Rising application of AI in EU banking and payments sector

25/09/2025

Over the past decade, the EU banking sector has undergone a profound digital transformation, embracing a broad spectrum of technologies to enhance operational efficiency and customer experience. Among those technologies, AI has become increasingly prevalent and is playing a pivotal role in reshaping banking processes.

AI refers to a broad range of machine-based systems designed to operate with varying levels of autonomy and which generally adapts to input data and context.

Observed use cases and market trends

The EBA monitors the adoption of AI, including relevant use cases and market trends. To-date, the EBA observes 92% of EU banks are currently deploying AI, and 8% are pilot testing or discussing AI use cases.

Profiling or clustering of clients or transactions

- Delineating customers profiles according to their behaviour, preferences or transaction/credit history
- Grouping customers according to their similarities

AI enables the analysis of very large and unstructured datasets and the identification of non-obvious clusters and patterns.

Optimisation of internal processes

- Summarising and classifying documents
- Preparing meeting minutes
- Improving IT applications, including generating codes

AI enables automatisation of tasks in a way that improves time- and cost-efficiency.

Creditworthiness assessment and credit scoring

- Evaluating the creditworthiness of individuals
- Assigning credit scores to individuals

AI improves accuracy and predictive power thanks to a fast analysis of complex and vast amounts of data.

AML/CFT and Fraud detection

- User identification and verification, including remote onboarding and digital identification
- Detection of patterns and anomalies related to ML/TF and predicate offences, also for enhanced risk profiling
- Fraud detection
- Real-time monitoring of user activity and transactions

AI enables a faster, more accurate, and scalable analysis that improves speed and efficiency in the identification, verification and detection of fraud or suspicious activities.

Risk modelling

- Detecting anomalies in transactions patterns (amounts, frequencies, counterparties) that may indicate fraud, operational errors or risks
- Analysing customer sentiment to indicate cases that warrant further investigation or risk mitigation

AI enables an improved detection of abnormal results, flaws, market trends, shifts in customers' preferences.

Customer support

- Customer support, including chatbots
- Other customer-facing applications

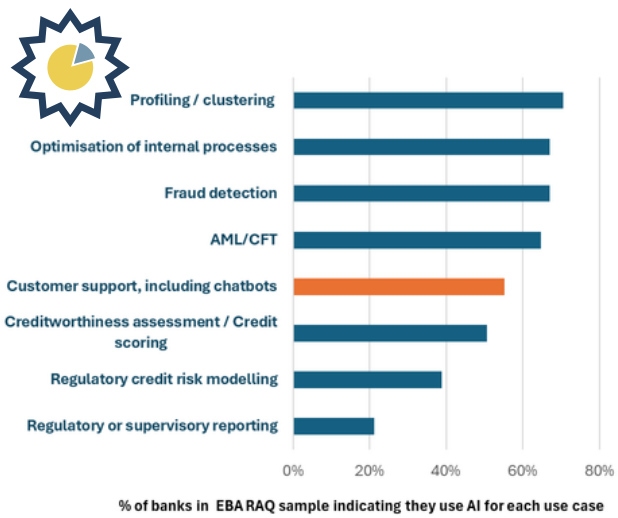
AI improves the personalisation and responsiveness of customer service channels and of digital customer experience.

Use of General-Purpose AI (GPAI) and Agentic AI in consumer-facing applications

The EBA monitors the adoption of GPAI and so-called Agentic AI in the EU banking sector, with a focus on consumer-facing applications. The EBA is engaging directly with market participants, consumer organisations and supervisors.

55% of surveyed banks are already using GPAI or agentic AI in consumer-facing processes. Most common uses:

- detection and notification of fraudulent or suspicious activities,
- assisting customer service agents and call centre operators to handle service requests,
- automating the provision of information or guidance for customers to self-serve for digital actions,
- automating support and financial education tools (e.g. FAQs or Q&As), and
- making digital assistants, including voicebot assistants, available for banking customers.



% of banks in EBA RAQ sample indicating they use AI for each use case

Relevant use cases of GPAI and AI agents are:

- coding & programming
- summarising & obtaining insights from documentation
- drafting legal, support or marketing documents,

The adoption of GPAI & agentic AI is ultimately subject to balancing of risks & opportunities

Drivers

- improvements in **productivity** and **efficiency** of staff
- **optimisation** of processes
- ability to enhance **customer interactions**

Challenges

- **reliance on third-parties**
- **quality of input data,** adequate **data governance & human oversight**
- ensuring **consumer consent** to use data in training GPAI models
- **consumer access to clear & meaningful explanations** on AI logic & risks
- **reputational and litigation risks** as a result of hallucinations or inappropriate / inaccurate information