slimmer AI

The use of AI

in AML transaction monitoring

Joost van Houten
Head of Sentinels at Slimmer AI

Table of contents

The use of AI in AML transaction monitoring

Overview

Clearly, the approach to money laundering detection and prevention needs to change – and technology, like artificial intelligence and machine learning may provide part of the solution.

Financial institutions are on the frontline in the battle to combat financial crimes, such as fraud, money laundering and terrorism financing. These criminal activities impose massive costs on the global economy both financially and socially.

To combat these crimes, regulatory authorities have adopted increasingly comprehensive and demanding regulations that put the onus on financial institutions to identify, process, and alert the authorities of suspicious transactions.

However, around the globe, banks are struggling to make meaningful inroads into the problem despite significantly increasing financial investment and expanding compliance teams year after year.

Clearly, the approach to money laundering detection and prevention needs to change – and technology, like artificial intelligence (AI) and machine learning (ML) may provide part of the solution.

However, before introducing AI on a widespread basis, stakeholders will need to buy into the step change needed to harness the benefits, while making sure the associated ethical, governance, and transparency considerations are taken into account.

The transition to a new AI-supported system that maximises the effectiveness of AML detection cannot happen without the support of regulators. Regulators need to create a regulatory environment which allows for more flexibility than the current prescriptive regulations that have inadvertently resulted in a tick-box approach to AML compliance requirements.

Regulators also need to grapple with privacy issues that may stand in the way of financial services sharing relevant information that would maximise the ability of AI to detect sophisticated criminal behaviour and adapt to changes in that behaviour.

Incorporating AI in transaction monitoring and reporting in a considered and deliberate way could turn what has been a losing battle up until now into a far more effective strategy to combat financial crime.

The problem

Unbalanced fight

Financial institutions invest huge amounts in security and wider compliance systems, while also filing millions of reports to authorities.

European financial institutions are spending about €100 billion on compliance annually, according to the European Banking Federation (EBF), and 10% of banks' staff are dedicated to compliance tasks. Yet their efforts are not paying off. The EBF estimates that barely 1% of the cases are prosecuted and barely 1% of criminal proceeds in the EU are confiscated by the authorities, with the value of money laundered estimated by the World Bank to be upwards of $2 trillion per year.

EBF CEO Wim Mijs summarises the problem the banking and payments industry is facing: "European banks invest huge amounts in security and wider compliance systems, while also filing millions of reports to authorities. The actual results which come from preventing money laundering can prove disappointing unless supplemented with better-targeted efforts to identify and tackle the underlying threats."

The cost of combatting financial crime is likely to continue growing, possibly at the double-digit rates experienced by financial institutions over the past few years. Regulatory authorities, particularly in the EU, continue expanding regulations in an attempt to close the loopholes and in the hopes of making better inroads into the vast sums being laundered.

The biggest problem up until now is that introducing new regulations has done little to address the issue. Instead, it has had unintended consequences. The EBF sums these up[1]: "Over time, the prescription elements of the AML and CFT regime have created a division between the management of financial crime risk and the management of financial crime compliance risk, with the latter overwhelming the former." Given the demanding regulatory requirements and the threat of being fined, financial institutions are devoting significant resources to managing the compliance risk rather than ensuring they have the most effective capacity and resources to ensure what they are doing achieves better results.

1 Lifting the spell of dirty money – EBF blueprint for an effective EU framework to fight money laundering

The problem

Detection

Detection of AML transactions is tough because criminals are smart, sophisticated, and highly motivated to reintegrate the proceeds of their crimes into the normal economy. They continuously adapt their behaviour to take advantage of loopholes and new ways of avoiding detection, which, given the current labour-intensive approach to compliance, makes it difficult, if not impossible, to keep up with their activities and their new, sophisticated ways of doing things.

In its publication, *The case for artificial intelligence and terrorist funding*, Deloitte[2] spells out the challenge financial institutions are facing: "These criminal minds are also capable of using new technologies such as online banking, electronic payments, and cryptocurrencies to move illicit funds across borders at breakneck speed. These sophisticated measures to avoid being caught create complex and layered transactions that are increasingly real-time, making it difficult to monitor and to detect with traditional approaches."

In addition to the enormous challenges in keeping up with the volumes of potentially suspicious transactions, data protection laws, like the GDPR, up until now has prevented information sharing between financial institutions.. As a result, the banks and other financial services players only have access to their client information and thus make decisions based on a single institutional view of the world.

Sharing information under strict conditions would significantly enhance the ability of financial institutions to combine forces in detecting criminal behaviour that is multi-faceted and multi-national. Oftentimes, this behaviour is almost invisble, making it extremely difficult to identify, measure, and combat.

2 *The case for artificial intelligence and terrorist financing - A deep dive into the application of machine learning technology - Deloitte*

The problem

Tools

At the heart of the problem, however, is that financial institutions don't have the tools necessary to do a better job at detecting high-risk transactions that need to go to the head of the queue for further investigation by authorities.

The industry-standard way of flagging suspicious transactions is by developing business rules on prescriptive regulatory requirements. These are crude if-else statements that don't adjust to continually adapting criminal behaviour.

> *Regrettably, this fight has proved unbalanced, with criminals adapting faster than regulations.*

The business rules assess the risks the institution could be exposed to if the transaction is a suspicious one instead of focusing on what the information tells us about what the criminals are doing.

As a result, there is a high volume of false-positive assessments of transactions. Also, suspicious reporting that is of no immediate value to financial intelligence units is estimated to be as high as 99%.

With only some 1% of transactions flagged by financial institutions around the globe on average found to be useful to authorities, the financial sector's compliance efforts are as effective as throwing out a dragnet to catch a rare fish, which could be in an entirely different ocean. The EBF sums up the situation: "Regrettably, this fight has proved unbalanced, with criminals adapting faster than regulations."

The problem

Workload

Compliance departments are processing large volumes of transactions to little effect, as evidenced by the high false-positive rates and low rate of conviction based on the suspicious activity reports sent through to the authorities. Thus, compliance officers' jobs effectively consist of checking and rechecking alerts, with almost all proving to be irrelevant.

As the illustration below shows, McKinsey estimates that over 90% of AML alerts are false positives, largely as a result of data inconsistency and diversity of sources and that data consolidation could have prevented half of these.

Major culprit of false positives: internal data issues

90%

Over 90% of AML alerts are false positives

McKinsey 2018

63%

63% of FIs cite data inconsistency and diversity of sources as their main challenge

KU leuven - Belgium university of Southampton - UK

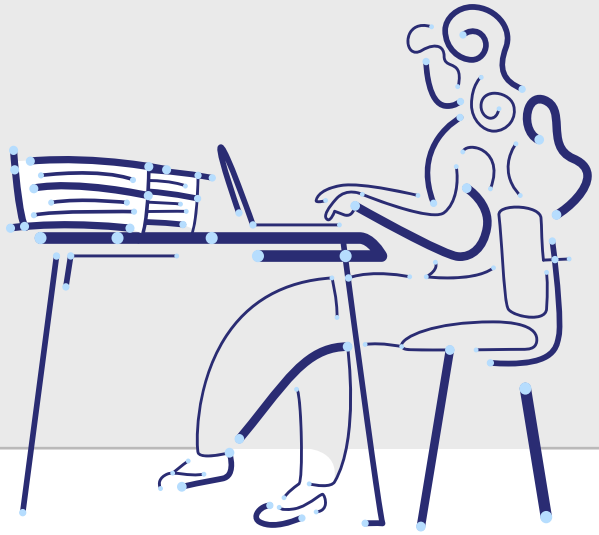
50%

50% of alerts could have been prevented through consolidation of data across sources

McKinsey 2018

The problem

Workload



European banks are filing millions of reports to authorities and, given the rules-based approach, the massive flow of information to the competent authorities, is “typically unguided by feedback and limited by the individual banks’ limited intelligence picture.”

Deloitte points out that the high volume of backlog alerts swamp compliance teams and potentially distract them from ‘true’ high-risk events and customer circumstances.

European financial institutions have an even more challenging time given the higher regulatory burden on them, including GDPR, high profile sanctions violations, and increased compliance regulations. The size of the workload, which has been growing year after year, is unlikely to reduce anytime soon.

That will put even more pressure on already overloaded financial authorities. The EBF says European banks are filing millions of reports to authorities and that, given the rules-based approach, the massive flow of information to the competent authorities, is “typically unguided by feedback and limited by the individual banks’ limited intelligence picture.”

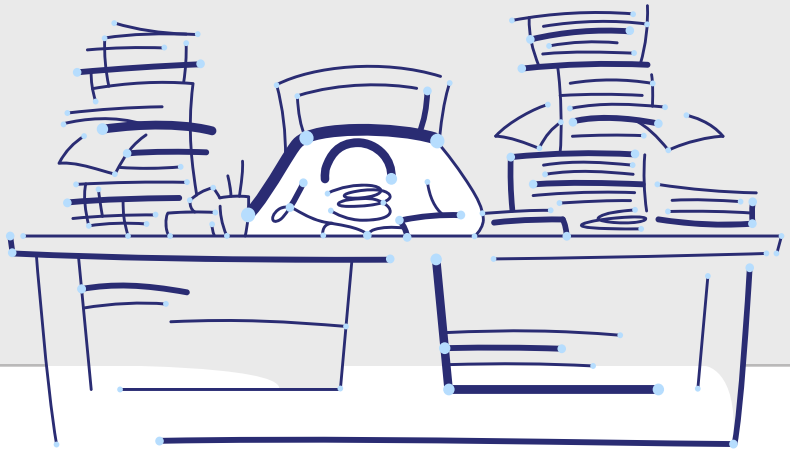
The Financial Intelligence Units (FIUs) receive far more Suspicious Activity Reports than they can handle because, out of fear of being found to be non-compliant, financial institutions tend to report more than necessary. The FIUs, which are responsible for following up the reports with additional analysis and investigation, are struggling to get through the caseloads. As a result, regulations tend to be tweaked each year, as regulators try to find a better, more durable solution to the problem.

The EBF concluded that the current approach doesn’t support the efficient allocation of specialist bank compliance resources “or more innovative approaches to tackling complex threats such as human trafficking and trade-based money laundering.”

The unsatisfactory results of overstretched compliance departments and FIUs are a far cry from the what is needed to reduce money laundering and terrorism funding activities – and has potentially significant consequences for financial stability and the safeguarding of citizens.

The problem

Cost of compliance



It's not a shortage of funding that is the problem. The European financial sector spends about €100 billion on compliance annually and 10% of banks' staff are dedicated to compliance tasks.

Looking forward, even more money is going to be invested in compliance, with various surveys finding that at least half, and as many as two-thirds, of financial institutions expect to increase their compliance budgets in 2021.

The costs to financial institutions are not just financial but also include employee dissatisfaction, which eats into the productivity levels of skilled, and expensive, compliance staff members. The volume of work, together with the low levels of achievement, weigh heavily on compliance staff.

Compliance staff are overstretched, engaged in time-consuming and unsatisfying work and, worst of all, they are not achieving the desired results. Fines imposed on financial institutions were increasing and amounted to $8.14bn worldwide in 2019 alone.

While technology could play a valuable supportive role in alleviating the burden of work on compliance officers, financial institutions still spend the bulk of their compliance budget on human resources.

Unless the current status quo changes, financial institutions will find they are spending more and more money to hold their current, undesirable, position or, worse, move backwards and face the prospect of costly reputational damage.

The costs of not solving the problem of expensive and largely ineffective AML transactional reporting are considerable and wide ranging. Not only will failure to make inroads into preventing AML activities result in significant societal costs, as highlighted in the graphic below, but financial institutions will face the following:

- Double-digit growth in the compliance costs, without achieving the necessary results;
- The real possibility of being fined millions, if not billions, of dollars for falling foul of regulations
- Financially unquantifiable damage to their reputations as trusted stakeholders that have efficient and effective internal financial systems.

The problem

Money laundering what is at stake?

- Transforming the proceeds of crime into ostensibly legitimate assets;
- Much more than white-collar crime;
- Connection to organised crime gangs and extremely harmful threats.

Human trafficking

Illegal drugs crime

Corruption

Terrorism

Environmental crime

Counterfeiting and smuggling

Financial fraud

The solution

Incorporating AI and ML

Incorporating AI and, as a subset of it, machine learning into compliance processes shows great promise and is expected to become pervasive in years to come.

Former Google and Baidu world-renowned computer scientist Andrew Ng describes financial technology as the new electricity. He believes the financial sector is one of the best-suited industries for "an AI-led transformation" and says the only way the uptake of technology will slow down is if talent is scarce and companies struggle to harness their data effectively.

In its paper exploring general principles in the use of AI in the financial sector, De Nederlandsche Bank (Dutch central bank) said: "In the near future AI is expected to become more advanced and increasingly ubiquitous, driven by the continuous increase of computer power, data availability and the advance of the Internet of Things."

Many other participants in the private and public sector are also excited about the potential AI has to make inroads in the battle to combat financial crime.

In a letter to the European Commission on the recent consultation on a roadmap for changes to the Union's AML/CFT framework, Andrés Portilla, Managing Director, Regulatory Affairs Institute of International Finance, commented on the enhancements to the use and adoption of technology in fighting illicit finance. He said: "New technologies have dramatically bolstered financial institutions' AML efforts and also hold promise for effective deployment at FIUs. Further work and leadership at the EU level to foster new technologies and review regulatory impediments to innovation will greatly assist efforts to fight financial crime."

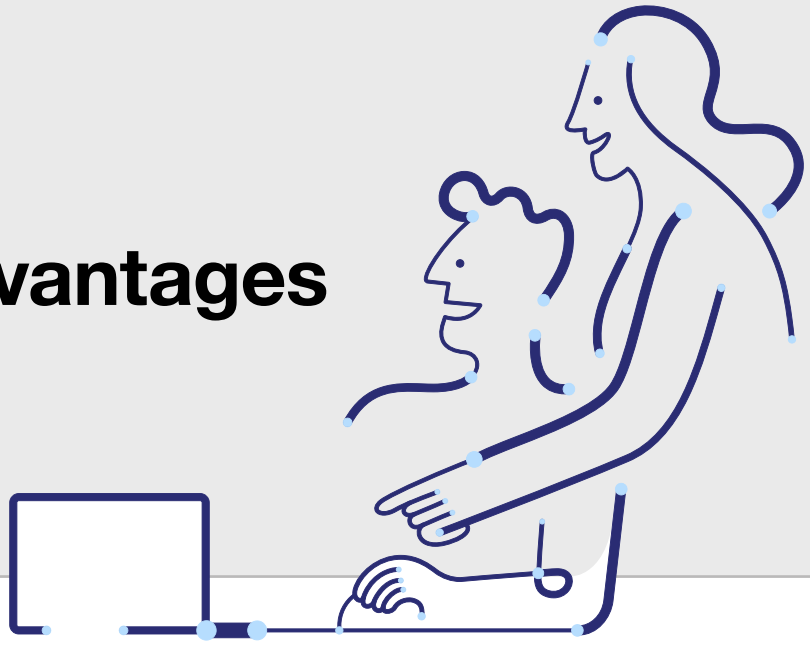
Deloitte also views innovation in compliance as needed to "both reduce the false positives and to bring about greater effectiveness in the manner in which AML and/or Counter Terrorist Financing risks are monitored and addressed by the banks."

Financial institutions and regulators are recognising that incorporating AI in compliance has the potential to address many of the challenges with the current AML compliance approach mentioned earlier in this paper. In essence, it improves the capability of compliance departments to detect suspicious transactions; it reduces the overwhelming manual workload skilled compliance officers are currently handling, and there are indications that it could reduce the cost of compliance.

Most importantly, incorporating technology into AML compliance could put authorities in a better position to spend most of their efforts investigating high-risk transactions rather than a mountain of low-risk suspicious alerts.

The solution

AI and ML advantages



AI and machine learning are particularly well suited to the task at hand because the technology can detect suspicious behaviour and activity more critically and effectively – and learn and adapt to changing criminal activities.

> *AI is expected to become more advanced and increasingly ubiquitous, driven by the continuous increase of computer power, data availability and the advance of the Internet of Things.*

Deloitte encapsulates the power of machine learning, saying that machine learning understands patterns in data or tasks without having pre-defined coding. Doing so, enables financial institutions to analyse large volumes of data and "learn" from the results. "ML algorithms can be taught to detect and recognise suspicious behaviour and risk rate them accordingly." It does so by identifying previously undetected transactional patterns, data anomalies and relationships amongst suspicious individuals and entities.

Thus, the most useful role machine learning plays in the process is that it focuses on the riskiest transactions, "knowing when to omit non-anomalous transactions that do not present any risks as dictated by customers' profile and behaviour."

This ability to prioritise potentially risky transactions materially reduces the proportion of false positives. It then enables the skilled compliance officers to pick up on these risky transactions and put worthwhile time and effort into investigating them further before sending through an unusual or Suspicious Activity Report (SAR) to the authorities. It thus makes the work for compliance more engaging and rewarding, while helping society by catching criminals that would otherwise have gone undetected.

The next page shows how a multi-layered approach to financial crime that incorporates AI could address the risks and compliance and result in a more effective solution.

The solution

A multi-layered approach

A multi-layered solution approach to financial crime compliance and identity proofing is essential as criminals become more sophisticated, thus requiring a sophisticated approach to fighting them.

Based on the variety of unique risks that emerge from individuals, transactions, related financial products, countries, and contact channels, it is important to assess both the individual and the business (if a business account) with a need for real-time behavioral data/analytics.

Risks

- Bogus business or misrepresentation of business ownership with intent to commit financial crime
- Fake, synthetic identities developed from breached data
- Mobile and online channel transactions, and digital onboarding that provide anonymity for synthetic identities
- Non-bank payment providers/ systems that transaction and customer transparency difficult, and pose risk of being non-compliant themselves
- Cryptocurrencies that enable criminals to move illicit funds, especially across borders

Financial crime compliance challenges

- Customer risk profiling
- Sanctions screening
- Efficient alerts resolution
- Complex payment chains
- Positive ID of PEPs

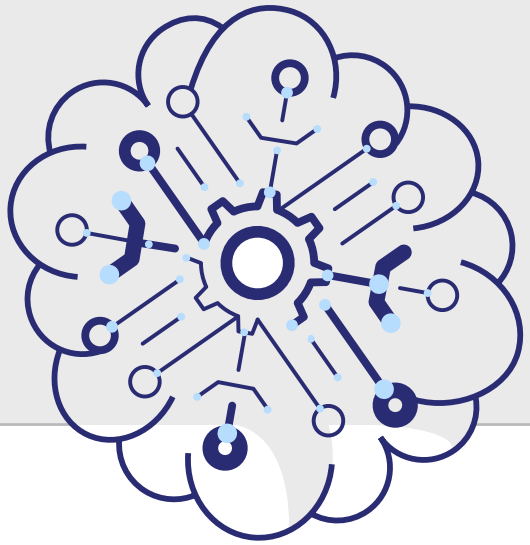
Effective solution

A multi-layered approach to financial crime compliance and identity proofing should:

- Investigate both the physical (name, address, documents) and digital identity attributes (the digital footprint, devices, and behavior of the entity)
- Assess both the individual (Is this the right person?) and the transaction (Are there anomalities with the transaction?)
- Incorporate both KYC (individual) and KYB (business) processes
- Leverage data analytics to assess risks and behavior in real-time

The solution

Components of an AI solution



How would an AI solution actually work? The specifics of incorporating the AI components in the compliance process would include the following:

- A data source collector/entity profile that is dynamically updated with a large variety of internal and external data sources. These could consist of know your client (KYC) onboarding data, transaction behaviour, third-party databases, sanctions lists, web content screening and scraping and alert handling feedback.

- An alert handling interface which provides an alert overview that explains why each alert was generated in a simple, easy to visualise format. When applicable, other information would be presented, like Google maps, Chamber of Commerce information and sanctions checklists. The user-friendly interface would then make it clear to the compliance team on the next step they need to take.

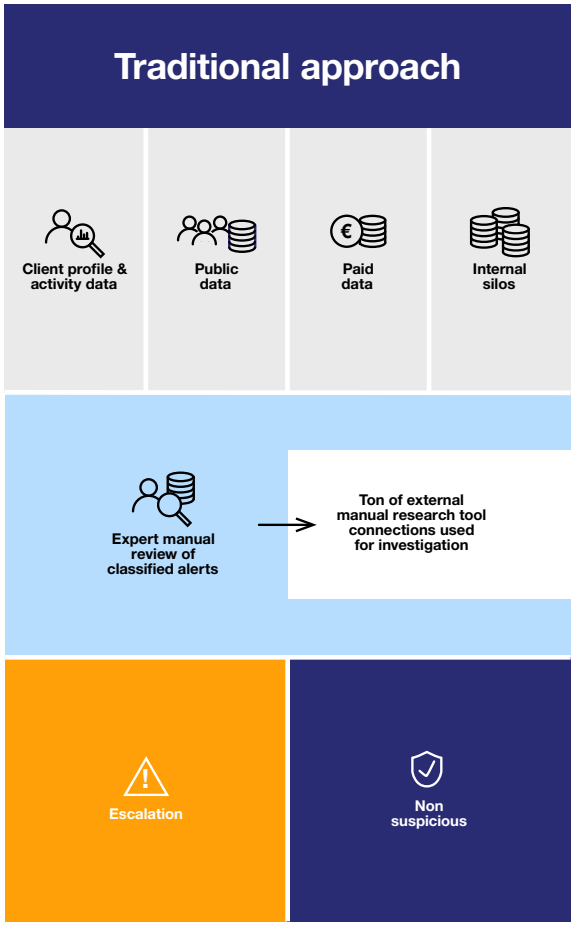
- A risk engine and alert generator that runs on a combination of objective rules and explainable AI that reduces the false positive alerts. The machine learning would be trained for different risk scenarios and harder to catch criminal typologies. Predictions would be based on changes in behaviour versus expected behaviour by assessing transaction behaviour versus peers, countries paid from versus meta-data and website content versus onboarding data.

This unsupervised anomaly detection would give the system the ability to detect previously unseen money laundering patterns. By detecting deviations from the normal state, the machine learning model would not need to rely on already observed behaviour. That allows for easily configuring and editing and tunes the rules and the model to reduce the proportion of false-positive rates dramatically.

The solution

Components of an AI solution

Introducing these AI/ML components to the compliance process would create a less labour-intensive, far more efficient and streamlined process, while vastly expanding the amount of data that could be interpreted from a myriad of external sources. The infographics below show the difference between the way the compliance approach currently works and a new more efficient and effective AI-enabled approach.



The solution

Implementation process

There are many factors to take into consideration when implementing an AI solution into the compliance process. These include choosing the right technology partner, ensuring they manage the internal data sufficiently well to enable the ML to deliver the results required and overseeing the smooth technical implementation of the technology. The graphic below highlights all the considerations a financial institution needs to take into account - and the questions they need to ask - before they go ahead.

READINESS FOR AN ML PILOT

Broadening the benefits

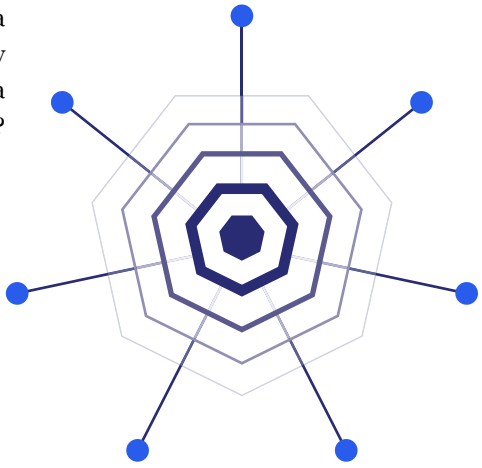
What are the benefits of the applications beyond compliance operations?

Data

Is there sufficient data quality that is easily accessible to create a meaningful model?

Business problem

What is the problem being solved?
Is the problem statement clear?
Have the internal stakeholders been informed?



Leadership

Does your organisation trust ML?
Is there buy-in from your organisation with an allocated budget?

People

Are there people internally who understand the value of ML?
Can they work with the vendor on that project to validate outcomes?
Are there people to take over after the POC?

Hardware

Is there somewhere to host the ML application that is secure and powerful enough?

Process

Is there a process in place to select and on-board a new vendor?

The solution

Implementation process

Deloitte outlines six steps to success in incorporating machine learning in the compliance process:

- Validating the existing technology that is in place and identifying where it can be enhanced
- Putting together a strategy and structure to guide the deployment of the AI and ML operationally and ensuring there is an in-depth understanding of the models and algorithms
- Understanding the key
- Determining the appropriate operational structure for monitoring and validating the outcomes and ensuring it meets regulatory objectives and appropriately addresses the risks
- Devising an effective governance framework to address data quality, project management, stakeholder expectations
- Putting in place robust due diligence of the vendors selected to provide the technology, know-how and infrastructure

Incorporating AI into compliance processes inevitably raises various risks that need to be addressed responsibly by a financial institution. De Nederlandsche Bank[3] addresses some of these and suggests measures to address them in its General principles for the use of Artificial Intelligence in the financial sector.

3 *General principles for the use of Artificial Intelligence in the financial sector – De Nederlansche Bank*

The solution

Implementation process

The DNB identifies six fundamental principles, with the acronym SAFEST, to guide financial institutions through the responsible application of AI in compliance processes. These are soundness, accountability, fairness ethics, skills and transparency.

Soundness – AI should be reliable and accurate, behave predictably and within the boundaries of applicable rules and regulations. The Bank sees this as its primary concern.

Accountability – Firms are required to take responsibility for their use of AI, particularly if it doesn't function as intended and results in damages for the firm, its customers and other stakeholders.

Fairness – Financial firms need to ensure that AI applications do not inadvertently disadvantage any groups of customers.

Ethics – Customers and other stakeholders should not be mistreated or harmed – directly or indirectly – as a result of the firm's deployment of AI. DNB notes that this moral obligation goes above and beyond complying with applicable legal requirements.

Skills – All staff, from the work floor to the board room, need to be sufficiently qualified and have a sufficient understanding of the strengths and limitations of an AI-enabled compliance system.

Transparency – Financial firms must be in a position to explain how the AI applications function and sufficiently justify any material decisions made.

Regulatory authorities will need to play their part in extracting the maximum potential offered by AI in compliance. More flexible, risk-based rather than prescribed rule-based regulations will give a new technology-enabled compliance approach the best chance to deliver more effective and useful results than have been achieved in the past. Also, given that financial crime is multinational, more significant consideration needs to be given to how authorities can enable financial institutions to access shared data across multiple jurisdictions and the industry.

Results

The optimal result

Taking all of the considerations outlined in this document into account, a more innovative and effective approach to fighting financial crime is entirely feasible and well within reach. The transition to a compliance system that effectively incorporates AI would achieve the following results compared with the current status

Towards an AI-optimised regulatory future		
	From	**To**
Compliance approach	Prescriptive rules-based approach	Flexible risk-based prioritisation
Resources	Skilled, expensive staff	Complement experienced compliance staff with sophisticated and effective AI/ML
Output	Masses of rule-based alerts	Risk-prioritised alerts
Effectiveness	Immense proportions of false positives and few prosecutions	Considerable reduction in false positives with machine learning, behaviour-based results
Staff morale	Low. Undermined by repetitive, high volumes of mundane tasks that don't deliver meaningful AML results	Job satisfaction is higher as the AI takes care of the systematic tasks and allows compliance staff to pursue more satisfying investigative work
Customer impact	Time-consuming, onerous onboarding negatively affects client acquisition success rates	Could improve compliance turnaround times and customer onboarding

Results

The optimal result

> If AI is successfully incorporated, we will have a compliance system that has a much better chance of getting, and hopefully staying, one step ahead of the criminals to the benefit for financial institutions and the society at large.

Regulators are making headway and recognise the importance of creating the framework within which AI can contribute towards fighting crime in the future. The financial institutions are also coming together and collaborating, looking at ways to incorporate AI, with the broader regulatory and industry picture in mind. One of the priorities of the EBF in its blueprint for an effective EU framework to fight money laundering is Be Smarter, in which it says the financial sector should "Encourage the use of enhanced analytics and machine learning tools for KYC purposes which are respectful of privacy rights."

Much work still needs to be done to maximise the many benefits offered by AI at a regulatory, industry and firm level, while putting in place measures to deal with any risks that materialise along the way. However, it is encouraging that support is there, and the foundations are already being laid.

If AI is successfully incorporated, we will have a compliance system that has a much better chance of getting, and hopefully staying, one step ahead of the criminals to the benefit for financial institutions and the society at large.

slimmer AI

We believe AI is a people's business

Contact

Joost van Houten

joost.van.houten@slimmer.ai

Slimmer AI has a rich history in making the power of artificial intelligence and machine learning accessible in the daily work of people-driven companies. Together with their team of 30+ AI software developers, Slimmer AI's Sentinels combines a best-in-class user-centric design with cutting-edge AI techniques to fight financial crimes. Slimmer AI has offices in Groningen and Amsterdam in the Netherlands.

For more information: https://slimmer.ai.