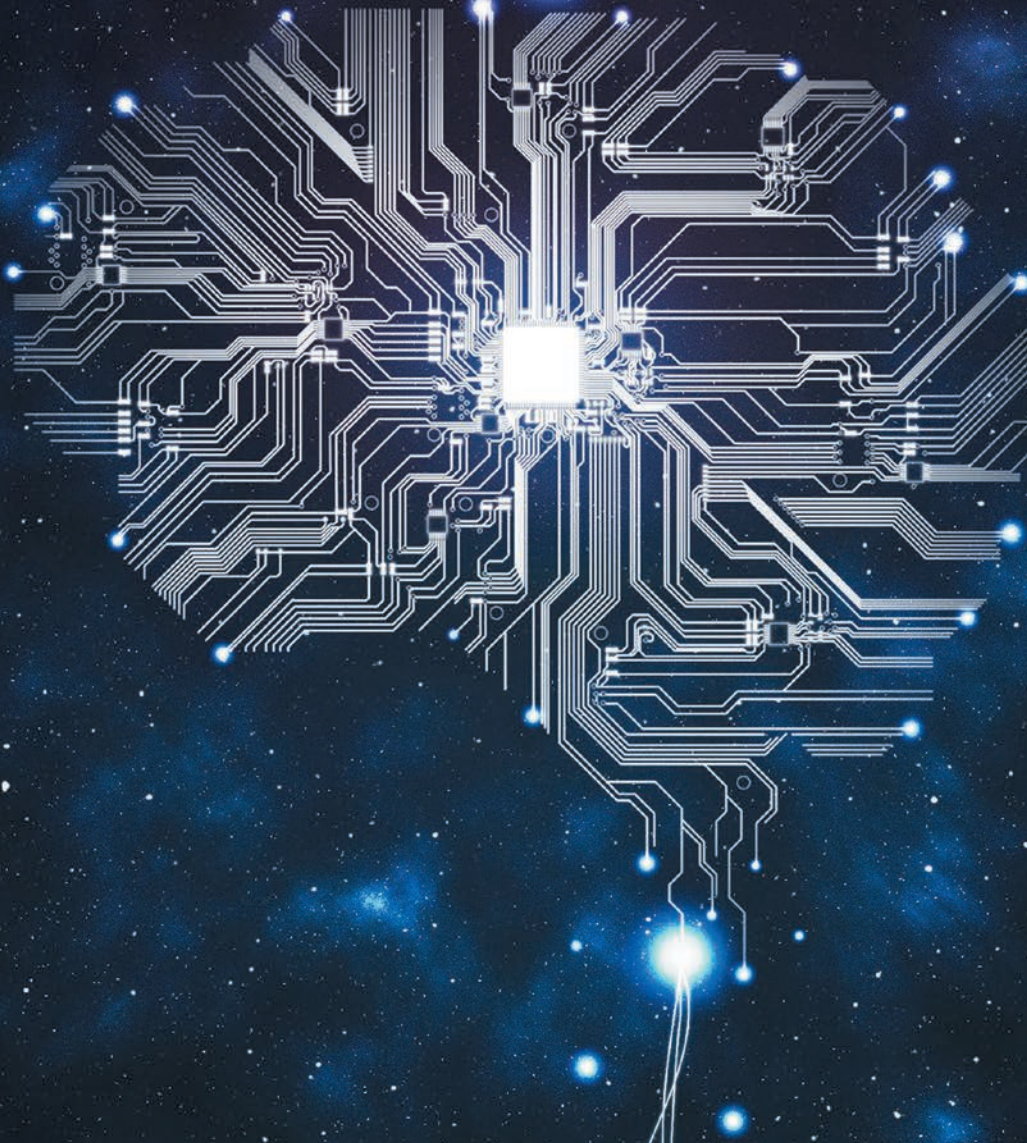


WHITE PAPER

Artificial Intelligence and Machine Learning in the Fight Against Financial Crime

JUNE 2020



In recent years the financial crime prevention industry has seen an increase in regulation driven by the behavior of the ‘bad guys’. Issues such as the Panama Papers, the Paradise Papers, lone-wolf terrorist attacks, increase in the use of digital currency and the global migration crisis are not only driving an increase in regulatory change, but also the pace of change. With the evolving nature of threats, recent regulation calls for faster response times to address financial crime; therefore, there needs to be a rapid acceleration in technological developments.

Recent regulation calls for faster response times to address financial crime; therefore, there needs to be a rapid acceleration in technology.

Furthermore, LexisNexis® Risk Solutions True Cost of Compliance research has indicated that Financial Institutions (FIs) struggle with the time it takes its staff to perform manual repetitive compliance tasks. **Labor is still accounting for the largest cost of compliance functions.** With that, as the behavior of FIs is mostly driven by regulatory changes, compliance functions are seen as cost centers, rather than profit generators.

Today, the industry is at an inflection point. **We are witnessing the development of new technologies, such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, big data, behavioral analytics and many others, which are making their way into different operations within FIs.** While many will think of these developments as the future, the fact is that the future is already here, and some western FIs have already implemented these technologies into their processes. Challenger banks have been particularly effective in building such technologies into their compliance processes as a part of their customer onboarding function, due to the lack of incumbent technology holding such developments back.

Terminology disambiguation

- **Artificial Intelligence** – Artificial Intelligence (AI) is a broader concept of machines being able to carry out tasks that we would consider smart. AI allows machines to learn from experience, adjust to new inputs and perform human-like tasks.¹
- **Supervised Machine Learning** – Machine Learning (ML) is a subset of AI built on the idea that systems can learn from data, identify patterns and make decisions with minimal human interaction.² Supervised ML utilizes algorithms, which already contain a known value for a target variable, where the humans provide answers to the questions during the training stage to the machine. This allows them to learn from humans in a “supervised” fashion.³
- **Big Data** – Big data is data that contains greater variety, arriving in increasing volumes and with ever-higher velocity. This is known as the three Vs... variety, volume and velocity.⁴
- **Data Analytics** – Data analytics, more specifically as it relates to big data, examines large amounts of data to uncover hidden patterns, correlations and insights that can be extracted from the data itself.⁵

AI, ML, big data and data analytics in financial crime operations

Today, most people understand the data driven approach when it comes to their recent online shopping behavior. We purchase goods online, and our preferred vendor will offer us goods that have previously been bought that might complement our purchase. The more data this algorithm has, the easier it is for it to make predictions and recommendations for users. Of course, this algorithm does not care about why the associations between recommendations exist, it only cares that they do. In compliance, industry analysts will care to know why.

FIs are focusing their efforts on introducing new technologies into their processes, and while there is still a lot of hype in the regulatory compliance market about them, the market research highlights four main areas that are being explored:

1. AI and data analytics as an enabler of efficiencies for FIs
2. AI and data analytics as a cost cutting/labor saving innovation
3. Risk reduction through pattern detection
4. AI and data analytics as a strategic value add for FIs



1. AI and data analytics as an enabler of efficiencies for FIs

The first thing that comes to anybody's mind when we talk about AI is the efficiency that such technology can drive for FIs. When we talk about introducing efficiencies into the process, industry reports discuss doing the same things better or faster, rather than introducing radical changes into FI strategic initiatives. The opportunities to pursue for driving efficiency are abundant, from deposits and lending, to insurance, capital markets, payments and other sectors, as the World Economic Forum illustrates.⁶

Additionally, FIs have been able to automate as much as 90% of their processes through the automation of manual work, thereby allowing human agents to focus on key decisions.

AI can help standardize time-consuming tasks and make them more efficient. With that, FIs have been introducing Robotic Process Automation (RPA), text analytics, insights and entity resolution, and network analysis into compliance for some time. AI and ML have the potential to enhance the efficiency of information processing and to reduce information asymmetries.

Similarly to AI, data analytics can help FIs to create more efficient and smarter organizations. Through the utilization of such technologies, FIs can get ahead of market changes and regulatory forces, which will drive business strategy and results, while using automation to handle huge volumes of data.



2. AI and data analytics as a cost-cutting/labor-saving innovation

Numerous FIs in the market are exploring the option of utilizing new technologies as a labor-saving innovation, due to the extremely high costs associated with compliance staff. The LexisNexis® Risk Solutions True Cost of Financial Crime Compliance Global Report published in 2020 estimates that **labor accounts for 57% of costs for FIs globally**. Compliance functions within FIs continue to be cost centers, and the costs of being compliant are increasing annually. With that, replacing menial repetitive tasks that humans perform today would be highly beneficial for FIs. However, humans should be repurposed for more strategic and comprehensive tasks, rather than just replaced by a machine.



3. Risk reduction through pattern detection

Most organizations aim to reduce the risks that surround it, which is also true for FIs in the market. These technologies have already been hailed as a solution to money laundering, fraud and terrorism financing. **FIs see the technology as means to help them improve their risk appetite**. Risk management is a consistent topic that comes up among banks, and it is mostly linked to pattern detection in customer behavior.

In other words, this technology could help to spot patterns in behaviors, which will later highlight anomalies in transactions in order to indicate that potential fraud or money laundering risks exist. AI can parse the masses of unstructured data to separate the signal from the noise. Machines can be taught to observe patterns from the past, therefore predicting how these patterns might repeat.

However, FIs should be careful about letting these technologies self-correct. AI, data analytics and ML based tools could miss new types of risk that arise, as they could potentially be over-trained on previous events.



4. AI and data analytics as a strategic value add for FIs

Organizations still struggle to select the right areas to use these new technologies. The reality is, only marginal improvements on existing data processing capabilities have happened to date.

Most of the western FIs are operating in a highly digitized environment, and developing economies are following suit. The volumes of online and mobile transactions, or even new account openings, are increasing, leaving FIs with a vast amount of data that can be leveraged to enable them to think more strategically about their customers. With that, the new technologies can help organizations to:

- **Scale the data they have**
- **Offer a more tailored experience to their customers**
- **Utilize compliance data gathered on an ongoing basis to help with tailored experiences**
- **Retain their customers**
- **Augment their performance**

AI can also be viewed as Intelligence Augmentation for all the organizations benefiting of this technology.

AI – the explainability

For the financial crime industry to be accepting of these new technologies, and for the regulators to be on board with their utilization, FIs should have a clear view of what it is that the technology is doing for them. The technology should be:

- **Explainable** – Algorithms used and the outcomes produced by the model must be fully transparent. In most cases special features are needed to make explanations useful and domain specific.
- **Risk-based** – This approach must remain top of mind. FIs must decide what problems they are addressing with the technology. They should document what they are doing and why, and then apply it consistently.
- **Performant** – Objective measures of benefits and risks must be calculated on a sufficient amount of data.
- **Not only AI/ML focused** – The likelihood of fraud or misconduct identified based on ML predication cannot and should not be the sole basis of any enforcement action. Therefore, FIs should be coupling technology and humans to get the best outcomes for their financial crime processes.
- **Aligned** – The technology should be aligned with data privacy concerns.

Our economic growth is highly reliant on the value that data creates, while data analytics and AI are great examples of such a data economy.

In its recent white paper on AI, the European Commission sets out the proposals to promote the development of AI, while safeguarding the respect of human rights. The Commission clearly outlines that our economic growth is highly reliant on the value that data creates, while data analytics and AI are great examples of such a data economy. The paper further states that authorities should be able to test and certify the data used by algorithms, and a risk-based approach should indeed be applied to AI applications.⁷

The application of AI, big data and data analytics is not an easy task for FIs. As AI is pulling FIs in many different directions, they need to be clear on their investments and activities, and more importantly, they need to separate their marketing story from the implementation story.

Finally, given recent changes in regulatory requirements for data privacy, data protection is coming to the fore. New systems that utilize AI, big data and data analytics will have to take into account in the first instance if certain data is subject to privacy rules before it can be used to train the system for compliance purposes. Although, regulatory requirements should always trump privacy concerns. With money laundering prevention, it is critical to distinguish between ‘guidance’ and ‘regulated advice’, and there is a fine line between the two.

The next generation in watchlist screening is here

LexisNexis® Intelligent Match Decision Solution uses AI and ML to reduce false positives and manual reviews.

As the volume of alerts, transactions and list entities grows, FIs and corporations are expected to absorb the rising operational costs for match remediation. Continually adding compliance staff only treats the symptom—too many false positives—and is not a practical, long-term strategy. Time spent remediating matches and distinguishing false positives from relevant risk drains resources and diverts attention from your core mission.

LexisNexis® Intelligent Match Decision Solution takes an innovative approach to efficient compliance by dramatically reducing the number of matches that require manual review. It can automatically remediate a significant percentage of matches found through Politically Exposed Person (PEP), adverse media and sanction screening.

Contact us to learn more.

For more information, call 800.658.5638 or visit risk.lexisnexis.com/FCC



About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

¹ https://www.sas.com/en_gb/insights/analytics/what-is-artificial-intelligence.html

² https://www.sas.com/en_gb/insights/analytics/machine-learning.html

³ <https://www.datarobot.com/wiki/supervised-machine-learning/>

⁴ <https://www.oracle.com/uk/big-data/guide/what-is-big-data.html>

⁵ https://www.sas.com/en_gb/insights/analytics/big-data-analytics.html

⁶ http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf

⁷ https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

This white paper is provided solely for general informational purposes and presents only summary discussions of the topics discussed. This white paper does not represent legal advice as to any factual situation; nor does it represent an undertaking to keep readers advised of all relevant developments. Readers should consult their attorneys, compliance departments and other professional advisors about any questions they may have as to the subject matter of this white paper.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Copyright © 2020 LexisNexis Risk Solutions. NXR14444-00-0620-EN-US