing, transaction monitoring, operational resilience and oversight of fintech distribution partners

Embedded Finance Providers

- Customer relationships often originate outside the regulated sector

- Consider whether customer information from commercial platforms remains sufficiently accessible to regulated AML-responsible firms

Crypto-Asset Service Providers

- Increasingly rely on vIBANs for fiat payment flows
- Ensure governance develops alongside MiCAR, the Transfer of Funds Regulation and evolving AML requirements

Bafin's supervisory communication expressly references payment chains involving Hong Kong and China as examples of elevated risk. This has implications for non-EU firms with German or EU payment relationships:

Third-country considerations

- **UK firms.** Post-Brexit, UK payment institutions and EMIs operating through master accounts at German credit institutions should expect heightened scrutiny of vIBAN arrangements. German credit institutions may seek enhanced contractual information rights, more detailed KYC documentation on underlying customers and assurances regarding UK AML compliance. UK firms should proactively review their German banking relationships and ensure governance arrangements meet Bafin's expectations.

- **Swiss firms.** Swiss payment service providers using vIBANs linked to German or EU master accounts face similar considerations. While Switzerland has a robust AML framework, Bafin's focus on third-country payment chains means Swiss firms should ensure transparency arrangements with EU partner banks are sufficient to satisfy German supervisory expectations.

- **US firms.** US payment platforms and fintech companies operating through EU banking partners should review whether their vIBAN governance arrangements are consistent with Bafin's expectations. The supervisory communication's focus on information fragmentation is particularly relevant where US platforms use embedded finance arrangements with European payment infrastructure.

- **Correspondent banking relationships.** German credit institutions with correspondent relationships involving third-country payment institutions should review whether existing due diligence addresses vIBAN-related transparency risks. Bafin's communication suggests that standard correspondent banking due diligence may be insufficient where the third-country institution operates complex vIBAN structures.

- **High-risk jurisdictions.** Where vIBAN structures involve payment chains through or with connections to jurisdictions identified as high-risk by FATF or the EU, enhanced due diligence under Section 15 GwG will apply. Bafin's supervisory communication reinforces the expectation that firms should have specific transaction monitoring scenarios for such payment flows.

Board-Level Governance Questions

The following questions may assist boards and senior management in assessing their institution's preparedness:

Customer transparency

- Can we identify the underlying customer for every vIBAN?

- Can we identify the ultimate beneficial owner where required?
- Are customer records sufficiently complete throughout the payment chain?

Information Architecture

- Do we understand how customer information moves between participating institutions?
- Where does information become fragmented?
- Can information be reconstructed rapidly during a supervisory inspection?

Governance

- Are AML responsibilities clearly allocated between participating institutions?
- Are contractual rights sufficient to obtain information when required?
- Does senior management receive adequate reporting on vIBAN risks?

Transaction monitoring

- Have monitoring scenarios been calibrated specifically for vIBAN structures?
- Can systems detect fragmented payment behaviour across multiple institutions?
- Can payment flows be reconstructed end to end?

Outsourcing

- Have outsourced providers introduced supervisory blind spots?
- Are information rights contractually enforceable?
- Is outsourcing documentation consistent with DORA and AML expectations?

Five predictions and what firms should consider doing

Based on our analysis of this and related developments, we anticipate:

1. Similar guidance across Europe as other NCAs adopt comparable expectations alongside EBA work and AMLA's assumption of supervisory responsibilities.

2. Greater focus on payment ecosystems in future AML inspections, examining complete payment chains rather than individual firms in isolation.

3. Governance becoming the primary supervisory focus rather than whether firms use vIBANs per se.

4. Banking-as-a-Service receiving greater regulatory scrutiny regarding the allocation of responsibilities between licensed institutions and technology partners as BaaS expands across Europe.

5. Information architecture becoming a supervisory objective in its own right, with institutions demonstrating transparency, traceability and accountability across complex ecosystems better positioned than those relying solely on formal legal allocations of responsibility.

Bafin's supervisory communication applies immediately and will remain in force until the AMLR becomes applicable on 10 July 2027. Firms should distinguish between immediate actions and medium-term AMLR readiness:

- **Gap analysis.** Conduct a gap analysis of existing vIBAN governance arrangements against Bafin's risk indicators and supervisory expectations.

- **Contractual arrangements.** Review contractual arrangements with payment service providers to ensure adequate information rights and AML responsibility allocation.

- **Transaction monitoring.** Assess whether transaction monitoring scenarios are calibrated specifically for vIBAN-related risks, including fragmented and multi-tier payment structures.

- **End-customer transparency.** Evaluate end-customer transparency within master account structures and the adequacy of beneficial ownership identification.

- **Outsourcing arrangements.** Review outsourcing arrangements to ensure information accessibility and consistency with DORA and AML expectations.

- **Board-level governance.** Prepare board-level governance documentation demonstrating how the institution addresses vIBAN transparency risks.

- **Regulatory benchmarking.** Benchmark existing controls against emerging expectations under the AMLR, AMLA, PSD3, the PSR and DORA.

- **Supervisory engagement.** Consider proactive supervisory engagement to demonstrate awareness of and responsiveness to Bafin's updated expectations.

- **AMLR readiness and transition.** Align vIBAN governance with AMLR requirements; prepare for AMLA supervisory expectations; integrate with PSD3/PSR and DORA frameworks; benchmark against emerging NCA guidance; and embed information architecture as a core governance objective, positioning transparency, traceability and accountability across distributed payment ecosystems as a competitive advantage.

Given the increasing adoption of embedded finance and Banking-as-a-Service across Europe, this communication is likely to influence supervisory expectations well beyond Germany and may foreshadow similar approaches under the forthcoming EU AML Regulation and the future AML Authority (AMLA).

Outlook

Bafin's latest supervisory communication is not a warning against innovation; it is a reminder that innovation and transparency must evolve together. vIBANs will continue to underpin many of Europe's most successful payment, BaaS and embedded finance business models and their importance is likely to increase as financial services become more digital, platform-based and interconnected.

The regulatory challenge is not whether these technologies should be adopted, but whether institutions can demonstrate that governance surrounding them has become as sophisticated as the technology itself. This is an illustration of a wider transformation in European financial supervision: from supervising institutions in isolation towards supervising the quality of information that flows between them.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from relevant related developments. We have assembled a multi-disciplinary and multi-jurisdictional team of sector experts to support clients navigate challenges and seize opportunities as well as to proactively engage with their market stakeholders and regulators.

Moreover, we have developed a number of RegTech and SupTech tools for supervised firms, including PwC Legal's Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from more than 2,500 legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Equally, in leveraging our Rule Scanner technology, we offer a further solution for clients to digitise financial services firms' relevant internal policies and procedures, create a comprehensive documentation inventory with an established documentation hierarchy and embedded glossary that has version control over a defined backward plus forward looking timeline to be able to ensure changes in one policy are carried through over to other policy and procedure documents, critical path dependencies are mapped and legislative and regulatory developments are flagged where these may require actions to be taken in such policies and procedures.

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

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

Contact

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

Mariya Atanasova-Rigas
Tel: +49 151 42669964
mariya.atanasova-rigas@pwc.com

EU RegCORE Team
de_regcore@pwc.com

www.pwc.de