Position paper

Transparency Register Number: 0767788931-41

Towards a Resilient, Trusted and Fraud Resistant Digital Single Market

July 2025

An integrated perspective on Artificial Intelligence, Fraud Prevention and IT Operational Resilience for the EU "Digital Omnibus"

Why focus on these three pillars?

The forthcoming "Digital Omnibus" package offers a rare opportunity to weave together Europe's most pressing digital policy strands into one coherent fabric. Among the many topics on the table, Artificial Intelligence (AI), fraud prevention and IT operational resilience stand out for three reasons:

1. Mutually reinforcing risks – Sophisticated AI models accelerate innovation but can also amplify fraud vectors and magnify the impact of IT outages when embedded deep in critical infrastructures.
2. Shared policy levers – All three areas hinge on data availability, supervisory cooperation and proportionate safeguards. Streamlining them together prevents duplication, closes loopholes and creates a level playing field for firms of every size.
3. Strategic autonomy & competitiveness – Secure AI adoption, effective anti- fraud collaboration and robust digital resilience are indispensable if Europe is to remain globally competitive while preserving sovereignty over its financial system.

The text that follows therefore treats the three pillars as parts of one policy continuum rather than isolated dossiers. It offers targeted recommendations to simplify, align and future proof the EU rule book—suitable for the Digital Omnibus debate.

1. Smart AI Regulation – Coherent, Proportionate, Practicable

1.1 Clarify scope and definitions

A crisp, risk oriented definition of AI is essential. The current wording of the AI Act leaves too much room for ambiguous interpretation of transparent, rule based models such as linear or logistic regression that pose none of the opacity or learning related risks of modern AI systems. Excluding non learning or fully transparent statistical models would sharpen supervisory focus and conserve compliance resources.

1.2 Differentiate high risk use cases

In finance, AI is often deployed for operational tasks (fraud detection, anomaly spotting, pattern recognition) rather than for decision making with direct legal effect

Association of German
Public Banks, VÖB, e.V.
Lennéstraße 11, 10785 Berlin, Germany
www.voeb.de

President: Eckhard Forst
Vice President: Rainer Neske
Executive Managing Director and
Executive Board Member:
Iris Bethge-Krauß

on individuals. The high risk catalogue in Annex III should therefore retain the explicit carve out for fraud prevention tools, while keeping credit worthiness assessments decisions, derived from real AI-Models within scope.

1.3 One supervisor, one playbook
Fragmented oversight would erode the Single Market. Assigning primary responsibility to existing financial supervisors (e.g. the ECB/SSM, EBA coordinated national competent authorities) avoids double standards and ensures that AI oversight dovetails with prudential supervision.

1.4 Eliminate overlap with sectoral law
Before additional AI specific controls are imposed, an overlap and gap analysis against CRR/CRD, DORA, PSD 2, IPR, AMLR and existing EBA guidelines needs to be completed. Equivalent safeguards should be deemed compliant by default.

1.5 Integrate reporting & tooling
Rather than building standalone channels, incident reports and compliance attestations can ride on established portals such as the European single supervisory reporting platform (MVP). A modular self assessment tool that outputs tailored compliance guidance according to the AI Act's four level risk taxonomy would dramatically lower barriers for SMEs.

1.6 Align with data protection law
Joint EBA EDPB guidance should harmonise bias mitigation, data minimisation and accuracy requirements, and map the AI Act's Fundamental Rights Impact Assessment to the GDPR Data Protection Impact Assessment. The legal status of pseudonymised data for AI training must be clarified as a matter of urgency.

1.7 Respect realistic timelines
Politics has underestimated the time required for standardization. As a result, the entire framework is delayed, and the industry is unable to plan in a timely manner. Mandatory standards via CEN/CENELEC are already a year late; supervisory guidelines on General Purpose AI (GPAI) remain in draft. Phased implementation or explicit reliance on interim instruments (e.g. the GPAI Code of Practice) until formal standards maturity will preserve legal certainty without diluting safeguards.

2. Combating fraud through cooperation along the entire chain

2.1 The evolving threats of Fraud
Fraud against customers and companies is becoming increasingly professional. We are now dealing with a fraud industry that is organized and capable of flexibly responding to countermeasures. Measures such as Verification of Payee are too rigid for the fraud industry and are easily circumvented with simple tactics. Therefore, we need effective fraud prevention based on collaboration between various market players and government authorities.

2.2 A Stocktake of today's Fraud
Fraud today is largely based on the manipulation of customers or employees in companies who are forced to make fraudulent payments (social engineering). This manipulation process typically begins

with an email, letter, SMS, WhatsApp message, or phone call. The payment is the final step in a fraud process that may take days, weeks, or even months. Focusing solely on banks – the last link in the chain – means missing out on valuable information about the early stages of fraud. That's why providers of email, postal services, social media, and telecommunication services must also be included.

2.3 Break the silos

Because the fraudulent journey crosses multiple communication layers, exclusively tackling banks– the final link – misunderstands critical early stage intelligence. An effective model must bring together:

- → Law enforcement – Federal and state criminal police offices (e.g. BKA/LKA)
- → Communication & platform providers – email hosts, postal services, telcos, social media networks
- → Banks & payment institutions

2.4 What is blocking cooperation today?

Currently, there is no possibility for data exchange across telecommunications companies, postal service providers, platform operators, and banks. The responsibility for sharing fraud-related data is fragmented and spread across various sectors. The Digital Omnibus offers an excellent opportunity to enable this cross-sector collaboration. Multiple committees exist, but no cross sector legal basis enables real time exchange of contextual data necessary to trace fraudulent campaigns end to end.

2.5 Digital Omnibus as opportunity for effective fraud prevention and law enforcement!

The Digital Omnibus is Europe's best chance to unlock cross-sector collaboration against fraud. The Omnibus should therefore create a framework that permits proportionate, purpose-bound data sharing for fraud prevention.

Design pillars

- → Targeted GDPR exemption for fraud-related data
  A clear exemption from the legal basis, supplemented by access controls and audit trails. Retention periods and conditions for sharing and deleting data must be defined in a legally secure manner.
- → Mandatory exchange of information on fraud and appropriate measures
  Regular meetings at which law enforcement authorities, online platforms, telecommunications and postal services, and banks jointly analyse emerging fraud and decide on appropriate countermeasures.
- → Safe harbour protection
  Protection of participants from civil or regulatory liability if they respond in good faith to shared alerts.

Without these provisions, billions will continue to be lost through fraud in the EU and taxpayers will be cheated. Fraud undermines trust in the digital agenda and burdens European citizens and the economy. If Europe wants genuine digital sovereignty and competitiveness, seamless data exchange must become a cornerstone of its fraud-defence strategy.

3. Making DORA Fit for Purpose – Proportional Resilience

3.1 Lex specialis and simplification

DORA is poised to be the lex specialis for financial sector cyber resilience. To avoid overlap, financial institutions should be explicitly exempt from the horizontal Cyber Resilience Act when DORA applies.

3.2 Tiered proportionality

DORA's one size fits all approach risks gold plating through divergent national interpretations. A tiered framework aligned with CRR segments (G SIBs, O SII, non systemic) would tailor obligations such as documentation depth, testing frequency and incident thresholds to actual systemic relevance. Promotional banks with public mandates and modest risk profiles could benefit from reduced reporting cadences.

3.3 Smarter incident reporting

Non critical outages and small scale customer impacts swamp supervisory bandwidth and firm resources. Raising customer impact thresholds (e.g. 200 000 or 5 % of base) and extending the reportable downtime for non critical systems from one to four hours would keep focus on material events.

3.4 Efficient third party oversight

Continuous bespoke audits of hyperscale cloud or SaaS providers are unrealistic for smaller banks. DORA should formally recognise EU wide certifications (e.g. the forthcoming EUCS for cloud) and joint audit models. A single annual outsourcing overview centred on SLA compliance could replace disparate, overlapping questionnaires.

3.5 Risk based testing

Threat led penetration testing (TLPT) is resource intensive and should be limited to systemic or high exposure entities. Lower risk institutions could rely on red team exercises, tabletop drills or sector wide TLPT participation, with non critical systems on a two to three year test cycle.

Conclusion – A Unified Roadmap for the Digital Omnibus

Treating AI governance, fraud prevention and IT resilience as discrete silos would multiply bureaucracy, leave exploitable gaps and slow innovation. A streamlined, proportionate and interoperable rule set across these three pillars will:

- → Boost trust – Citizens gain confidence that AI innovations are safe, fraud risks are contained and essential services remain available.
- → Cut costs – Firms avoid redundant audits, overlapping reports and inconsistent supervisory demands.
- → Strengthen sovereignty – Europe forges a competitive advantage based on secure, responsible digital infrastructure rather than regulatory sprawl.

The recommendations above chart a pragmatic path: clarify definitions, assign single point supervision, enable targeted data sharing to fight fraud, and calibrate DORA's obligations to risk. Anchoring them in the Digital Omnibus will convert policy ambition into operational coherence—laying the groundwork for a resilient, innovative and fraud resistant European financial sector.

The Association of German Public Banks (Bundesverband Öffentlicher Banken Deutschlands, VÖB) is a leading association within the German banking sector. It represents the interests of 64 banks, including the Landesbanken (the head institutions of the German Savings Banks Finance Group), as well as the promotional and development banks owned by the Federal Republic of Germany or the individual German federal states. With total assets of some 3,029 billion euros, VÖB's member institutions cover approximately one quarter of the German banking market. Public-sector banks honour their responsibility towards SMEs, other enterprises, the public sector, and retail customers; they are deeply rooted in their respective home regions, all over Germany. With a 57 percent market share, ordinary VÖB member banks are market leaders in local authority financing; in addition, they provide some 22 percent of all corporate lending in Germany. In 2024, development and promotional banks at federal and state level provided 60 billion euros in new development and promotional loans. VÖB is the only German banking association exercising the functions of an employer association for its member institutions: the Public-Sector Banks' Employer Association (Tarifgemeinschaft Öffentlicher Banken), which comprises VÖB member institutions with a total of 60,000 employees (as at financial year 2024) and which performs collective bargaining duties.

More information is available at www.voeb.de/en