



AI biases in AML/KYC

AI biases in KYC/AML



Marius Frunza • IntelBlitz • 5 mins read • Nov 12, 2021

Artificial Intelligence is rapidly reshaping all sectors of the financial services industry. Leading financial institutions made a priority of adopting AI-powered KYC/AML solutions as part of their process automation roadmap. However, while AI-driven software can accelerate the onboarding of new clients and the monitoring of existing ones, it is also subject to algorithm biases. What are the hidden dangers of unqualified AI biases? Can criminals exploit such biases and outwit banks' surveillance?

Similar to human intelligence, AI learns to make decisions following a training process based on training data. If the training data is biased in any way, shape or form, the resultant algorithm will mimic those biases. For example, during the onboarding process, many banks are training their operations to decline applications of cryptocurrencies business. In addition, the same AI-based solutions are also declining any company that seems related to or has a brand similar to crypto-firms.

Moreover, if the training algorithms are not fit for the target data, then they could lead to biased outcomes. Thus, the use of models could help in mitigating risk but can also generate new risks.

Financial institutions have specific policies for managing the risk stemming from the use of models. Pursuant to the current prudential frameworks (SR 11-7: Guidance on Model Risk Management), model risk is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model risk can lead to financial loss, poor business and strategic decision-making, or damage a financial organisation's reputation. Concerning AI biases, model risk occurs primarily for two reasons:

AI is not perfect

- an AI model may have fundamental errors and produce inaccurate outputs because the training data is inappropriate;
- an AI model may be used incorrectly or inappropriately, or there may be a misunderstanding about its limitations and assumptions.

In the case of KYC/AML solutions, AI biases concern the following aspects:

- **Data** - If training data have biases or is very different from the application dataset, the AI will have intrinsic biases. Humans have prejudices from their past experiences, and AI has biases stemming from the learning process.
- **Overfitting** - Overfitting occurs when a statistical model fits precisely against its training data. An AI built with an overfitted model could show serious limitations when applied to data that is different from the training data.
- **Mimetising human cognitive biases** - One of the primary roles of AI is to replace human actions. Thus, when AI is replicating human cognitive processes, it inherits also the underlying cognitive biases.
- **Usage** - If an AI solution is used in an area where it is not fit for its purpose, it could carry biases.

AI-driven KYC/AML solutions aim to reduce the number of false positives and negatives. AI biases may solve in some areas this issue but can generate wrong classifications in other areas. For example, before the digitalisation of the financial services industry, when client-banker contact was in person, criminals made a science from exploiting the human cognitive biases. If AI-biases become persistent in the KYC/AML frameworks, they could easily be used by criminals who want to trick the bank.

“The upheavals [of artificial intelligence] can escalate quickly and become scarier and even cataclysmic. Imagine how a medical robot, originally programmed to rid cancer, could conclude that the best way to obliterate cancer is to exterminate humans who are

genetically prone to the disease."

Nick Bilton, tech columnist

Sanctions: Minsk

A new migrants crisis

The proxy war between Minsk and Brussels that erupted last year amid controversial elections escalates new tensions. Migrants from Iraq, Syria, Iran and several Northern African states massed on the Belarus-Poland border,

Brussels has accused Minsk of pushing migrants to come to European Union countries then channelling thousands of them to cross into Poland and other neighbouring EU states in retaliation for sanctions imposed on Minsk. As a result, thousands of people remain stuck in the open in harsh weather on the Belarusian-Polish border amid a neverending proxy war between Minsk and Brussels.

The European Commission is now deciding to extend sanctions to include "third-country airlines" involved in flying migrants to Belarus. Brussels was looking at flights to Minsk from several countries, including Syria, Iran and Qatar, and Russia and several North African states.

Thus, EU officials are finalising a new fifth round of sanctions on 30 Belarus officials and entities, including the foreign minister and state-owned airline Belavia. Brussels is also considering the sixth package of asset freezes and travel bans, including orders to stop EU firms supplying Minsk National airport. Moreover, the EU is accusing Moscow of being involved in this coup.

In retaliation, Alexander Lukashenko has raised the prospect of cutting the Yamal-Europe pipeline, which supplies gas to Germany and Poland, if Brussels imposes new sanctions against his regime over the influx of migrants on the country's western border.

Word on the street: Lords of scam

Crime imitates art

The fraud on carbon markets took place more than a decade ago. Netflix brings attention back to that episode with [Lords of scam](#). This documentary traces the rise and crash of scammers who conned the EU carbon quota system and pocketed millions before turning on one another. The movie's key character is Mardoché "Marco" Mouly, a figure of the French-Israeli gang with extensive experience in VAT fraud with mobile phones. Mouly was born in Tunis and grew up in one of Paris's poorest districts. Mouly was a close friend of Arnaud Mimran, who invested over 800 thousand euros in IGA Électronique, a mobile phones trading company based in France, Dubai and Hong Kong. Later, the two men enter into the CO2 emission trading. He was in charge of logistics in the carousel fraud engineered by the Mouly-Mimran group.

Mouly fits the profile of old-style crooks that stayed faithful to his criminal philosophy. He helped the Souied family after the death of his friend Samy and also cut ties with the posher and more flamboyant Mimran. Mouly was a fugitive for 18 months, until November 2016 when he was arrested in Geneva, where he allegedly attempted to get some funds from several accounts opened with HSBC. These accounts were controlled by companies registered in Panama, named Phantomas, one of Mouly's nicknames.

Know Your Network, AI meets KYC

More insights at schwarzthal.tech



Marius Frunza
marius.frunza@schwarzthal.com

The information and data published in this newsletter were prepared by the market research department of Schwarzthal Tech

Contact

contact@schwarzthal.com
FR: (33) 6 27 29 78 34
UK: (44) 7 95 22 08 734
RU: (44) 7 95 22 08 723

Address

Devonshire House, 582
Honeypot Lane,
Stanmore, England,
HA7 1JS

Social

twitter.com/schwarzthal
linkedin.com/company/schwarzthal-tech