1 July 2019

EBF_037419

EBF position paper on AI in the banking industry

Key points:

- Artificial Intelligence (AI) presents opportunities to **increase prosperity and growth**. For the banking sector, it provides great opportunities to enhance customer experience, democratize financial services, improve cybersecurity and consumer protection and strengthen risk management.
- **Transparency and explainability**, are important in maintaining trust in AI, given the statistical nature of this technology. However, we would highlight that a **risk-based approach** should be preferred to maintain a high-level of customer protection and trust.
- Ensuring a **level playing field for all industries and geographies** is of capital importance to ensure the uptake of AI in the European banking sector and to maintain a strong level of customer protection, ensuring customers are empowered.
- AI is an evolving technology and it is paramount to ensure that the **regulatory environment is fit for the use of AI** by promoting innovation and legal certainty. We highlight the need for a "future-proof"/ "technology-ready" legal and regulatory framework.
- We thus stress the need to maintain a **high level of consumer protection** while ensuring a level playing field and an activity-based/technology-neutral approach to regulation.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

Table of contents:

INTRODUCTION

Banking institutions have been using "Artificial Intelligence" for a number of years, although it was initially limited to specialised applications.

Today, Artificial Intelligence (AI) techniques are being rapidly adopted for a new range of applications in the banking services industry. Banks are investing more in research and development of AI applications, and the technology has come to play an integral role in a range of activities, from improving customers' experience to a more efficient management of compliance. This evolution is due to an improved access to large data sets and an increase in data-processing power.

There has been an increase in interest from supervisors, regulators and policy-makers in the last few years who have been looking at the way AI is used, both in a horizontal and vertical way.

The present paper aims at **providing more information on the context and way AI is developed and used in the banking sector**. It aims to provide some foundations for a meaningful conversation around the use of AI in the banking industry and **lead to a deeper understanding of its practical implementation and the challenges banks face today when implementing AI solutions**.

By first acknowledging that "AI" is actually a polysemous word which covers a multitude of realities, we present some concrete examples and use-cases presenting the way AI has been used (and could be used) in the future to enhance consumer experience, streamline banking operations, and increase security in our industry.

Drawing from these first two parts, we then turn to the opportunities and challenges provided by the evolution in the technology, starting with some ethical considerations. From general and more horizontal considerations (touching not only on the current legal framework but also on the competitiveness of EU players), we finally focus more specifically on the issues impacting the banking sector – both in terms of opportunities as well as risks and challenges.

What is Artificial Intelligence ?

"*Artificial Intelligence is typically defined as the ability of a machine to perform cognitive functions we associate with human minds, such as perceiving, reasoning, learning, interacting with the environment, problem solving, and even exercising creativity*"[1]. However, Artificial Intelligence (AI) is actually a combination of advanced computational technologies in varying degrees of maturity.

Some of these technologies have been around for decades[2] while others are relatively new. With the advent of Big Data, the technologies commonly referred to under "AI" are rapidly evolving. It is however an incremental technological evolution, sometimes based on old technologies, which has now been made possible by access to large volumes of data and new capacities in processing these volumes of data.

The wording "Artificial Intelligence" is based on terms that can sometimes seem overused as it is used generically to cover multiple technologies. Most of the time, the use of algorithms is limited to mimicking scenarios; reproducing and automating the processing of repetitive tasks that a human being could perform.

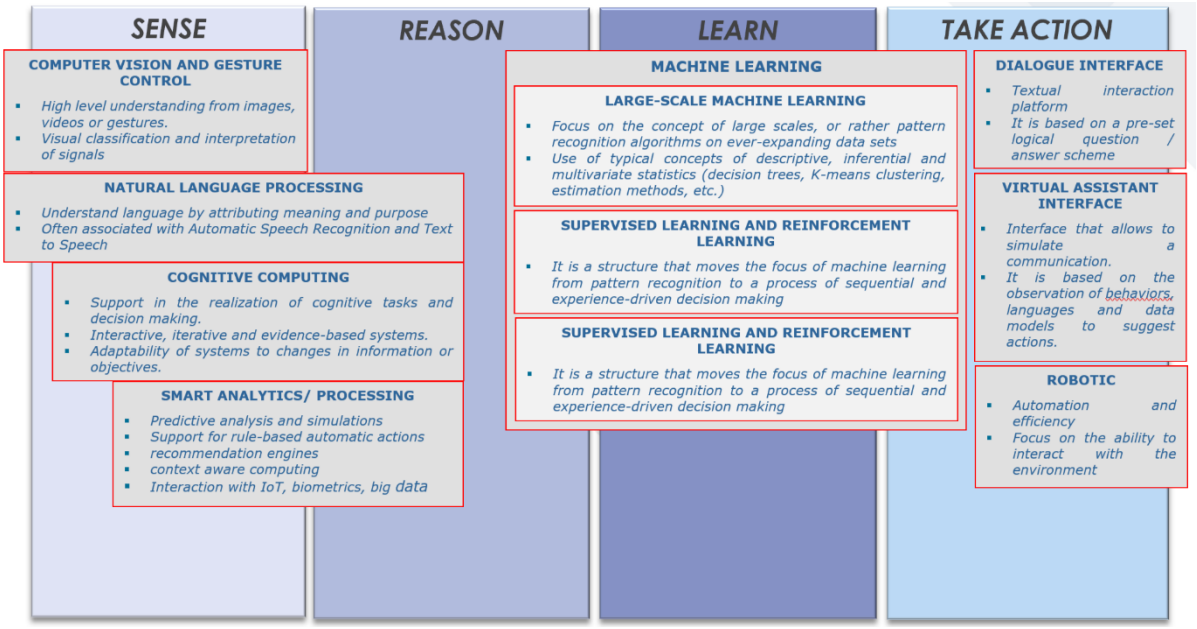
By AI it is generally "*cognitive technologies that rely on large volumes of structured or unstructured data (big data)*" that is meant. In this sense, "cognitive intelligence" is defined as any unstructured data processing, modelling that emulates and/or allows to augment and enhance the cognitive abilities of humans.

For example, here is a non-exhaustive list of some areas of technological research:

- ***Natural language processing***: understands language by attributing meaning and purpose. It is often associated with Automatic Speech Recognition and Text to Speech.
- ***Cognitive computing***: support in the realization of cognitive tasks and decision making. These are interactive, iterative and evidence-based systems.
- ***Smart analytics/ processing***: predictive analysis and simulations. These provide support for rule-based automatic actions (e.g. recommendation engines).
- ***Deep learning and reinforcement learning***: structure that moves the focus of machine learning from pattern recognition to a process of sequential and experience-driven decision making.

[1] McKinsey & Co, Executive's guide to AI.

[2] For instance, the Fair Isaac Company (FICO) created its first credit scoring system in the late 1950s and it was mainly based on statistical analysis.



Please refer to Annex 2.

AI encompasses a set of principles, problem definitions, algorithms, and processes for extracting non-obvious, useful patterns and actionable insight from large data sets. The term data science is closely related to "machine learning" as well as "data mining". Machine learning (ML) focuses on the design and evaluation of algorithms for extracting patterns from data, and data mining generally deals with the analysis of structured data. Data science on the other hand also takes into account other challenges such as the capturing, cleaning, and transforming of unstructured data, the use of big data technologies to store and process big, unstructured data sets, as well as questions related to data ethics and regulation[3].

Please see Annex I for a glossary of common terms.

[3] John D. Kelleher and Brendan Tierney, *Data Science*, The MIT Press Essential Knowledge series, Cambridge, MA, 2018.

Use cases:

As stated above, AI is a polysemous term, encompassing a multitude of realities and flavors. Further to what we have said on the definition of AI (and to our more detailed mapping of the areas of focus in Annex II), we propose to you the following use-cases (further detailed in Annex III).

The use cases are organised in three categories, highlighting the potential areas of opportunities for the banking sector.

- **Enhancing customer interaction and experience:** *e.g.,* chatbots, voice banking, robo-advice, customer service improvement, biometric authentication and authorisation, customer segmentation (*e.g.,* by customized website to ensure that most relevant offer is presented), targeted customer offers;
- **Enhancing the efficiency of banking processes:** *e.g.,* process automation/optimisation, reporting, predictive maintenance in IT, complaints management, document classification, automated data extraction, KYC (Know-Your Customer) document processing, credit scoring, etc;
- **Enhancing security and risk control:** *e.g.,* enhanced risk control, compliance monitoring, any kind of anomaly detection, AML (Anti-Money Laundering) detection and monitoring, system capacity limit prediction, support of data quality assurance, fraud prevention, payment transaction monitoring, cyber risk prevention.

AI in the banking sector: use cases

An additional category of opportunity for AI in the banking sector is the ***creation of new business opportunities and the generation of new sources of revenues:*** *e.g.,* personal finance management, investment analysis, asset allocation, lead generation (*e.g.,* through customer demand analysis, transactional analytics, client network analysis, etc.), churn reduction etc.

AI for customer interaction: the example of robo-advice and handling of customer complaints:

Robo-advice:

Robo-advisors are automated platforms that provide algorithm-driven financial and investment management advice, starting from the information collected from individuals.

Using a combination of different technologies such as cognitive systems, machine-learning and natural language processing, expert systems and artificial intelligence algorithms, the robo-advisor is able to suggest (automatically or with a financial advisor's support) possible investment solutions, tailored to the client's expectations and needs.

This technology enables a great consumer-experience, especially for those customers that prefer digital interactions and the "do-it-yourself" approach, by offering contextualised products and experiences, providing targeted financial advice, and reducing the cost for consumers.

Financial institutions offering investment advice (automated or not) have to respect an array of horizontal and sectoral legislation, both at national and EU level, notably on financial market and wealth management (*e.g.,* MiFID II, Regulation 285/2013 of Bank of Italy).

Customer complaints:

Based on the current regulatory framework, credit or financial institutions have to offer a customer service for customers to send their complaints and are required to solve those claims within a specific timeframe. If customers are not satisfied with the response given to their complaint by the financial institution, they can appeal to national competent authorities (NCAs).

This create a scale issue as large volume of data have to be processed (in a specific timeframe) in order to reply to a claim or complaint.

By using AI technologies (notably natural language processing), banks are able to automatically classify large volumes of unstructured text documents and categorize hundreds of thousands of queries into types and ensure they are routed to the right team for resolution.

This allows for faster resolution of complaints, benefitting the consumer who made the complaints, the financial institution, and the national competent authority (both in case a claim is dealt with quickly and appropriately and thus not escalated, and also as NCAs can rely on these processes).

In addition, it will also help financial institutions to ensure consistency in responses to the same type of complaint, as well as making the auditability of the process easier than with traditional manual classification processes.

AI for banking operation: the example of credit scoring:

It should firstly be noted that credit scoring is not new and was actually one of the first application of statistical modelling in the financial sector[4].

Today, with the objective of measuring the credit worthiness of their clients, banks rely on gathering transactional data, statistical analysis, decision trees, and regression to better estimate a consumer's credit risk and assess whether they will be able to repay a loan.

The use of AI technology enables more accurate scoring and allows for improved access to credit by reducing the risks and the number of false-positives and false-negatives. This will help banks to determine the most suitable debt plan for their customers. It also ensures banks properly manage credit risk, which is essential for financial stability.

This is notably important as there exist a number of supervisory requirements in this area, including the European Banking Authority Regulatory Technical Standards On Assessment Methodology for internal rating based (IRB) Approach[5]. These technical standards aim at ensuring consistency in models' outputs and comparability of risk-weighted exposures.

AI for security purposes: Fraud prevention:

AI is providing great assistance in the detection of fraud and other suspicious activities that are linked to financial crime generally.

Banks traditionally divide fraud into two main categories: external (*e.g.,* attacks on the bank or its clients related to money transfer, identity fraud, online payments, etc.) and internal fraud (*e.g.,* malevolent actions from employees).

A Fraud Detection System (FDS) copes with such threats through feature engineering, supervised, unsupervised, and adaptive learning, by collecting transactional data, analyzing it and learning from it, or through the interaction with FDS maintainers. It is able to identify suspicious events and limit fraudulent activities by suspending or blocking said activities. Fraud prevention proves to be even more efficient when customer profiles are created.

Such AI applications, in addition to saving money for financial institutions, are crucial in the fight against money-laundering and terrorism-financing and other types of financial crimes.

[4] The Fair Isaac Company (FICO) created its first credit scoring system in the late 1950s and it was mainly based on statistical analysis.
[5]https://eba.europa.eu/regulation-and-policy/credit-risk/regulatory-technical-standards-on-assessment-methodology-for-irb-approach

Opportunities and challenges of AI:

Ethical considerations:

Preliminary considerations:

Currently, a lot of the debate is focused on the ethical concerns which are raised by AI. Although we understand the importance to raise and address such issues, we would emphasize the need to ensure these discussions are part of an on-going process. Ethics as a branch of philosophy studies and analyses moral concepts (*e.g.,* justice). As a discipline, many different answers have been provided to the central question of ethics ("Is it wrong or is it right?") and many competing theories have emerged. As such, any "ethical approach" to AI (or technology in general) will be faced with having to answer the same questions philosophers have faced, and position itself within a theory (whether utilitarian, Kantian tradition, rights theories, ethics of communication, etc.). Ethics is subjective and varies between individuals, culture and time. There are thus no easy answers to ethical considerations.

We would thus suggest a flexible, technology-neutral and principle-based approach high-level principles, instead of strict prescriptions which runs the risk of stifling innovation or becoming obsolete as culture and technology evolves.

As we stated above, there is no commonly-agreed definition of what AI is, and we are of the opinion that it is thus important for ethics standards to be **technology-agnostic**: to apply to all technologies alike and not set different standards for different solutions.

For instance, the ethical principle of non-maleficence provides that the use of AI (or similar technology) should not harm individuals. We agree that technology should not be created with harmful intent and should be socially beneficial, meaning that the likely benefits of its use substantially exceed the foreseeable risks overall. A practical approach should be adopted, and the potential harms should be carefully balanced against the positive benefits of the technology.

Indeed, a literal interpretation of this principle ("no individual will ever be harmed") does not consider many situations where individuals will potentially be harmed in a "legitimate and reasonable" way. For example, access to an account might be refused based on potential money-laundering activities. Too strict an interpretation will render the use of AI overly restricted and use-cases of potential benefit to other individuals or to society will be prevented. Continuing from the example above of money-laundering, this potential benefit to society may include the prevention of a crime.

It is also important in our view that policy-makers and society **remain neutral towards the technology** and look at its application, intent and the objectives behind it. More often than not, the same technology can be used differently and yield different results.

We strongly believe in the need to foster reflection and discussion on an ethical framework for AI at a global level. These discussions are of the utmost importance in ensuring consumers' and citizens' trust in the technology.

Finally, we would like to emphasise the need to follow an *Ethics by design* approach when developing new systems. This means having ethical principles in mind from the beginning of the design phase of a new application. We believe that besides complying with regulation it is also necessary to ensure that ethical principles are followed, as proposed in the European Commission High-Level Expert Group on Artificial Intelligence's Ethics Guidelines for Trustworthy AI. You will find below some further thoughts and reflections on issues being discussed in the field of "AI ethics".

Ensuring fairness:

"Fairness in AI" goes beyond the fairness principle provided under Article 5(1)(a) of the General Data Protection Regulation (GDPR)[6], which relates only to fair personal data processing. In general, there is no standard definition of fairness for machine or for human decision-making. Even in simple situations, people may disagree on what is fair or not, since it involves ethical, legal, political, social, historical and cultural considerations, and most of the time involves a trade-off decision.

Addressing fairness and inclusion in AI covers all the use-case life cycle: setting a concrete goal (and thus limiting the number of features that are used in a specific use-case), the use of representative datasets to train and test the model, and the continuous testing of the final system for unfair outcomes.

AI presents opportunities to conduct more objective decision-making. AI can help identify, detect and correct **conscious and unconscious** human biases or errors in judgment. Bias has unfortunately been prevalent in all societies and systems, well before the advent of AI, and no means have been found that would ensure that all individuals remain free from all kinds of bias or that the positives and negatives resulting from AI are evenly distributed. As a consequence, historic data sets used for training of AI systems reflect human biases[7]. In this context, it is worth mentioning that there is a branch of research on AI systems that investigates how to detect biases in data sets[8].

It is of course important to ensure the development of this technology does not reinforce biases and does not heighten unfair discrimination.

Based on this assessment, we believe that the appropriate test would be **whether the AI leads to equal or less unfair bias than an alternative system would**. Expecting absolutely zero bias will not only be inoperable but will prove harmful to the development of AI. AI technology should be seen as a chance to identify and correct unfair bias in future.

Regarding unfair bias, the main source of potential unfair bias is data. It should also be noted that an algorithm and its result can only be as good as the data provided as input ("*garbage-in, garbage out*"). As such, it is important to ensure access to high-quality data as a starting point. Indeed, running data through AI based systems can help to determine the quality of such data and thus achieve high data-quality overall. In order to limit and avoid unfair bias several types of measures can be implemented. For instance:

- Taking large input data samples resulting from different sources: this will not only help to get more accuracy but also to avoid bias that could come from using a single specific source with limited data.

---

[6] Regulation 2016/ 679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[7] This is notably true if the training data comprises of historic human decisions. If it is obtained from historic events, then AI goes beyond human observation biases (also we note that it may be difficult to find historical events/data without any human/social influence). This is exactly what has been observed in some recruiting engine. There has been hiring tools aimed to identify the best candidate for a job. An issue arose when it turned out that the hiring tool prefered men over women as in the historic training data good software developers where mainly men in the company using the hiring tool.

[8] http://www.aies-conference.com/wp-content/papers/main/AIES-19_paper_220.pdf

- Minimising the use of potential biasing variables from the model (*e.g.,* gender, age, sexual orientation, ethnicity, religion, etc.). It should however be noted that these variables may be useful in order to verify (and correct) if there is a bias induced by features correlated with such variables.
- Using factual variables versus opinion-based variables (*e.g.* using the variable of buying a house rather than a propensity to buy a house).
- Encourage the training of employees to identify potentially unfair biases and the deployment of appropriate policies, procedures and control mechanisms.

It should also be noted that algorithms are mathematical processes. Algorithms should not be forced to provide the same results for different types of customers. This would impact on the effectiveness of the AI models whose results simply respond to mathematical processes applied to input data. The use of representative and quality samples will help to minimise the risk of unfair bias. However, if the results of the algorithms happened to have any unfair bias, then as mentioned above this should be detected and solved by establishing subsequent appropriate control mechanisms and policies to ensure fair results for the AI applications. These policies and control mechanisms will help also to avoid any unfair bias in the development phase.

Transparency and explainability:

Although not ethical values in themselves, the concepts of transparency and explainibility are often included within discussions on ethical AI. Transparency is generally understood as a mechanism to ensure the availability of the necessary information to make an informed choice. Explainability is defined by the High-Level Expert Group on Artificial Intelligence as "*the ability to explain both the technical processes of an AI system and the related human decisions (e.g., application areas of a system). Technical explainability requires that the decisions made by an AI system can be understood and traced by human beings*"[9].

Transparency is key to building and maintaining citizens' trust in AI systems. However, it is crucial to find the right degree of transparency *vis-à-vis* individuals, competent authorities, jurisprudence, etc.

We emphasise the need for abstract and practical principles, notably providing enough flexibility to ensure that situations where full transparency cannot be provided or appropriate can be dealt withadequately. To draw again from the case of fraud prevention, detailing the exact processes used and exposing how the technology works could allow the system to be gamed and risk undermining the (socially beneficial) purpose of the AI system[10].

Consideration should also be given to intellectual property. Not only the algorithms, but also the variables used and their weights in the model, (their relevance to generate the outcome), or even how much historical data is used, result from research activities to

[9] Independent High-Level Expert Group on Artificial Intelligence established by the European Commission, *Ethics Guidelines for Trustworthy AI*, 8 April 2019, page 18.

[10] Another example, in the field of customer segmentation would be the possibility to increase the probability to be ranked as a high-income person by using an iOS device. According to the article "On the rise of fintechs – credit scoring using digital footprints", published by the National Bureau of Economic Research in July 2018, "the difference in default rates between customers using iOS (Apple) and Android (for example, Samsung) is equivalent to the difference in default rates between a median credit score and the 80th percentile of the credit score. Bertrand and Kamenica (2017) document that owning an iOS device is one of the best predictors for being in the top quartile of the income distribution".

obtain the best results in each case. Providing free access to all this information could reduce its value and put at risk the incentives to keep improving those activities.

As mentioned above, we do however believe that transparency and explainability are important in maintaining trust in the technology. As such, we need to find ways to deploy some of the most promising AI techniques (such as deep, recurrent neural networks technologies). Despite their low levels of explainability these techniques could be very useful in multiple applications such as detecting financial crime or terrorist financing and cybersecurity, since their use could lead to more accurate predictions.

Different algorithms, operational choices and business scenarios necessarily lead to different types / levels / expectations of appropriate "explainability". It is important to understand that AI models model a complex reality, so it cannot be expected that they "explain" complex reality in a scientific sense. Moreover, one cannot expect that a model perfectly "fitting" this complex reality could provide simple explanations that could be understood by everyone, including lay-persons. If the model describes perfectly a complex situation, a proper explanation of the decision mechanism will most likely be complex as well.

It should also be noted that there could be situation where a trade-off exists between predictive accuracy of a model and the model interpretability[11]. For instance, while a linear regression is typically easier to interpret, it does not have the predictive power of a neural net with millions of parameters, although its results will be harder to explain. However, should this mean that the neural network should not be favoured in some cases? For example, in screening skin cancer: should the diagnosis be made by a single doctor with experience on maybe a few hundred cases, versus a system that can access and analyse millions of diagnosed cases, only because one option can provide an explanation more easily?

In order to ensure a certain level of explainability, a two-layered scheme could be developed based on the use-case and applications. For instance, outcomes from high-accuracy but low-explainability AI models could be complemented by a second set of analysis focused on providing the level of explainability required considering the use-case and users' needs [12].

We believe a **risk-based approach**, based on the impact of the outcomes of the system would be better suited in ensuring transparency and explainability. **Different solutions could be more useful in different situations.** These could range from **high explainability** (for regulatory reasons) **to tested functionality**; which would be use case driven. For example, levels of explainability appropriate to different scenarios could include:

- Explaining the purpose but not the AI decisions to individual / customer;
- Providing a description of input data and optimisation factors to individual / customer on request;

[11] See Institute of International Finance (IIF), Explainability in predictive modeling (November 2018): the U.S. Department of Defense's "Explainable AI" illustrates this point, by plotting current learning techniques and the explainability notion, where it uses predictive accuracy and explainability as two separate axes. "Explainability (notional)" is synonymous with the machine's inability to explain its decisions and actions to users, and "prediction accuracy" with maintaining a high level of learning performance. (U.S. Department of Defense, Advanced Research Projects Agency, 2017).
[12] Techniques such as clustering, or the development of surrogate models, could help to explain the conclusions reached by machine learning models and provide the necessary answers to customers and supervisors.

- Providing short, automatically generated, description of an AI decision to individual / customer on request;
- Having a human analyse an individual / customer query and provide a response.

We believe that two considerations should be made when implementing this risk-based approach:

- Although firms should have a good understanding of their own data processing, their models and how a result has been obtained, the appropriate level of detail provided to data subjects should be based on the **relevance and the impact of the outcomes of the system for individuals**. For instance, an algorithm suggesting music recommendations based on past listening habit would not necessitate the same level of scrutiny as an algorithm suggesting political adverts. In this sense, existing regulations to which firms are subject in the course of their business are also applicable to AI and should drive firms' approach to explainability.
- The **principle of technology-neutrality** should be followed. The use of AI should not increase explainability requirements *per se*.

Several solutions can be implemented in practice to ensure meaningful transparency and explainability: execution and documentation of the learning phase, tests, and simulations; implementation of back testing procedures; alerts in case of unexpected outcomes, etc.

Finally, we would like to highlight that AI can offer new alternatives to the challenge of explainability. There is a lot of on-going research in the field of explainable AI which aim to create new techniques that could produce more explainable models, while maintaining a high level of accuracy.

RECOMMENDATIONS:

- The EBF welcomes the on-going discussion and reflection on ethics and note that these will continue as the understanding of the technology deepens. What is deemed "ethical" varies between individuals, societies, and jurisdictions, and can change over time. It is important to recognize that the purpose of ethics is to help decide what is right or wrong, which is **best accomplished through a set of high-level principles which would leave flexibility in practice.**

- Ethical considerations will necessitate the undertaking of a careful balancing test between competing values and possible outcomes.

- As a general matter, **we suggest that any ethics standards should apply to all technologies and not set different standards for different solutions**. This is critical as there is no commonly agreed definition of AI.

- Finally, we would like to stress the importance to **remain neutral towards the technology** and look at its application and the objectives behind it. Indeed, the same technology can be used very differently and yield very different results[13] and other technologies or even human intervention can raise similar ethical challenges.

- **Transparency and explainability** are important in maintaining trust in the technology. However, they should be **well balanced and a risk-based approach should be preferred**. Explainability should be **based on the impact of the outcomes for individuals.** At the same time**,** using AI should not increase explainability requirements *per se*. **Explainability requirements should be case-based and not technology-based.**

[13] We can take the example of facial recognition. Facial recognition in the hand of a government in order to track and surveil its population would be deemed unethical and raise a number of question and issues. However, the same technology – facial recognition – can be used by banks in order to better and more efficiently tackle fraud claims. The focus should thus, in our opinion, be on the application and policymakers should try to avoid blanket statements.

General considerations on AI:

> *"Unfortunately, while it is easier than ever to run state-of-the-art ML models on pre-packaged datasets, designing and implementing the systems that support ML in real-world applications is increasingly a major bottleneck. In large part this is because* ***ML-based applications require distinctly new types of software, hardware, and engineering systems to support them****. Indeed, modern ML applications have been referred to by some as a new "Software 2.0" to emphasize the radical shift they represent as compared to traditional computing applications. They are increasingly developed in different ways than traditional software—for example, by collecting, preprocessing, labeling, and reshaping training datasets rather than writing code—and also deployed in different ways, for example* ***utilizing specialized hardware, new types of quality assurance methods, and new end-to-end workflows****. This shift opens up exciting* ***research challenges and opportunities around high-level interfaces for ML development, low-level systems for executing ML models, and interfaces for embedding learned components in the middle of traditional computer systems code****."*
>
> *"Modern ML approaches also require new solutions for the set of concerns that naturally arise as these techniques gain broader usage in diverse real-world settings. These include* ***cost and other efficiency metrics*** *for small and large organizations alike, including e.g.* ***computational cost at training and prediction time, engineering cost, and cost of errors in real-world settings****;* ***accessibility and automation****, for the expanding set of ML users that do not have PhDs in machine learning, or PhD time scales to invest;* ***latency and other run-time constraints, for a widening range of computational deployment environments; and concerns like fairness, bias, robustness, security, privacy, interpretability, and causality, which arise as ML starts to be applied to critical settings where impactful human interactions are involved, like driving, medicine, finance, and law enforcement.****"*
>
> *SysML: The new frontier of machine learning systems*[14]

As the above quotation shows, the challenges and considerations on AI are wide-ranging and touch on a number of separate issues. In this next section, we will look at some of the main points we have identified as impacting the full development and deployment of AI in Europe, both generally and in the banking sector.

Taking into account the global perspective:

Throughout this paper, the global perspective should be kept in mind. Consumers must always be protected, regardless of where they access services or who provides them. However, this is not always guaranteed due to the fragmentation of regulation and enforcement in different jurisdictions, as well as the existence of different regulatory frameworks.

From a competition point of view there is a need to ensure a global level-playing field which allow all actors to benefit from the advantage in data training and not only a limited number of actors which could have an unfair advantage due to their access to data through their already-existing infrastructure. Companies commonly referred to as "BigTechs" are at the forefront of AI developments as they have access to increasing amounts of data,

[14] Ratner, Alexander & Alistarh, Dan & Alonso, Gustavo & Bailis, Peter & Bird, Sarah & Carlini, Nicholas & Catanzaro, Bryan & Chung, Eric & Dally, Bill & Dean, Jeff & S. Dhillon, Inderjit & Dimakis, Alexandros & Dubey, Pradeep & Elkan, Charles & Fursin, Grigori & R. Ganger, Gregory & Getoor, Lise & B. Gibbons, Phillip & A. Gibson, Garth & Talwalkar, Ameet. (2019). *SysML: The New Frontier of Machine Learning Systems*.

including the personal data of millions or even billions of data subjects across the world. This gives them a competitive advantage in the development and testing of their AI models compared to other industry players who lack such all-encompassing data sources. A balance should be taken to ensure EU personal data is well protected while AI's potential benefits are attained.

The European Commission has noted this point in its Communication on Artificial Intelligence for Europe, which states that the "*EU should be ahead of technological developments in AI and ensure they are swiftly taken up across its economy*" and that "*without such efforts, the EU risks losing out on the opportunities offered by AI, facing a brain-drain and being a consumer of solutions developed elsewhere*".

In this regard, **the EU could for instance encourage the creation of research centres in the open-source environment.** This should also provide a boost for the EU in the field of AI, not only enabling stronger actors in new or niche markets but should also accelerate the uptake of AI in the EU more generally.

A level playing field in data sharing could be established; allowing some leeway in data gathering for experimentation purposes should also be taken into consideration. Please note that on the question of data sharing and access, the European Banking Federation is currently working on recommendations which will present the views of the European banking industry in relation to this crucial component to the European Data Economy.

The EBF also stresses the importance of knowledge-sharing with other jurisdictions. Attention should be given to avoid a fragmented approach at international level which would risk putting European companies at a competitive disadvantage.

The importance of ensuring citizens' trust and demystifying AI:

One of the main challenges the EBF and its members have identified is the need to proceed to "busting the myths" around AI. This technology has been the focus of many books, articles, and movies – most of them taking a dramatic approach to its development. As is the case with many new technological developments, it is important to rebuild and maintain the users' trust.

A pedagogical approach to AI should be encouraged with positive communication based on pedagogy and training, with a contribution from public authorities and private actors, particularly through partnerships with schools/ universities.

Encouraging investments:

Significant investments in terms of research and development are required should the EU and European actors want to compete on the global stage. Efforts still need to be made to develop, within each organisation, methodologies to industrialize these applications and accelerate the implementation of projects while reducing their cost. In this respect, and to facilitate the scale-up of AI applications in Europe, a proportionate approach should be favoured and no- or low-risk use cases should be subject to lower standards.

Establishing a tax system that will facilitate investments made by banks in research, particularly through partnerships with schools/universities would be appreciated. As highlighted by the European Commission, investments are of the utmost importance to ensure the uptake and development of AI made in Europe. As such, it is also critical to establish a tax system that will facilitate investments made by banks in infrastructure, hardware and software, as well as in terms of depreciation and amortization rules.

Experimentation should further be supported and coordinated across Member States in order to identify, at an early stage, potential barriers to the effective scaling of AI-enabled

solutions across Europe. This may include potential legal and regulatory differences around data, which will need to be addressed to better support pan-European solutions.

Finally, investments in software are restricted for banks in general, but especially in the case of entities based in the EU, where the accounting treatment of software as an intangible asset causes it to be fully deducted from the Core Equity Tier 1 (CET1) when calculating the capital requirements. This is perceived as a significant disincentive for investments in innovation and a major factor of unfair competition.

Platforms and infrastructure:

Developing and deploying AI solutions require investments at EU level in the appropriate computation and communication infrastructure. This notably includes the provision of excellent High-Performance Computing resource in Europe. Indeed, this is essential to the wide availability of next-generation networks to support data collection and analysis.

It could be useful to work towards the creation of a harmonized European research framework, with a level playing field[15] to retain talent and counterbalance the strength of non-European banking or non-banking players; to develop a European ecosystem with governance and steering structures, and material infrastructures which would help and preserve European sovereignty.

Moreover, solutions that are well established in other industries – for example cloud storage – are often difficult to implement in practice in a financial services context. It has to be noted that appropriate technical and organisational safeguards are unavoidable in this context. The use of cloud, as a key enabler technology for artificial intelligence, should be fostered, and barriers to adoption should be eliminated.

The dependence on large IT companies (providers of IT solutions or services, such as cloud services, consulting companies, etc.) should be taken into account. Excessive concentration of the market in the hands of a few players may result in concentration of risks, artificially high prices, limited access to services, and unbalanced business relationships. It further raises the question of sovereignty linked to the control of platforms, technologies and data and the lack of big European players in this space (*e.g.,* cloud services providers, suppliers of AI solutions, etc.).

Access to data[16] for testing and training is another challenge. This requires easier collaboration and data sharing of anonymised data across companies for establishing industry solutions which faces challenges under current **competition law**.

Fostering skills and education:

As identified in much of the literature and debate on AI, the technology carries the potential to change the way the workforce operates. The challenges in this area are manifold:

- Encouraging the development of programs to foster the **skills and knowledge needed by data scientists of today and tomorrow**. Data scientists are central to the development and deployment of AI application. The EU should thus aim to become a "beacon" for talent all across the world. Companies can for example form

[15] For instance, remuneration caps in the banking sector.
[16] Please note that on the question of data sharing and access, the European Banking Federation is currently working on a longer paper presenting the views of the European banking industry in relation to this crucial component to the European Data Economy.

a partnership with a trainee program. Building data labs can be a way to qualify data scientists. In such a data lab different researches can be combined: software development, traditional research, domain and business knowledge, data science, compute science & IT, machine learning, mathematics and statistics. The model of some universities in the United States or in Canada should be studied. The creation of a network of universities in Europe, focusing on data science and its use could be envisaged.

- Although data scientists play a central role in the development of AI, **attention should also be paid in ensuring the training and education of the engineers** needed to support the underlying infrastructure of AI.

- Job displacement also remains a fear. It is important to ensure a **proper system for re-skilling** the individuals whose jobs will be most impacted by the AI revolution. Studies show that many tasks will be impacted by the increasing use of AI and the individuals currently executing these tasks should have access and opportunities to participate in life-long learning initiatives.

As a member of the European Commission's Digital Skills and Jobs Coalition, the EBF is committed in providing support in this area.

We also note that any education initiatives should also aim to create a better understanding of the technology itself and participate in the effort of "myth-busting" around AI and its application. This could start from a young age and could, for instance, take the form of training "toy models" (in a notebook for example) with an illustration of the results and limitations. This could provide a good introduction to what Machine-Learning consists of and would help to debunk the myths surrounding the technology.

Furthermore, we believe another important step would be to ensure **regulators, policy makers and supervisors have the necessary knowledge** and understanding of the technology in order to better assess the challenges, risks and opportunities of AI applications. For this, sharing their knowledge and experience as well as interacting with the industry and stakeholders in general is key.

Accountability and governance of AI:

While AI is not necessarily a new technology, it continues to evolve at a rapid pace and has the potential to change the way the sector operates. It is thus important in our opinion to look at a number of challenges which may arise and at the best remedies to be provided for them.

Firms who develop and deploy AI will most likely need to experiment with different governance approaches which would work for them based on their size, organisational structure, the type of AI applications, risk appetite, etc. Governance approaches could take several forms (*e.g.,* "accountable person(s)" for specific AI projects), but these should be up to the individual firms to determine.

An option for firms to consider as a part of their AI governance could be to ensure that AI systems have a clear statement of "purpose" that the system is trying to achieve. This could be accompanied by a description of the measures which the AI designers have sought to optimise in order to achieve that Purpose. This Purpose would make clear to users / subjects of the AI system what it is trying to achieve. It could also be a tool for the firm to document its intentions *vis-à-vis* auditors or regulators.

The requirements for accountability and auditing should be tailored based on the AI use cases and their potential impact and risks (*e.g.,* requirements for marketing models can be different than those for risk estimation models).

In the banking sector, the "three lines of defense" model already sets a high standard in effective risk management and control. Banks have the structure, and the necessary resources, to guarantee both the appropriate auditability and risk management of AI models. As explained before, banks are expected to provide an extra layer of security for the financial sector due to the prudential framework that other players don't have to comply with.

Finally, we would like to emphasise again the need to follow an *Ethics by design* approach when developing new systems. This means having ethical principles in mind from the beginning of the design phase of a new application. We believe that besides complying with regulation it is also necessary to ensure that ethical principles are followed, as proposed in the European Commission High-Level Expert Group on Artificial Intelligence's Ethics Guidelines for Trustworthy AI.

Ensuring a sound regulatory and legal framework:

An AI fitness check to better grasp the expectations of market participants:

Over the past few years, the legislative landscape regarding technological innovation has evolved, notably under the European Commission's Digital Single Market initiative which led to many positive actions Although much of the new framework was developed without necessarily taking into account the rapid evolution of AI.

The EBF therefore calls for a full-fledged AI fitness check of the current regulatory framework in order to adapt rules where relevant and remove obstacles to the deployment by European companies of truly digital strategies. This exercise could include the proposal for an e-Privacy Regulation, the copyright directive (which comprises parts on text and data mining), the proposal for a platform-to-business regulation, etc.

You will find below some further considerations on horizontal regulations which would benefit from further clarity regarding their interaction with AI.

Data protection and privacy:

A lot has been said about the new data protection regulation and its impacts on innovation. Notably, automated decision-making rules (and rights of individuals) under article 22 of the GDPR may hinder banks from embracing AI to provide better services and safer solutions, since significant manual processes may still be necessary. AI-based decision-making should be subject to oversight and control, but efficiencies may not be realised if human intervention in individual cases becomes significant. In this regard, the exemptions provided by Article 22(2) of the GDPR are welcome.

In general, the "Data minimisation" and "purpose limitation" principles under data protection law stipulates that only the data required to achieve a specific purpose may be used. However, a feature of modern user-centric services is that they cater comprehensively to users' needs, so this purpose focus is becoming increasingly blurred. Furthermore, determining what data is useful to the project at hand may only happen after tests are carried out: no *a priori value* should be attributed to data before machine learning processing has found it useful or not regarding a task. If data is proven not to be useful, by experience, then it should be discarded from an AI product in a perspective of minimization.

Some of the principles set forth in the GDPR are particularly relevant and may pose some challenges for the development and use of AI. One example is the *data minimisation principle* against the volume of data needed to develop accurate AI data analytics. Another is the *purpose limitation principle,* which requires that models developed using AI will not "recycle" information which may prove useful to provide more accurate analysis, if collected for other purposes, etc. The GDPR has set a high standard of data protection in the EU that will help to build trust and confidence on the use of technology. However, the challenges mentioned above need to be addressed in a pragmatic way. The GDPR is a principle-based regulation that relies on a risk-based approach. Supervisory authorities should aim to better understand the interactions among the principles set in the GDPR and the needs of AI developments. This is notably true as it relates to the position of Europe in the global AI field.

Intellectual property:

Careful consideration should be given to intellectual property matters in particular regarding patentability, copyright and ownership's rights. For instance, who should be the holder of the IP rights when a supplier provided an AI solution with the technical and financial support of a bank?

Program code and techniques can be valuable commercial intellectual property: requiring protection and open to "inspection" only from entitled third parties (*e.g.,* supervisory authorities).

A balance needs to be struck between the need for transparency and intellectual property rights and trade secrets issues.

Liability rules:

As with a lot of technologies, especially those with the transformative potential of AI, some questions related to liability have emerged.

The current legal framework surrounding liability should be closely monitored to ensure that respective liability for damages can be properly determined in the context of AI technologies. In this regard, the work conducted by the European Commission Expert Group on liability and new technologies is welcomed as it aims to provide an overview on the applicability of the Product Liability Directive to traditional products, new technologies and new societal challenges, and to assist in the potential development of principles and guidelines for possible adaptations due to new technologies. However, we would note that such adaptation would need to involve a broader involvement of stakeholders in order to ensure applicability, and a flexible approach to limit unintended consequences.

Consumer protection:

Insights gained on the basis of data and AI can help to enhance consumer and investor protection. A broader base of data will enable a customer's personal situation, such as their risk appetite or temporary financial difficulties, to be better and more promptly identified. This could enable consumer and investor protection to be designed more effectively than current instruments allow. Better knowledge of customers also has positive effects on a bank's risk management and thus on financial stability in general.

The declared aim of the policy is to guarantee a fair AI and to avoid unjustified discrimination. However, it is often in the consumer's interest to receive a differentiated offer based on his or her individual characteristics. This can manifest itself, for example, in a needs-oriented service or in a risk-adjusted lending rate. If certain characteristics such as age are classified as discriminatory *per se*, they cannot be used to tailor customer-specific offers. In this respect, a thorough balancing of potential gains and losses by the

legislators and supervisors is required. Furthermore, special attention should be given to the issue of access to data. Access to high-quality data is key for competitive AI technologies. This requires a pro-innovation approach for on-going and future regulatory initiatives, such as copyright and privacy, without compromising on the necessary safeguards of core rights.

RECOMMENDATIONS

- The EBF notes that developing and deploying AI solutions require investment at EU level and the appropriate computation and communication infrastructure to be put in place. The EBF encourages reflection on how to best **incentivise investment in research and development of AI technologies**, notably through tax incentives.

- The EBF recommends encouraging the development of **programs to foster the skills and knowledge** needed by data scientists, engineers, mathematicians, etc. and to ensure a **proper system for re-skilling**.

- **The EBF calls for a full-fledged AI fitness check of the current regulatory framework** in order to adapt rules where relevant and remove obstacles to the deployment by European companies of truly digital strategies.
  For instance, further clarity on the articulation of the data protection framework and AI technologies, striking a balance between transparency and intellectual property rights; taking into account in the liability rules the rapidly changing technological landscape, etc.

AI in the banking sector:

Opportunities in the banking sector:

As stated by the AI HLEG in its draft ethics guidelines, "*AI is one of the most transformative forces of our time, and is bound to alter the fabric of society. It presents a great opportunity to increase prosperity and growth*". One of the main objectives of AI technology is to increase efficiency. However, the main opportunity of AI is to adopt an even stronger customer-centric approach, ensuring that customers are empowered through innovative products and services stemming from the technology. In the banking sector this leads to the following opportunities:

Better customer experiences:

The continually evolving data-driven approach can be applied to and improve many processes that might typically rely on intuition or limited or incomplete information. In compliance with data protection regulation and data usage requirements, AI-supported automated services will bring a wide range of choice in terms of services offered and customization capabilities driven by better use of data through advanced analytics, for example:

- offering contextualised, personalised products and experiences;
- making more accurate credit-worthiness assessments;
- providing better financial advice;
- reducing costs for consumers; and
- better protecting customers from fraud.

In the use-case presented above on customer complaints handling, leveraging AI enables the credit or financial institutions to meet consumer expectations of a high level of service. It also ensures complaints are treated efficiently and in a timely manner. In the UK, where 22 categories of serious complaints are reportable to FCA, AI has helped reduce both the number of complaints filed to the FCA and resolution times for customers.

Democratization of financial services:

Through the lowering of the complexity and costs associated with some services (*e.g.,* advisory services and credit provision services), it is expected that AI will lead to easier access to financial services. For instance, it is expected that robo-advisor's main contribution will be bringing portfolio investment to client groups who previously had no access to it. Furthermore, the ubiquity/ geographic scope of financial advice availability will also improve. Through expert systems and artificial intelligence, financial institutions are able to reach outside the usual pool of investors and offer advice-services to new customers. This technology also enables ideal portfolios to be build and monitored more efficiently.

We would like to stress that increased automation will not remove the possibility of a personal contact for clients with a financial adviser. Banks will continue to cater for the digital-savvy and for traditional client demographics. Financial institutions will still provide access to human advisers to assess best approaches to financial structuring and to cater for very specific or complex customer needs, together with continuing services for those customers that prefer personal interaction.

Furthermore, it should be noted that AI technologies enable a better access to credit through higher accuracy of the models used for credit-worthiness assessments, thus reducing the risks of false-positives and false-negatives. This will help ensure that banks provide loans to those customers that will be able to repay them and ensure that

customers who cannot do not enter into over indebtedness. It also ensures banks properly manage credit risk, which is essential for financial stability.

Gains in term of efficiency and robustness in banking processes:

These technologies can be used to improve the focus of resources and sales on the right customers at the right time, leverage better/more sophisticated products with lower costs, etc.

As stated above, most banks use automated agents to augment client's interaction. Automated agents can be an effective tool to lower the costs of repetitive tasks, to provide more consistent execution, and to free up some time for managers to focus on higher value-added areas of financial planning and wealth management. It is also an opportunity to meet customer's increasing demand for faster services. AI can also be used to improve the robustness of processes by making them more systematic.

New business opportunities:

The potential of data analytics and AI allows banks not only to improve customer services and raise efficiency but also create new customer propositions in the traditional business segments as well as new fields of activity beyond banking. This can contribute to sources of revenue, and thereby compensate for declining profitability due to low interest rates and increasing competition from nonbanking sector.

Better risk management:

Data analytics contributes widely to a better internal understanding of banks' activities, a more effective risk management, and an improved monitoring of compliance. Financial institutions of all types, whether incumbent, challenger or digital-only, are investing great resources to deploy such services within the framework of already existing regulation, including, but not limited to CRD IV, MiFID II and the GDPR. Banks and other financial institutions have indeed long been custodians and users of data and have well established systems and protocols for using and protecting sensitive data on a large scale, compared to other relatively new technology providers. Being supervised from two angles (data protection and operational risk perspectives), banks have integrated the management of this risk into their risk framework.

The use of AI could fall within the scope of Article 19 of the 4th EU AML Directive: "*New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering*".

AI could allow banks better control and raise the visibility of all data they hold, including solutions for data ranking or cartographies regardless of source: data base, transactions, emails, excel files, etc. This supports compliance with conduct of business rules, such as MiFID II, short-selling, etc.

Furthermore, Anti-Money Laundering/Financial Crimes/Fraud are complex and persistent challenges for financial institutions. Segmentation is source of better AML/FC outcomes. As presented above, AI may transform the current segmentation step process, help them reduce the burden and increase the controls. The combination of AI and, more specifically, machine learning may be very useful in conducting suspicious activity monitoring and transaction monitoring.

The cost of frauds associated to non-cash means of payment can be quite high: in the Single European Payment Area (SEPA), it is estimated that non-cash payment fraud caused 1.44 billion euros loss in 2013[17].

Moreover, the risk associated with fraud is almost certainly not going to decrease. As the digital space is growing at a rapid pace, fraudsters may take advantage of new system's vulnerabilities and people's lack of digital awareness. Put this all together and it is a recipe for scaling-up fraudulent activities. Frauds, and especially cyber-attacks, are a growing concern not only for banks but across all other industry. Today, hackers (black hats) are offering hacking kits for relatively small amounts of money on the "Dark Web".

Having a more secure system means increasing trust in the bank for both clients and financers. Risk of fraud has, like all other risks, an influence over the interest rates with which banks refinance themselves and thus has an impact on their profitability. This potential distrust could slow economic activity or undermine investments.

Prevention of systemic risks:

AI and the underlying technologies must be part of "responsible innovation" processes as they could disrupt the stability and security of the financial system.

All the risks must be taken into account: operational, reputation, contagion, security of financial transactions, solvency and credit, in order to avoid situations like those observed in the field of high frequency trading (HFT). Examples here include the Flash crash of the Dow Jones index in May 2010, as well as risks of manipulation.

At the same time, AI has the potential to be used to better detect and manage these risks.

Increased cybersecurity:

The security needs of financial institutions are unique, as cybercriminals constantly target attacks at entities where they can experience the most financial gain. Meanwhile, consumers trust their institutions to protect their confidential information.

By leveraging AI, financial institutions can automatically analyze massive amounts of data traffic to detect anomalies which may be threats. The more data that is analyzed, the more effective AI becomes: developing familiarity with typical behaviour patterns and recognizing suspicious activity faster which leads to more efficient alert systems and threat remediation.

Analyzing high volumes of security data allows machine learning algorithms to anticipate future attack vectors based on existing data. With AI, banks can constantly improve their security posture.

Ensuring a sound regulatory framework for the banking sector:

In addition to horizontal rules applicable to all sectors, the banking industry is subjected to additional specific regulation which covers the use of AI in the sector. Indeed, many specific requirements of banking regulations are already affecting the lifecycle of AI in several ways, as highlighted throughout this paper.

We will develop below a few areas where banks suffer from a competitive disadvantage when compared to other market participants which are not subject to the same regulatory framework (e*.g.,* prudential requirements) or where the regulation could limit the use of

[17] https://www.consilium.europa.eu/en/press/press-releases/2018/03/09/fighting-fraud-with-non-cash-means-of-payment-council-agrees-its-position/

AI in the provision of financial services (*e.g.,* prescriptive requirements regarding creditworthiness assessment under Mortgage Credit Directive).

In the past few months several supervisory authorities have noted that there may be gaps that will be created by the rapid evolution of the technology and by the rapid growth of data sets and data processing power. However, we would encourage supervisors and policy makers to ensure the suitability (or lack thereof) of existing requirements on governance and risk management regarding the use of AI. This should first be assessed before any new measures are considered or introduced. In order to adapt rules where relevant and remove obstacles to the deployment by European companies of truly digital strategies, a full-fledged AI fitness check of the current regulatory framework should be undertaken, accompanied by a comprehensive analysis of national and European legislation to detect and assess potential divergences across national regimes as well as potential gaps, overlap and the potential impact of legislation on the level playing field and on consumer protection.

Particular attention should be paid to new market participants that are not yet adequately covered by the current regulatory framework and respect the principle of "*same services, same risks, same rules and same supervision*".

As mentioned above, the banking sector operates with specific requirements which some other and newer market players are able to bypass due to their categorization as "not banking institutions" although they provide the same services.

We would thus encourage supervisors and policy-makers to keep in mind the principle of **"same services, same risks, same rules and same supervision"** when looking at AI. The focus should always be on the technology, the outcomes and potential impact of a specific application rather than on the entity who is providing it. Ensuring a level playing for all industries and geographies is of capital importance to ensure the uptake of AI in the European banking sector.

Data use and data quality:

Several pieces of EU legislation aim at providing the highest consumer protection levels while also ensuring financial stability. These laws require banks to undertake an assessment of their customers to ensure their eligibility for certain products or services. This is notably the case for the Consumer Credit Directive and the Mortgage Credit Directive which require firms to perform a credit worthiness assessment of the applicant before granting the loan / mortgage (as mentioned above in the use-case on credit scoring). This creditworthiness assessment is frequently subject to prescriptive requirements such as those imposed in EBA's "Guidelines on creditworthiness assessment" under the MCD[18]. In such situations, the capacity of financial players to innovate is reduced since alternative uses of data for creditworthiness assessments are constrained by those requirements.

Under the second Markets in Financial Instruments Directive financial institutions and investment firms are also required to undertake a suitability and appropriateness evaluation in order to propose to consumers the products that can meet the clients' profile considering the financial situation of the client. This includes the client's investment knowledge, experience, and investment objectives.

The above-mentioned use-case on robo-advice would be considered as advice activities falling under the remit of MiFID 2. As such, when developing and introducing robo-advice

[18] https://eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-creditworthiness-assessment

applications to the market, the financial institution providing this service would be required to ensure the performance of a suitability assessment.

It should also be borne in mind that, compared to other industries, banks are subject to legal and regulatory obligation which oblige them to provide for high data quality. Risk Data Aggregation requirements are a clear example, as they provide principles on how to organize, verify and maintain information, by which banks should abide[19].

Finally, all initiatives so far to open data and develop technical standards for this have only targeted the financial sector such as the Payment Services Directive 2. This creates an uneven playing field with other sectors.

Prudential requirements:

Banks have strict capital requirements,[20] including the need to have models to measure their solvency based on comparing their assets and the risks they take.

Prudential regulation allows banks to develop internal models for calculating capital consumption, which are then approved by supervisors on a case-by-case basis. These processes of approval, which sometimes take a long time, come prior to any use of a new internal model by a bank. This is challenging for AI usage, since this previous approval requires supervisors to fully understand the implications and inner workings of the internal model. A review of the supervisory approach to this is necessary to guarantee a full uptake of AI by banks. It is of paramount importance for supervisors to have a full understanding of the technology to assess and approve AI-based internal models.

Under strict prudential rules, banks also need to be able to measure, monitor and manage all their sources of risk. Operational risk here includes cybersecurity and data protection risks. The banking supervisory authorities add a layer of security to cybersecurity and data protection authorities through their capacity to recommend certain requirements or provide capital to reinforce the banks' robustness in case of an event. However, this put additional burdens on banks as opposed to non-regulated new market players. To provide for a level playing field a more horizontal approach is needed.

As stated above, investments in software are restricted for banks in general, but especially in the case of entities based in the EU, the accounting treatment of software as an intangible asset causes it to be fully deducted from the Core Equity Tier 1 (CET1) when calculating the capital requirements. This is perceived as a significant disincentive for investments in innovation and a major factor of unfair competition.. We welcome the amendments introduced in the final text of the CRD/ CRR Review[21] that should exempt certain investments in software assets from this deduction. We believe this is a positive step that will help to promote innovation and foster investments from the banking sector in AI research and development.

---

[19] Basel Committee on Banking Supervision, "*Principles for effective risk data aggregation and risk reporting*", January 2013

[20] "CRD IV package" (Capital Requirement), including EU Directive 2013/36/EU and the EU Regulation 575/2013: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0036&from=EN and https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0575

[21] CRD/ CRR Review: "Institutions shall deduct the following from Common Equity Tier 1 items intangible assets with the exception of prudently valued software assets whose value is not negatively affected by resolution, insolvency or liquidation of the institution" (Article 36.1(b)).
"EBA shall develop draft regulatory technical standards to specify the application of the deductions referred to in (…) including the materiality of negative effects on the value which do not cause prudential concerns" (Article 36.4).

Remuneration:

Further to the points made on the prudential requirements of banks, there is an area that creates a competitive disadvantage for financial institutions: remuneration policies.

EU Directive 2013/36/EU provides strict rules with regards to remuneration policies and practices in credit or investment firms. Further to this directive, the European Banking Authority has published guidelines on sound remuneration policies[22] which provides for the correct and consistent calculation of "*the so called 'bonus cap' by setting out specific criteria for mapping all remuneration components into either fixed or variable pay and detailing how specific remuneration elements such as allowances, sign-on bonuses, retention bonuses and severance pay are to be recognised over time*".

These rules put financial institutions at a competitive disadvantage when trying to hire or retain the valuable talents need to develop AI solutions.

Hosting and processing of data – the use of cloud computing services by the banking industry:

Another area where banks suffer from a disadvantage compared to other market players is in the hosting and processing of data. When a bank wishes to use a cloud service to host its data it needs to comply with specific rules and requirements regarding security, data protections, auditability, etc.[23] Some national supervisory authorities also require a notification (*de facto* a process for approval) before a migration to a cloud service provider of data used for banks' essential functions.

Additionally, the more general framework of outsourcing[24] (which also includes outsourcing to cloud service providers), generates requirements for banks using third-party services, especially if these relate to essential functions (*e.g.*, providing credit). The outsourcing bank has to keep responsibility of the outsourced services and should retain rights to audit, control the outsourcing chain, etc.

[22] https://eba.europa.eu/documents/10180/1314839/EBA-GL-2015-22+Guidelines+on+Sound+Remuneration+Policies.pdf/1b0f3f99-f913-461a-b3e9-fa0064b1946b

[23] European Banking Authority recommendations on outsourcing to cloud service providers, https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf/e02bef01-3e00-4d81-b549-4981a8fb2f1e

[24] CEBS guidelines on outsourcing (currently under review by the EBA), https://eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf

RECOMMENDATIONS:

- The principle of **"same services, same risks, same rules and same supervision"** should be enforced: any actions undertaken should strive to remain neutral and look at the technology an its use instead of focusing on the entity providing it. While banks have to comply with a very strict regulatory framework, other companies and non-banking players (including big IT companies) who enter the field to propose similar services do not. The principle of equality is not respected.

- **Measures aimed at data sharing, experimentation and cloud usage** should be taken to foster innovation in banking services and AI adoption[25].

- **Collaboration and dialogue between the European Commission and said supervisory/regulatory authorities should thus be encouraged**.

- The **suitability of existing requirements on governance and risk management** should first be assessed before any new measures are considered or introduced.

- A comprehensive analysis of national and European legislation should be carried out. In this exercise, the EBF believes that it would be very important not only to detect and assess potential divergences across national regimes, but also their potential impact on the level playing field and on consumer protection.

[25] Please note that on the question of data sharing and access, the European Banking Federation is currently working on a longer paper presenting the views of the European banking industry in relation to this crucial component to the European Data Economy.

Summary of EBF recommendations and main challenges:

- The EBF welcomes the on-going discussion and reflection on ethics and notes that these will continue as the understanding of the technology deepens. What is deemed "ethical" varies between individuals, societies, and jurisdictions, and can change over time.
- It is important to recognize that the purpose of ethics is to help decide what is right or wrong, which is **best accomplished through a set of abstract and high-level principles which would leave flexibility in practice.**
- Ethical considerations will necessitate the undertaking of a careful balancing test between competing values and possible outcomes.
- **We suggest that any ethics standards should apply to all technologies and not set different standards for different solutions**. It is important to **remain neutral towards the technology** and look at its application and the objectives behind it.
- **Transparency and explainability** are important in maintaining trust in the technology. However, they should be **well balanced, and a risk-based approach should be preferred.**
- The EBF notes that developing and deploying AI solutions require investment at EU level and suggest to leverage the EU budget to ensure the appropriate computation and communication infrastructure be put in place as well as in order to encourage the development of **programs to foster the skills and knowledge** needed by data scientists, engineers, mathematicians, etc. and to ensure a **proper system for re-skilling**.
- The EBF encourages reflection on how to best **incentivise investment in research and development of AI technologies**, notably through tax incentives.
- Experimentation should further be supported and coordinated across Member States in order to identify, at an early stage, potential barriers to the effective scaling of AI-enabled solutions across Europe.
- **The EBF calls for a full-fledged AI fitness check of the current regulatory framework** in order to adapt rules where relevant and remove obstacles to the deployment by European companies of truly digital strategies (*e.g.,* data protection framework, intellectual property, liability rules, etc.). This fitness check should be accompanied by a comprehensive analysis of national and European legislation to detect and assess potential divergences across national regimes as well as potential gaps, overlap and the potential impact of legislation on the level playing field and on consumer protection.
- The principle of **"same services, same risks, same rules and same supervision"** should be enforced: any actions undertaken should strive to remain neutral and look at the technology an its use instead of focusing on the entity providing it. While banks have to comply with a very strict regulatory framework, other companies and non-banking players (including big IT companies) who enter the field to propose similar services do not. The principle of equality is not respected.

  Collaboration and dialogue between the European Commission and said supervisory and regulatory authorities should thus be encouraged to ensure consistency and alignment across Europe and across sectors.

MAIN CHALLENGES FACING THE BANKING INDUSTRY IN DEALING WITH AI:

- **Ethical concerns**: the EBF welcomes the on-going discussions on ethics and recommends the *Ethics by design* approach and a set of **abstract and high-level principles** to allow for flexibility in practice.
- **Lack of transparency**: the EBF recommends a **risk-based approach** to transparency and explainability, based on the impact of the outcomes of the systems.

- **Asymmetric regulation between industries**: the EBF recommends enforcing the principle of "**same services, same risks, same rules and same supervision**";
- **Asymetric regulation in a global context**: the EBF encourage the creation of research centres in an open-source environment and notes the importance of ensuring a strong AI eco-system in Europe;
- **A dated regulatory framework**: the EBF recommends a **full-fledged AI fitness check** of the current regulatory framework in order to adapt rules where relevant and remove potential obstacles

- **Ambivalence and low perception of AI relevance and context in the banking sector**: the EBF belives an important step is to ensure regulators, policy makers and supervisors have the necessary knowledge and undertanding of the technology and its impact in the banking industry. The EBF recommends **collaboration and dialogue** between the European Commission, banking supervisors and regulators, data protection authorities, and lawmakerss as well as with the industry.

- **Education** : the EBF recommends encouraging the development of **programs to foster the sills and knowledge** needed by data scientists, engineers, mathematicians, etc. and to ensure a **proper system for re-skilling**.
- **Competition with other sectors** for recruiting: the EBF would welcome further analsysis on the way the banking sector's **remuneration rules** impact its ability to compete when recruiting data scientists.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

Annex I

Glossary of common terms and recurrent concepts[26]:

Algorithm: an algorithm is a process or set of rules to follow in order to complete calculation or solve problems.

Big data: Big data are often defined by the 'three Vs': the extreme volume of data, the variety of the data types, and the velocity at which the data must be processed. Big data has led to the development of a range of new databases technologies.

Data (structured and unstructured): In its most basic definition, a piece of data is an abstraction or measurement from a real-world entity (*e.g.,* person, object, event). Structured data refers to data that can be stored in a table: every instance in the table has the same set of attributes. Conversely, unstructured data refers to a type of data where each instance in the data set may have its own internal structure (*e.g.,* text data are often unstructured and require a sequence of operations to be applied to them in order to extract a structured a representation for each instance).

Machine learning: Set of algorithms, or execution rules, to solve a problem(s) whose performance improves with experience (data) without hindsight. Deep learning is a subcategory of machine learning. Machine learning is mainly used for scoring, fraud detection, portfolio management, risk assessment.

Model: In the context of machine learning, a model is a representation of a pattern extracted using machine learning from a data set. Consequently, models are trained, fitted to a data set, or created by running a machine learning algorithm on a data set. Popular model representations include decision trees (a type of prediction model that encodes *if-then-else* rules in a tree structure) and neural network (see below). A prediction model defines a mapping or function from a set of input attributes to a value for a target attribute. Once a model has been created, it can be applied to new instances from the domain.

Neural network: A type of machine-learning model that is implemented as a network of neurons (simple processing units). A neuron takes a number of input values as inputs and maps these values to a single output activation.

Deep learning: Deep learning is a subcategory of machine learning. A deep-learning model is a neural network that has more that two layers of hidden units – or neurons. Deep networks are deep in terms of the number layers of neurons in the network.

Supervised and unsupervised learning: supervised learning is a form a machine learning in which the goal is to learn a function that maps from a set of input attribute values for an instance to an estimate of the missing value for the target attribute of the same instance. In contrast to supervised learning, in unsupervised learning no target attribute is defined in the data set. The goal is to identify regularities in the data.

[26] John D. Kelleher and Brendan Tierney, *Data Science*, The MIT Press Essential Knowledge series, Cambridge, MA, 2018.

Annex 2: areas of technological research

SENSE

COMPUTER VISION AND GESTURE CONTROL

- *High level understanding from images, videos or gestures.*
- *Visual classification and interpretation of signals*

NATURAL LANGUAGE PROCESSING

- *Understand language by attributing meaning and purpose*
- *Often associated with Automatic Speech Recognition and Text to Speech*

COGNITIVE COMPUTING

- *Support in the realization of cognitive tasks and decision making.*
- *Interactive, iterative and evidence-based systems.*
- *Adaptability of systems to changes in information or objectives.*

SMART ANALYTICS/ PROCESSING

- *Predictive analysis and simulations*
- *Support for rule-based automatic actions*
- *recommendation engines*
- *context aware computing*
- *Interaction with IoT, biometrics, big data*

REASON

LEARN

MACHINE LEARNING

LARGE-SCALE MACHINE LEARNING

- *Focus on the concept of large scales, or rather pattern recognition algorithms on ever-expanding data sets*
- *Use of typical concepts of descriptive, inferential and multivariate statistics (decision trees, K-means clustering, estimation methods, etc.)*

SUPERVISED LEARNING AND REINFORCEMENT LEARNING

- *It is a structure that moves the focus of machine learning from pattern recognition to a process of sequential and experience-driven decision making*

SUPERVISED LEARNING AND REINFORCEMENT LEARNING

- *It is a structure that moves the focus of machine learning from pattern recognition to a process of sequential and experience-driven decision making*

TAKE ACTION

DIALOGUE INTERFACE

- *Textual interaction platform*
- *It is based on a pre-set logical question / answer scheme*

VIRTUAL ASSISTANT INTERFACE

- *Interface that allows to simulate a communication.*
- *It is based on the observation of behaviors, languages and data models to suggest actions.*

ROBOTIC

- *Automation and efficiency*
- *Focus on the ability to interact with the environment*

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

Annex III

Detailed use-cases

AI for customer interaction: the example of robo-advice and handling of customer complaints:

Robo-advice:

Purpose / what problem is being solved

Robo-advisors are automated platforms that provide algorithm-driven financial and investment management advice (investment strategy), starting from the information collected from individuals. In most cases, robo-advisors could recommend humans on how to best proceed, while there are some cases in which they may automatically make the financial transactions (*e.g.,* portfolio management and rebalancing).

Moreover, we talk about "robo-for-advisors" in the case of platforms that support human advisors (financial expert managers) in assisting clients for investment decisions.

Consequently, robo-advice platform providers could have a Business to Consumers (B2C) or a Business to Business (B2B) business model with a very different approach, costs and target clients. In the B2C case, the "on boarding" procedure to acquire the client (*e.g.*, fully or partially digital) should be considered an integral part of the use case.

Technology

Robo-advisors may be put in place through the combination of different technologies, the most important ones are:

1) **Cognitive systems**: support in cognitive tasks and decision making.
2) **Task automation tools**: interactive, iterative and evidence-based systems.
3) **Machine Learning**: tools to support the machine capabilities in learning, depending from the implementation, it could be possible to refer to:
    - large-scale machine learning (for large scale data sets)
    - supervised learning and reinforcement learning (supporting a process of sequential and experience-driven decision making
    - deep learning (algorithms based on neural networks).
4) **Natural language processing**: understand language by attributing meaning and purpose.
5) **Smart analytics/ processing** (Predictive analysis and simulations, support for rule-based automatic actions, recommendation engines, context aware computing)

Other technologies could be integrated to the robo-advisor platform, in particular regarding user interface, data visualization and operational support.

Process

The process starts from the collection of customer information, either directly or indirectly through the combination of different data-sources. The customer on-boarding can be fully automated, without the need for human intervention (at least for client identification)[27].

The client can select short/long term investment objectives (*e.g.,* retirement, university expenses, house purchasing, etc.) including capital growth and income integration, risk propensity (*e.g.,* assessed as per MIFID II).

Through expert systems and artificial intelligence algorithms, each objective could be associated with an ideal investment portfolio, built and monitored leveraging on the integration between the robo-advisor capabilities and the support of bank specialists.

Through an algorithm, built on historical training data, that combines risk propensity, time horizon and purpose, the robo-advisor is able to suggest (automatically or with a financial advisor's support) potential investment solutions, tailored to the client's expectations and needs. Portfolios can be reviewed periodically (unless the market conditions require more frequent rebalancing).

The process acts as a consultancy, so the customer must authorize from time to time the purchase and sale operations suggested by the advisor. It can do it autonomously or, at its discretion, with a human operator's support.

Maturity and (possible) evolution of the technology

Currently, most of the banks are able to use robo-advisors to augment, not replace, client interaction.

In the future, it could be inspiring to leverage analytics and smart machines to work even more in conjunction with banking specialist and advisors. In this way, clients' needs for customized and proactive advice will be better addressed. Furthermore, banks will be able to strengthen the provision of value-added services in an increasingly competitive industry.

Benefits for consumers and institutions:

Furthermore, such application can bring better consumer-experience through a wide range of choices in terms of services offered and customization capabilities driven by, better use of this data through advanced analytics *e.g.,* through:

- offering contextualised, targeted products and experiences;
- providing better financial advice;
- reducing costs for consumers; etc.

Regulatory framework and analysis:

In this particular use case, in addition to the European Data Protection Framework (and notably Regulation (EU) 2016/679, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data – GDPR), there exist a number of European and National regulation on financial market and wealth management (e.g., MiFID II, Regulation 285/2013 of Bank of Italy).

In order to be able to use natural language processing in customer front-ends, legal requirements on customer information and consent must be adapted to fit this purpose.

[27] The European Commission is currently looking at these remote on-boarding and KYC processes in its Expert group on electronic identification and remote Know-Your-Customer processes.

In general, the 'Data minimisation' and 'purpose limitation' principles under data protection law stipulates that only the data required to achieve a specific purpose may be used. However, a feature of modern user-centric services is that they cater comprehensively to users' needs, so that the purpose focus is becoming increasingly blurred.

The actually right 'privacy by default' rule leads in practice to providers not recognising their users in the digital world and being unable to proactively personalise their service. From the 'analogue' world, *e.g.,* bank branches, we know, however, that customers would in fact like to be recognised and personally looked after.

There is also a lack of transparency or knowledge by the customer about how their data is used. Controllers are required to provide the customer/data subject with detailed information on the processing of their data. However, comprehensive data privacy statements tend to quickly produce information-fatigue among customers. The degree of detail introduced by the GDPR as well as the 'juridification' of its language to avoid the risk of penalties diminish clarity and comprehensibility for the customer, thus undermining the original purpose.

Hence, we would suggest a more practical approach and call for the creation of a framework fostering the use of data while at the same time ensuring strong data protection for the data subjects:

1. Qualifying the 'data minimisation' principle, *e.g.,* by generally allowing the use of publicly available data (with and without reference to persons).

2. Freeing the 'purpose limitation' principle from an overly tight framework:

- enabling the customer to accept various processing purposes, possibly through one step in the basic settings or at the start of use of a comprehensive service (with scope for subsequent adjustment where required);
- moving in the medium term away from the outdated, since non-operationalisable, 'purpose limitation' rule towards inclusion of (and user consent for) certain application classes, providers, regions or other specifically designated types of data use that the user can understand.

3. Accepting two-level information communication approaches; *i.e.,* brief and concise information to provide an overview (level 1) and further detailed information upon request (level 2) – please see also Position II below.

Customer complaints:

Purpose/Problem being solved

The UK Financial Conduct Authority defines a complaint as "*any oral or written expression of dissatisfaction, whether justified or not, from, or on behalf of, a person about the provision of, or failure to provide, a financial service or a redress determination, which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience*"[28]. This leads to large volumes of data.

Credit or financial institutions have to offer a customer service for customers to send their complaints and are required to solve those claims following some regulatory requirements. If customers are not satisfied with the response given to their complaint, they can appeal to national competent authorities.

[28] https://www.handbook.fca.org.uk/handbook/glossary/G197.html

Given the volumes of data, Artificial Intelligence can help to prevent complaints and to enhance complaint handling and replying, reducing the number of complaints that are addressed to national competent authorities.

The ultimate goal would be to provide a seamless experience to customers to address their complaints in real time or even address queries before they become complaints.

What technology is being used?

In order to process the complaints, the credit of financial institution uses machine learning and big data technology.

Currently, the technology uses natural language processing to automatically classify large volumes of unstructured text documents and categorize hundreds of thousands of queries into types: from general questions to complaints.

Maturity and (possible) evolution of the technology:

Some banks actively use this technology described above to understand all the queries received and to route them to the right team for resolution.

In the future, some banks are exploring the use of voice analytics and computer vision to understand customer complaints in real time. This would not only accelerate the resolution process, it would also ensure a more seamless user-experience.

Benefits for consumers and institution (and regulators where applicable):

Mainly, this technology addresses a scale problem. As mentioned above, given the volumes of data and the need to address complaints in a timely manner, leveraging AI technology helps the credit or financial institution to address all queries coming from customers and route to the right team for the right resolution.

This allows for faster resolution of complaints, benefitting the consumer (who made the complaints), the financial institution and the national competent authority (both in case a claim is dealt with quickly and appropriately and thus not escalated, and also as NCAs can rely on these processes as well).

Regulatory framework and analysis:

There exist a framework for complaints handling for credit or financial institutions at both EU and national level.

The European Banking Authority states that if a customer is not satisfied with the products or services provided by a credit or financial institution, they should first contact the customer service department of the respective institution[29].

The EBA has published guidelines for the handling of complaints but this still falls on national competent authorities[30]. In the UK for instance, complaints as defined by the Financial Conduct Authority (FCA – the UK national competent authority) need to be reported to the FCA[31].

[29] https://eba.europa.eu/consumer-corner/how-to-complain

[30] https://eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-for-complaints-handling-for-the-securities-esma-and-banking-eba-sectors

[31] https://www.handbook.fca.org.uk/handbook/DISP/1/3.html

AI for banking operation: the example of credit scoring:

Purpose / what problem is being solved:

The objective of rating models is to measure the credit worthiness of the clients.

The Retail (which include both Mortgage and Other Retail segment) and SME Retail rating models assign a rating class to every client and at every rating class is associated a Probability of Default calculated statistically, using different data sources and calibrated through a long-run default rate.

Technology:

Both the Retail and SME Retail models are estimated through a consolidate and validated approach, the main steps are:

1) Data gathering (sample, target variable, ratio calculation)
2) Univariate analysis on the long list
3) Correlation analysis
4) Multivariate analysis and model estimation through logistic regression
5) Calibration on the long run default rate

The points 1-4 regard the risk differentiation, the point 5 regards the risk calibration.

Process:

The Retail rating model has been designed in order to take advantage of the widest informative set at disposal with reference to the customer: social – demographic information, behavioral data, internal/external credit bureau, asset under management, current account movements and products characteristics. The informative set is constantly updated, in order to determine a monthly rating calculation, available to both the business and the credit processes for a proactive credit approach.

This model is differentiated between customers and designed by modules. The model design by modules has allowed to differentiate each model depending on the available informative set referred to each customer typology, originating three separated rating models: customers with credit line, customer without credit line and new customers.

The main structure of the model consists in the integration of different scores that brings to an Integrated score on which calibration is applied to obtain an Integrated Rating.

Finally, in order to ensure adequate conservatism in the final estimates and address uncertainties due to data deficiencies and potential estimation errors, we applied a number of conservative adjustments throughout the development process.

Regarding the "rating philosophy", the retail rating model, can be defined as a hybrid model, in fact it incorporates both "Point-In-Time" components (*i.e.,* behavioral variables) as well as "Through The Cycle" components (*i.e.,* calibration through a long run default rate).

The SME Retail model is applied to small and medium sized enterprises with granted of less than euros 1 million and with turnover of less than euros 2.5 million.

The model is composed of a quantitative and a qualitative module. The variable selection process and the structure of the quantitative module is similar at the Retail model.

The qualitative module consists of a questionnaire filled in by the Relationship Manager and integrated with the statistical rating.

Maturity and (possible) evolution of the technology:

The credit risk department could adopt new data sources (big data), including external data (*e.g.,* social data, web sentiment, market place), and new data analysis techniques such as Machine Learning (*e.g.,* neural networks, random forest, gradient boosting) to develop new alternative models.

Currently an evaluation of the possible costs/benefits of the applications of these new data sources and techniques is carried on in terms of accuracy improvements, model explainability and maintenance capacity compared to the logistic regression.

Regulatory framework and analysis:

In this particular use case, in addition to data protection rules, the bank also has to comply with a number of European and national[32] regulations, including Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 (on prudential requirements for credit institutions and investment firms – part of the CRD IV package).

This creditworthiness assessment is frequently subject to prescriptive requirements such as those imposed in EBA's "Guidelines on creditworthiness assessment" under MCD[33]. In such situations, a bank's ability to innovate is reduced, since alternative uses of data or creditworthiness assessments are constrained by those prescriptive requirements.

Furthermore, there exist supervisory requirements in this area, including the European Banking Authority Regulatory Technical Standards On Assessment Methodology for IRB Approach[34]. These technical standards aim at ensuring consistency in models outputs and comparability of risk-weighted exposures.

According to that regulation, criteria for scoring must be provided for and hence deep learning or unsupervised learning is difficult to be used for this purpose.

However, AI-based risk models require more changes than previous models due to a faster validation feedback loop. Today's approval processes on the supervisory side often take too long and hinder shorter model cycles. In order to make use of the significant advantages of AI-based models, such as dynamic adaptation to environmental changes, it is necessary to process model change applications much more quickly. For this reason, the processes and procedures in supervision must be further developed and, if necessary, AI competencies expanded.

[32] *E.g.,* Regulation 285/2013 of Bank of Italy

[33] https://eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-creditworthiness-assessment

[34] https://eba.europa.eu/regulation-and-policy/credit-risk/regulatory-technical-standards-on-assessment-methodology-for-irb-approach

AI for security purposes: fraud prevention:

Purpose:

Banks traditionally distinguish between two main categories of fraud: external and internal fraud. The former encompasses attacks on the bank or its clients from outside its infrastructure. The latter involves fraudsters, typically employees, committing malevolent actions such as leaking private information or illegal funds' transfers.

External frauds relate to a wide variety of areas within financial institutions: non-cash payment over internet, money transfer, documents (identity fraud), bank cheque, etc.

A Fraud Detection System (FDS) is built to cope with such a threat. The pipeline follows these steps: collecting financial data, such as transactional data, analyzing them and learning from them or through the interaction with FDS maintainers (people implementing the detection rules).

The ambition is to become able to differentiate between normal actions and fraud attempts, which is called a binary decision problem in the Machine Learning jargon. AI algorithms are typically trained from databases that contain events' characteristics and their statuses (fraudulent or harmless). Their objective is to learn the association between characteristics and statuses, provided one exists.

In the following, the focus will be on the Data Driven Model of the FDS.

What is the technology?

Feature engineering: It is the foundation of any AI system. Feature engineering (and more generally data management) is crucial in helping the algorithm to be efficient but also interpretable. The construction of these features relies on discussions with operational people, common sense and a hint of intuition. Basic ones in the context of credit card fraud are, for instance, the total amount of money spent in the last hours.

Supervised and unsupervised learning: These are the two main categories of AI algorithms, translating features into decisions. Both tasks aim at spotting fraudulent behavior. The difference lies in the fact that in supervised learning we have prior knowledge of the ground truth (status of an operation) whereas in unsupervised learning the algorithm tries to infer the structure behind all behaviors to identify fraudulent ones (without having access to this prior knowledge).

The general rule in our use case is to use supervised learning when possible. The figure below illustrates why: outliers might not always be frauds, mostly because fraudsters goal is to mimic as accurately as possible the habits of a normal customer.

Adaptive learning: Adaptive learning allows taking advantage of data streams (by contrast with static datasets). Updates are done on the fly as soon as new data arrives which makes it able to adapt to paradigm shift. Thus, this class of algorithms seems to be the most appropriate tool to work on fraud detection considering its dynamic nature and the way data is collected continuously.

One would like to use this method exclusively in a supervised manner, as it would be optimal. However, the bottleneck of supervised adaptive learning is the delay between an operation and the disclosure of its status (fraud or normal behavior). To say it differently, one cannot adapt to a concept shift that is not understood yet. In order to overcome this issue, a semi-supervised adaptive method appears as an appropriate solution. It operates on yet unlabeled data guessing their status while waiting for the ground truth to be

revealed. On top of this unsupervised operation, a traditional supervised adaptive learning is performed. Hence the name semi-supervised.

Processes:

For each new financial operation, the AI system receives all the characteristics of this event. Based on these, it outputs a score (*e.g.,* probability) aiming at quantifying the abnormality. Such a result, on the basis of the preset threshold, identifies suspicious events and directly discriminates fraudulent from genuine events making it a convenient tool as part of a larger FDS.

This output also offers the possibility of sorting transactions from the most suspects to the least ones. By focusing on the most risky ones according to the algorithm, investigators could allocate their time optimally. Indeed, algorithms and FDSs' maintainers profit more from the disclosure of a fraud than of a genuine transaction in terms of information gain, given that the number of frauds is generally negligible.

Despite seeming currently somewhat remote from operational staff everyday concerns, processing and quickly investigating algorithms' output is the core of the issue at hand. It produces a virtuous circle: better investigations lead to better algorithms. The difficulty is in making sure that the data is updated regularly enough to reflect current fraud trends. On the opposite side of the spectrum, keep using outdated and non-extensive data generally induces a performance decline overtime. It is, understandably so, due to an endless action-reaction cycle between fraudsters and the bank: as banks find out and counter fraud patterns, fraudsters come up with new strategies and so on. Overall, it makes fraud detection a dynamic issue that is not trivial to solve.

Maturity and (possible) evolution:

Cost sensitive optimization: The huge imbalance between normal and fraudulent transactions means a bank has to be extra careful when estimating the performances of an anti-fraud system. A clever and traditional way of monitoring it is to measure two parameters:

1. Precision: proportion of actual frauds among suspended or blocked transactions.
2. Recall: proportion of frauds suspended or blocked.

Higher recall results in more avoided frauds but most of the time it comes with low precision meaning customer inconvenience is all but mitigated, since many more transactions will be suspended or blocked. AI algorithms are trying to balance both indicators.

Nonetheless, what is usually not considered is the cost associated with each event. Indeed, while the cost of a fraud is easily quantifiable, the damage resulting from wrongly blocking an operation is not. The functioning cost of an investigation team is neither accounted. Cost-sensitive learning initiates a new way of dealing with fraud bearing in mind the whole picture.

Reinforcement learning: Recently gaining in momentum, reinforcement learning paves the way for a new way of dealing with fraud. Instead of waiting for the fraudsters to make the first move, reinforcement learning aims at modelling the fraudsters' behavior and continuously trying to break the system. As a direct consequence, it helps the bank exposing flaws before they are used against it.

More global protection: Sometimes fraud detection looks ineffective, the reason plainly being that the needed information is not available or that the attack happened upstream.

For instance, fraud is often linked to cyber-attacks, which are difficult to cope with. Indeed, IT infrastructures (especially those of big companies) are of great complexity and thus it is problematic to transcribe logs into structured labelled data that is analyzable by supervised algorithms.

In addition, collaboration is a crucial way to improve global performances against fraud. Such kind of information sharing is essential for better tracking as identifying links between people across banks opens up new horizons. More precisely, links represent information about people you know and interact with on the banking side.

Among many ideas, building-up network-based AI models is, without a doubt, going to reshape the way banks are dealing with fraud by increasing the derived insights from real-world data.

Benefits:

The cost of frauds associated to non-cash means of payment can be quite high: in the Single European Payment Area (SEPA), it is estimated that non-cash payment fraud caused 1.44 billion euros loss in 2013[35].

Moreover, the risk associated to fraud is almost certainly not going to decrease. As the digital space is growing at a rapid pace, fraudsters may take advantage of new systems vulnerabilities and people unawareness. Put this all together and it is a recipe for scaling-up fraudulent activities. Frauds, and especially cyber-attacks, are a growing concern for not only banks, but also all other industry. As a matter of facts, hackers (black hats) are offering hacking kits for relatively small amounts of money on the "Dark Web".

Having a more secure system means increasing trust in the bank for both clients and financers. Risk of fraud has, like all other risks, an influence over the interest rates with which banks refinance themselves and thus have an impact on their profitability. This potential distrust could slow in some extent the economic activity or undermine investments.

Regulatory framework and analysis:

From a legal standpoint, banks must refund customers that have been victim of fraud. Banks completely incur the loss of money due to a fraud. It is still the case even if, for example, a client of the bank does not recognize a phishing[36] attempt and inadvertently provides his ID to the pirate, leading to a successful fraud.

Additionally, if a regular payment is carried out with a non-cash mean of payment and the client states that it is a fraud, it is the bank duty to prove that it was actually not the case. In other words, "the burden of the proof" that a fraud was in fact a regular payment lies on bank's side.

Opportunities are clear: tackling the issue of fraud could save a lot of money for financial institutions in the future.

The identified challenges are:

- Making use of more data and appropriate algorithms to block more frauds;
- Having an always more efficient and faster feedback return about statuses/targets;

[35] Source : https://www.consilium.europa.eu/en/press/press-releases/2018/03/09/fighting-fraud-with-noncash-means-of-payment-council-agrees-its-position/

[36] Phishing: circumstances during which a fraudulent mail is sent to a victim, usurping the identity of a company or a person, in order to retrieve private information, for example its login and password.

- Applying more interpretable algorithms so that experts trust and use them.

From banks' point of view, there exists a tradeoff between the security level and the customer's experience ease. In other words, the implementation of too much security measures can impair the customer's experience with services offered by the bank. It is also important to stress that AI cannot solve every issue: improving the set of tools, the platforms, data management and decision-making is necessary.

Furthermore, fraudsters often target the weakest point in the financial network system which can negatively affect one or more participants, or the system as such. Therefore, one could think of European banks taking action together against fraud. Building a collaborative European approach to stand strong against fraud sounds like a relevant and strategic long-term solution. This approach could be useful to fight financial crime more generally, including hot topics such as terrorist financing or money laundering.

For more information:
Hélène Benoist
Policy Adviser - Data Protection & AI
h.benoist@ebf.eu
+32 2 508 37 11

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu