BLECKWEN

Artificial Intelligence in the financial sector: 13 key challenges of the future

Bleckwen, 6 rue Dewoitine 78140 Velizy FRANCE

www.bleckwen.ai | contact@bleckwen.ai |

Introduction

This white paper presents Bleckwen’s contribution to the request for proposals initiated by the ACPR (French Prudential Supervision and Resolution Authority). This institution, under the auspices of the French central bank (Banque de France), is responsible for approving and monitoring the activities of banks, insurance companies and their brokers, defending the interests of their customers and preserving the stability of the financial system. In February 2019, the ACPR closed a vast debate on the stakes related to artificial intelligence in the financial sector.

Bleckwen, a French Fintech company founded in 2016, develops fraud and financial crime prevention software solutions for financial institutions. The models developed by Bleckwen enable real-time detection of both social engineering-type fraud attempts (CEO impersonation, fake supplier fraud, etc.) as well as unauthorised type fraud (account takeover, internal fraud etc) across many payment types and is currently being used by a number of major French banks in preventing financial crime.

The content of this document was drafted by Yannick Martel, Chief Strategist, and Leonardo Noleto, Senior Data Scientist.

« A graduate of the Ecole Normale Supérieure and Telecom ParisTech, I worked in IT and data science for over 20 years. Having held a variety of positions within major companies - software editors and consultancy firms -, I have acquired an overall vision of how to resolve strategic problems using innovative technology. I'm convinced that the integration of data science and Machine Learning into software programs is a key source of innovation for businesses. I've been developing the Bleckwen solution since 2016, applying data science and Machine Learning to the fight against financial crime, with the aim of making the world a safer place. »

@yannick_martel in/ymartel

« I'm a Senior Data Scientist with Bleckwen, specialising in fraud analytics. Before joining Bleckwen, I worked in the field of anomaly detection and set up a tailored fraud detection system for one of the leading European cloud suppliers. I'm convinced that the use of Machine Learning methods, combined with the professional expertise of analysts, is a game-changer when it comes to combating fraud. I have an Computing Science degree specialising in artificial intelligence. I help our customers improve their understanding of the stakes related to artificial intelligence applied to the fight against financial crime. »

@leonardo_noleto in/noleto

Contents

No artificial intelligence without data

Many financial organisations produce programs to set up data lakes or data warehouses, which make data available for all functions. A few years ago, these programs were driven by analysis and reporting needs. Artificial intelligence has brought a new dimension: collecting and grouping all the data available is crucial to ensuring the generation of high-quality AI algorithms.

This is a non-negotiable development for any bank seeking to defend its position in the 21st century. The major drivers of change in the business world- whether it be physical or online trade- are those firms that have grasped the need to set up chains for collecting and using data, for enhanced decision-making and to provide a better service. The same scenario is set to play out in the financial sector, and the emerging players- online banks and other alternative stakeholders- are well aware of this.

The cloud is no longer optional

The IT infrastructure of traditional banks currently constitutes a major obstacle to the availability of data and its use in AI algorithms. The shift to AI requires responsive infrastructure that can be set up and dismantled quickly.

The data centre technologies used by financial organisations (virtual machines, shared drives, etc.) do not perform well on fast data / big data-type technological tools, designed for large-scale standard systems. Financial organisations are therefore likely to have infrastructure that is both expensive and unsuited to AI requirements. By making the shift to a cloud-based infrastructure, the organisations in question could overcome these difficulties, avoiding major expense and the need to train production teams which are more accustomed to very different types of technology (mainframe or web applications).

Overcoming obstacles to the use of AI in finance

When it comes to fraud prevention and the fight against money laundering and terrorism financing, we maintain that the technology and methods are now mature, but two types of factors constitute obstacles to their implementation:

- Financial organisations operate in a sensitive sector, which carries considerable risks. Traditional techniques such as rule-based systems are preferred, because we already know how they work and have a solid stock of knowledge. The widespread adoption of AI in the sector should gradually make it easier to apply it to these sensitive organisations.

- Traceability and explainability are essential for defending AI to customers, regulators and the financial institution itself. And yet, traditional AI methods imposed a choice between predictive performance and the explainability of the result provided by the model. This is no longer the case: the model interpretability methods developed over the past 2 to 3 years provide the means of understanding the results of the model, however complex it is.

These same obstacles exist in other sensitive fields, in the financial sector as well as health care and cybersecurity, and can be overcome in the same way: through gradual adoption of the method and the use of model interpretability methods.

In parallel, increasingly complex threats and equally complex techniques for circumventing the regulations require a degree of sophistication and an upgrade frequency that traditional approaches are unable to meet. Only AI combined with human expertise can enable financial institutions to regain the upper hand. The financial sector must realise that security can only be achieved through innovation and experimentation. Given the threats generated by increasingly sophisticated, automated financial crime, institutions are obliged to respond accordingly- with an equal degree of sophistication and AI.

> *The increasingly complex threats and equally complex techniques for circumventing the regulations require a degree of sophistication and an upgrade frequency that traditional approaches are unable to meet. Only AI combined with human expertise can enable financial institutions to regain the upper hand.*

4 Adopting a scientific approach to limit bias

There is a high risk of bias, given that AI algorithms learn mainly from the data submitted to them. The data in question must therefore be properly understood and managed in order to limit the risks.

When it comes to combating financial crime, the bias factor generates significant risks. Bias can make the models less effective and more vulnerable, as a result of the limits imposed by the limits of the data itself. It may also discriminate against certain segments of the population, by introducing additional frictions on specific criteria (such as geographic criteria).

Modelling techniques provide an initial means of managing bias. It is possible to combine supervised models, which are more effective but more sensitive to the quality of the target data, with unsupervised models, which are less effective but offer the possibility of incorporating previously unexpressed or undetected threats. The new deep learning algorithms used by Generative Adversarial Networks and Reinforcement Learning may also provide a solution that makes better use of the data available by improving our understanding of said data and, consequently, our ability to detect bias.

The technical approach must be backed up by ethical and managerial considerations: any bias has the potential to disrupt the smooth flow of customer transactions. This disruption may be acceptable if it is limited, but cannot be defended if it becomes systematic (if certain categories of population are always affected, for example). Management will therefore need to accept that certain types of data cannot reasonably be used to their full potential, and that optimal performance will need to be sacrificed in the name of fairness.

Finally, these elements need to be completed by providing appropriate training to data scientists. The latter need to be trained in how to adopt a truly scientific approach by assessing the results and the limits of their system at every stage. As a result, they will be in a position to judge the actual performance of a model, which may not pass a test in operational conditions. This is one of the risks inherent to modern approaches to Machine Learning and data science, which are highly computerised and more empirical than the traditional statistical approach. The ability to assess performance and bias effectively will therefore be a key component of the training provided to data scientists.

In addition to the technical and scientific approach, data scientists will also be made specifically aware of the notion of bias and the impacts of their work on users, businesses and society as a whole. This will give them the means of analysing the results obtained and their consequences, which they can then explain to their managers.

5 Fighting on equal terms

Digitisation has exacerbated the vulnerability of our societies: increased dependence on third-party infrastructure, evermore sophisticated attacks and a rise in the proportion of cybercriminals using sophisticated tools and approaches.

These risks are real, and will become even more threatening if financial stakeholders do not fight back using the same weapons. The image here is that of an arms race between criminals- some of whom may have the support of government regimes and significant resources at their disposal- and financial institutions. The latter need to acquire the skills and tools that will enable them to fight on equal terms. At the same time, they must update their methods and infrastructure while managing the associated risks. Hiding behind well-established methods and approaches simply increases the risk of being taken by surprise when the threat unfurls- but this is not limited to AI and is part of the digital revolution.

More specifically, AI offers a very high degree of protection. In military strategy, the best defence is a good offence: the attacker chooses where to strike and is in a stronger position to focus its efforts where they are needed. This adage is equally relevant in the digital era, given that a defensive stance is based mainly on a mere handful of resources: the skills of cybersecurity experts. AI offers a way of channelling a large part of those skills into automatic systems, thereby helping to maintain them. In other words, the expert, when combined with the tool, becomes even more effective.

> *It is an arms race between criminals - some of whom may have the support of government regimes and significant resources at their disposal - and financial institutions.*

Unity makes strength

Through our regular discussions with the authorities in charge of combating financial crime, we have observed considerable obstacles to the sharing and use of data, both within companies and among companies. One of the consequences of the data protection regulation and privacy rules has been to hinder all data-sharing initiatives that are not explicitly approved or required by the regulator. Data sharing does occur, but it is currently informal and occasional.

On the other side of the battlefield, criminals are organised and share their information. They have no qualms about crossing borders between departments, companies and countries. By discouraging data sharing within financial institutions, we create an unequal situation in the fight against fraud, and the consequences affect all citizens and organisations. While imposing a framework and limitations, sharing of data should nonetheless be encouraged in order to improve the way we wage war on financial crime.

In this area, financial institutions should not see themselves as competitors but rather as stakeholders in the collective war against a common enemy. As an example of the collective approach in practice, we could point to French mobile network operators. Although they operate in a highly competitive sector, these operators have joined forces to create the Preventel Economic Interest Group. The latter offers a platform for sharing the identity of natural persons and legal entities which present a default risk. As a result, operators are better protected from the risk of non-payment, as well as fraud. This system is well supervised and a specific protocol is in place to control access to Preventel.

The financial sector regulator might therefore promote the development of such anti-fraud initiatives by welcoming them enthusiastically. The ACPR report on AI will undoubtedly help move the process forward.

> *By discouraging data sharing within financial institutions, we create an unequal situation in the fight against fraud, and the consequences affect all citizens and organisations. While imposing a framework and limitations, sharing of data should nonetheless be encouraged in order to improve the way we wage war on financial crime.*

> *Intelligibility is required so that the analyst can relate to the professional knowledge modelled and know how to interpret it.*

Explainability: understanding and taking action

Explainability is undoubtedly a major lever in accelerating the take-up of AI in the field of finance. We prefer the definition inspired by the social sciences and coined by Tim Miller[1]: “Interpretability (of Machine Learning algorithms) is the degree to which a human can understand the cause of a decision.” Although it is fairly broad, this definition seems to us to be the most appropriate, given the various forms of interpretability offered by Machine Learning algorithms (deep learning, graph analytics, machine learning, decision trees, etc.). It should also be noted that we use the terms “interpretability” and “explainability” interchangeably.

Regarding the methods already available, we use SHAP[2] (SHapley Additive exPlanations), which offers the possibility of extracting explanations from any predictive model (including black boxes).

When we try out these methods within financial organisations, we observe that explainability alone is not sufficient to enable effective collaboration and a relationship of trust between algorithms and human agents. Going further, at the modelling stage, the variables must be both intelligible and actionable. Intelligibility is required so that the analyst can relate to the professional knowledge modelled and know how to interpret it correctly. Actionability is a way of guiding the operator’s actions when responding to an alert or conducting a more detailed investigation into the reasons behind a score. An example of an unactionable variable in the framework of fraud risk modelling might be: “The customer is aged between 20 and 25”. Whereas an actionable variable would be: “The substantiating document provided by the customer is twice as risky as the average of other substantiating documents”. The variable in the second example helps the analyst focus his or her attention on a given aspect of the case under consideration (be vigilant regarding this type of substantiating document), unlike the first example, which is very broad (the analyst cannot change the customer’s age, even if it is a high-risk group).

[1] Miller, Tim. 2017. “Explanation in Artificial Intelligence: Insights from the Social Sciences.”

[2] http://papers.nips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions.pdf

8 Making AI reliable

The reliability of algorithms is without doubt a key factor when it comes to adopting AI, for ethical and security reasons and in terms of company effectiveness and good management. The level of reliability depends on the reliability of the data and the degree of control over the system as a whole and the algorithm process.

Regarding the latter, data science can draw inspiration from software development and test first approaches (such as Test Driven Development), which advocate constructing the approach and its test campaign before starting to develop the required algorithm. This type of approach places assessment and verification at the core and results in robust, reliable systems that withstand the test of time.

As in software engineering, these methods also require a new managerial approach: there is no silver bullet and, as any gourmet chef knows, producing great results takes time. The desire to pursue a quick win without simplifying or lowering the performance objective inevitably leads to a less robust, less reliable system. Yet these elements cannot be measured without specific checks. As in software engineering, management and functional experts need to be aware of the stakes before embarking on the development process.

> *Data science can draw inspiration from software development and test first approaches (such as Test Driven Development), which advocate constructing the approach and its test campaign before starting to develop the required algorithm.*

9 Cooperating with machines

Interaction between humans and AI algorithms is a crucial issue in the fight against financial crime, because the final decision is often made by a human analyst.

Efforts to improve explainability are important because they pave the way for smoother integration between humans and algorithms, resulting in better cooperation. Our anti-fraud solutions incorporate the means of explaining the individual decisions made by the algorithms, so that they are understood by analysts and the administrators who handle the alerts. Being able to explain the reasoning and causes of a decision about a customer to the person concerned is also a regulatory obligation.

Explainability also runs the risk of adversely influencing the judgement of human analysts. For example, as part of a pilot scheme, we asked our customer whether it would be helpful to provide the score calculated by our algorithms. Having access to the score could help the fraud analyst carrying out the investigation, but it might also influence his or her decision.

We believe that the main way of protecting against risks is to be aware of the (numerous) positive aspects of Artificial Intelligence as well as its (equally numerous) limitations. The Bleckwen solution opts to display the main factors that have led to a given result. This provides analysts with access to the factors taken into consideration and those that the algorithm chose to ignore, or was not able to use. Suitable navigation and investigation tools must be provided to enable analysts to comprehend these factors and the statistical criteria more effectively. Since our AI algorithms are based on data and a statistical approach, a data-centric culture and a sound approach to statistical indicators must be promoted.

10

Using data science to verify AI

In the financial sector as in the rest of society, AI is poised to play an increasingly important, determining role. In this context, we are right to raise the question of checks and verification. Such safeguards are even more important in the fight against financial crime, where internal checks and conformity are crucial and imposed by the regulations. With its ability to process large quantities of disparate data and leverage human expertise, AI can contribute to the verification process.

Traditional verification methods must be backed up by a data analysis approach, using cutting-edge probabilistic and statistical techniques (or even Machine Learning). This is especially useful as a means of verifying human processes as well as other probabilistic, statistical or Machine Learning algorithms. The methods used to track fraudsters and understand their behaviour also help us comprehend and verify the algorithms used to fight them.

To achieve this, the people responsible for performing these checks also need to adopt the methods of data science, while accepting their principles and limitations: empirical methods for the most part, providing probabilistic results incorporating a degree of doubt, the causes of which are difficult to pin down. Here again, the crucial element is awareness and adopting a new data-centric culture.

The methods used to track fraudsters and understand their behaviour also help us comprehend and verify the algorithms used to fight them.

11

Keeping people in the loop

Certain first-level checks can be improved through algorithms, and this is at the heart of Bleckwen's offer. However, we need to be vigilant regarding the objective: the aim is to optimise the effectiveness and security obtained with respect to the time and resources invested, and not simply to make the switch to an automated system without considering the overall effectiveness.

The automotive industry has proven that, in the controlled yet uncertain environment of a manufacturing plant, the best performance in terms of investment is achieved by fostering collaboration between human operators and automated systems. 100% automation, which looks tempting on paper, is difficult and fragile in practice. We suggest applying the same approach- based on selective optimisation and smoother integration- in order to combine the best qualities of the human agent and those of the automatic system.

When faced with certain constraints (real time, high volume, limited resources, etc.), we will aim to fully automate the verification process, especially at level 1. The risk generated will be controlled by increasing the level of vigilance at level 2 and via the mechanism for assessing results and trends.

Keeping people in the loop also ensures a better overall performance compared with an automatic system. Human expertise also helps improve the way the system operates overall, by injecting knowledge and analyses that are outside the scope of automatic processing.

Keeping people in the loop also ensures a better overall performance compared with an automatic system. Human expertise also helps improve the way the system operates overall, by injecting knowledge and analyses that are outside the scope of automatic processing.

> *As a Fintech addressing Fraud, AML/CTF, we have seen a decrease in our customers' fraud loss by more than 60%, while reducing the rate of false positives by 20 fold (or in other words a 95% reduction in unnecessary alerts).*

12

Pooling technological resources

The use of Machine Learning methods in finance has already proven its usefulness, as a way of optimising existing processes as well as creating new sources of income. As a Fintech addressing Fraud, AML/CTF, we have seen a decrease in our customers' fraud loss by more than 60%, while reducing the rate of false positives by 20 fold (or in other words a 95% reduction in unnecessary alerts). While this scenario is already a reality for some banking organisations, others are lagging behind and failing to adopt Machine Learning techniques- for the reasons evoked above.

When it comes to the fight against financial crime, we believe that the regulator should encourage the pooling of technological resources. This is an area which carries certain risks - for example, a shift in criminality targeting organisations with lower investment capabilities and market share, which are more vulnerable than the "bigger" players. When the first banking organisations started to adopt AI, this sparked the advent of more complex, fragmented fraud techniques. This shift creates an even worse situation for those organisations that are still using traditional systems based solely on rule-based systems.

We therefore invite the regulator to take the necessary steps to develop common alerts and signals that will enable financial institutions to cooperate in the public interest.

This cooperation might take several forms:

- Authorising the sharing of negative files and elements under surveillance, in a way approved by the regulator
- Training the organisations involved in the new Federated Learning[3] methods, which aim to pool fraud patterns without exchanging any data. This recent method is highly promising because it guarantees full anonymity for each bank's data while offering the possibility of building up a stock of collective intelligence. This collective intelligence is set to grow as more financial institutions take part.

[3] https://blog.fastforwardlabs.com/2018/10/29/federated-learning-machine-learning-with-privacy-on-the-edge.html

13

Supporting the development of AI to make the world a safer place

To support the fight against financial crime, the regulator could decide to clearly come out in favour of AI technology and innovation research. Technological innovation is without doubt essential in order to tackle the growing threat facing financial institutions within an increasingly constrained environment.

In the U.S., several financial regulators have stated their support for trials involving AI applied to AML[4]. By adopting a similar stance in France (or, better, at European level), the regulators could help dispel uncertainty and encourage trials. It's time to act! France is home to several big banking groups, some with a global presence, that have access to large quantities of wide-ranging data, making them good candidates for the launch of innovative initiatives.

[4] https://www.finextra.com/newsarticle/33057/us-regulators-push-for-new-technology-to-tackle-financial-crime

BLECKWEN

DEEP TRUTH REVEALED

To conclude, few facts about us:

Our name

Bleckwen refers to the famous American neurologist William Jefferson Bleckwenn (1895 –1965), who invented the truth serum. At Bleckwen, we listen to your data to let the truth emerge.

Our logo

Everyone knows about the iceberg theory: the tip of the iceberg actually only represents 10% of its total mass. Bleckwen helps you explore the hidden part of your data to combat fraud and make your business secure.

Our vision

We believe that the world will be a safer place through collective intelligence, the result of close cooperation between people and machines.