the payments association

The Payments Association's Guide to Artificial Intelligence

Use Case: Fraud detection

Gergo Varga
Content Manager
Seon

Read The Payment Association's Using AI Intelligently Guidebook **here**

> From a fraud perspective, the best time to adopt and upgrade AL capabilities is just before an attack!

What is AI and what are the different types?

When people talk about AI, they mostly talk about ML which is training machines to look for and recognise patterns within data sets. But it is important to remember that at the end of every transaction there is a human story. So there also needs to be human oversight and context as well, unless you can feed the ML with the entirety of the world's knowledge, which is basically impossible we need to keep human oversight. Tech is never the golden answer, but it is a key part of the jigsaw.

Why is AI so suited to fraud management?

The massive acceleration in all things digital over the past two years means volumes and scope are both up. The security around that has had to be beefed up. Sadly, the fraudsters have also beefed up their attack capabilities. AI is a very important tool that both the payments industry and the fraudsters have access to and its cost has come down. ML models now routinely run in the background looking for suspicious patterns or sequences.

Any ML system needs to be fed and updated constantly to learn, so that the quality of the data sets is up to scratch. The workman is the AI but it is only as good as the tools it is given data wise and instruction wise. The machine can only match the patterns given to it and connect what you tell it to or look for combinations that you tell it to. Facebook, for example, can predict behaviour looking at the behaviour of all the people someone is friends with, but payments and fraud is numerical and not behavioural to the same extent

Where the care is needed for the human element. It is easy to decline something and be super cautious but annoying for a customer if they have to go through verification checks on something. So it's important to get the balance right between identifying something as suspicious, double checking and deciding what, if anything, to do about it.

Where else can AI be deployed?

Chatbots are a lot better than they were but there is still a lot of hype around them. Especially since they can break a conversation down into small blocks, some of which they can deal with, some of which they can't. Thus, human intervention is still a must. You also need the buy-in of the user to convince themselves that they are having a real conversation with a person who cares, not a machine.

With regards to facial recognition, the more we eomply AI the more we abstract the problem. For example, we can use facial recognition technology, but enterprising fraudsters will also use it. They Photoshop your image and take your name and use it. The human element is important. For example, 10 years ago selfie verifications were not even a thing, the tech was not there. If a set of fraudsters all doing their selfie verification in the same place, the ML would not pick up on that it would be looking just at facial recognition, but to a human that would strike as immediately suspicious.

What is uptake like and why?

Legacy players are less able to provide cleansed and usable data and Neobanks are much better at this, but Neobanks tend to offer a limited product suite and so can't have enough data to make 360-degree views of the customers and thus their realm of experience is more limited.

Barriers to adoption – how best to do this?

From a fraud perspective, the best time to adopt and upgrade AL capabilities is just before an attack! Having something that you think is good enough is only good enough until it is not anymore. One of the biggest advancements is the use of adversarial networks where networks are pitted against each other to improve themselves. Accountability and the difference between having a black box or a white box set up is important. Where there is no human involved in a transaction it's hard to challenge an ML made decision unless you can see how and why that decision was made.

> "
>
> Facebook, for example, can predict behaviour looking at the behaviour of all the people someone is friends with, but payments and fraud is numerical and not behavioural to the same extent