THE EUROPEAN
BI-MONTHLY
JULY-AUGUST 2017
www.the-european.eu

UNDER PRESSURE
MBAs that take you out of your comfort zone

MOVING WITH THE TIMES
How to thrive in a mobile-first economy

FIGHTING FRAUD
Man and machine work in harmony

A STRATEGY FOR GROWTH
How Dr Coutinho Nobre Miguel and BANCO SOL are driving change in Angola

UK £3.95,
Europe €5.00

INSIDE: EXECUTIVE EDUCATION ▮ TECHNOLOGY ▮ BANKING & FINANCE ▮ BUSINESS TRAVEL

MAN AND MACHINE:
the perfect fraud-fighting team

Roberto Valerio, CEO of fraud prevention software experts Risk Ident, explores the rise of machine learning technology in helping businesses fight back against online criminals

Science fiction would have us believe that man and machine will one day wage war on each other, but the reality is that artificial intelligence (AI) and machine learning have been with us for years, and technology is already helping us in ways we may not have fully appreciated.

Big data was very much the technology industry buzzword of the last decade. The scale of technology access and adoption accelerated to the point whereby businesses and consumers were generating massive amounts of data on everything from payment transactions, to browsing and shopping habits, through to insurance claims and medical diagnoses. However, for years businesses struggled to make use of the data – in particular, how to extract actionable intelligence and meaning from it.

As technology evolved, though, it became more affordable and more accessible, enabling the development of algorithmic software to help make sense of this data. Popular machine learning algorithms, including Random Forest, Naive Bayes and Logistic Regression, have become widely adopted, while innovative, agile businesses began applying machine learning to their high-growth businesses.

Spotify, for example, will recommend new songs and albums suited to our music taste. The more music we listen to, the more data it has to make more accurate decisions. Similarly, Amazon will suggest books, groceries, electronics and more depending on our shopping habits over time. Meanwhile in healthcare, computer-aided diagnosis can be trained to spot health changes that may otherwise be missed.

Fraud prevention is another world in which machine learning is transforming ➤

how we operate. Currently, in Europe we have around 300 million online shoppers, spending more than 510bn euros each year.[1] This is rising rapidly and is great news for retailers across the continent. However, online fraud rates are also rising as fraudsters aim to exploit vulnerabilities online; we now see 66% of the EU's total card fraud coming from card-not-present (CNP) transactions.[2]

Man cannot fight vast numbers of fraudsters alone. But significantly, neither can machines. A common misconception about machine learning is that it's the silver bullet that solves all our problems and removes the need for human intervention or management. Many organisations claim that the machine learning component of their product is like a secret ingredient. But while machine learning is important in the overall recipe, it's not the only key ingredient you need.

One indispensable ingredient is the type of data you feed in – if you feed in only low quality data then you can only expect low quality results. In fraud prevention, the quality of data is paramount to strong results – and it is even more important to refine the data. This is called 'feature engineering', a process that uses the domain knowledge of data possessed by company fraud managers to create the very features that make machine learning algorithms work.

Human intelligence supported by domain knowledge is vital to this process of data refinement. From experience, fraud managers know how to handle different fraud scenarios for different companies, industries and consumers. If a company gets this process right, then it's easy to see how inputting the right features into the machine will generate the strongest results out of it.

Even then you cannot rest on your laurels – fraudsters won't give up and will work in highly 'professional' ways and teams to find weaknesses to exploit. Fraud prevention must evolve quicker than the fraud threat, which is why it is vital to scale a machine learning system, on a production level, in terms of the amount of data and response times.

Not keeping pace

Last year at Risk Ident, we conducted a survey, which found that online merchants followed worryingly long cycles when it comes to adjusting their fraud prevention rules. Less than half (42%) of businesses surveyed revealed that they change their fraud rules more than once a quarter, with 26% reporting that they review and amend their fraud rules once every six months, and a staggering 22% who only readjust them once a year. This is alarming and dangerous.

Think how often your laptop or mobile apps will download software updates each month or even each week. They are constantly doing so, not just to provide new features, but to patch security risks and respond to constant probing from hackers testing the system. Online fraud should be treated the same – fraudsters don't wait to change their tactics every quarter or once a year, so refinement of fraud rules should be far more frequent.

"Fraud prevention must evolve quicker than the fraud threat"

The good news is that machine learning helps significantly in this process, enabling businesses to scale their fraud prevention to handle the huge numbers of good customers while identifying and stopping fraudsters in their tracks.

We believe in being transparent

with businesses about the machine learning components they use, sometimes even explaining which specific set of algorithms are using their data to help reassure them via a stable, productive software solution where fraud managers know what they need to put in.

Machine algorithms will typically only understand numbers, so companies need to get their data pre-processed through what's known as "feature extraction". For example, a customer address can be converted into a geolocation, which can help identify local patterns or movements of fraudsters. Similarly, an email can be evaluated by name, domain or general structure of the email to help identify fraud patterns that may otherwise be missed, whether it be uncommon names, risky domains or uncommon outliers that suggest illegitimate activity. Feeding in an email address to the machine learning component enables the system to find other transactions with a similar email structure, name, or domain that may be at risk.

The best aspect of machine learning, as the name suggests, is that the technology learns and evolves over time. It gets stronger and more accurate the more relevant data it has fed into it, and because these incremental improvements are based on hard data, the technology can respond quicker and with greater surety to emerging threats such as credit loan application fraud and account takeovers, where fraudsters use stolen personal data to log in to genuine accounts before wreaking havoc behind the smokescreen of a good customer history.

Alone, the machine cannot factor in the nuances that a knowledgeable fraud manager can apply to the data in order to see through such smokescreens. Fully-automated machine learning out of the box might sound great, but if you truly want to reduce fraud, it's more of a myth; the reality is that man and machine – together – are our best defence. Rather than bringing about our doom, machines could well prove to be the best friends we have in staying safe in the digital world. ■

ABOUT RISK IDENT

Risk Ident is a software company that offers world leading anti-fraud solutions to companies within the ecommerce, telecommunication and financial sectors – empowering fraud managers with intelligence and self-learning machine technology to provide stronger fraud prevention. The company is home to a veteran team of skilled data scientists and software engineers with long-term experience in data analytics and machine learning. Risk Ident's products are specifically tailored to comply with European data privacy regulations.

About the author

Roberto Valerio is the founder and CEO of Risk Ident. He plays an active part within the fraud prevention community and is a member of the European Advisory Board at the Merchant Risk Council. He has also founded and worked within different management roles for software startups.

Further information

www.riskident.com

[1] www.ecommerce-europe.eu/app/uploads/2016/07/Infographics-2.jpg
[2] www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016