THE PAYPERS

Insights into Payments and Beyond

Fraud Prevention and Online Authentication Report 2019/2020

Managing Risks and Preventing Fraud with New Technologies and the Right Expertise

Endorsement partners:

MRC Building Better Commerce Fraud & Payments Professionals

Marketplace Risk.

Key media partners:

mpe MERCHANT PAYMENTS ECOSYSTEM

Money 20/20

Nethone

Hubert Rachwalski, Nethone's CEO, reveals how to adapt to new technology and attacks without a suitable pre-existing data set.

About Hubert Rachwalski: Hubert is responsible for creating and operationalising Nethone's go-to-market strategy, coordination of key business development projects and building relationships with all stakeholders. He is an experienced business executive with extensive professional experience earned in the world's leading consulting firms (BCG and PwC) and has been advising the Board of Daftcode, one of the most prominent tech venture builders in Central and Eastern Europe since 2016. Hubert wrote his first Master's thesis on leveraging AI for stock portfolio optimisation problem.

Hubert Rachwalski ▪ *Chief Executive Officer* ▪ Nethone

What are the fraud trends and challenges when it comes to real-time payments?

Preventing online fraud is a constant arms race with way too many civil casualties. Namely, online merchants often do lack appropriate tools to exhaustively understand their visitors and users and, consequently, their evaluation of transaction risk can be suboptimal. By leveraging rules-based systems they tend to systematically make mistakes and reject legitimate users. Given the ever-experimenting nature of fraudsters, merchants react by multiplying rules, which are supposed to address the issue. Over time, it leads to a deterioration of the system's precision and even further increased false positives number.

> *"Unlabelled data leads to a suboptimal situation that we have to deal with, and the reception of labelled data or feedback is something we should strive for.*

Furthermore, it is crucial to understand the modus operandi of the other side of the barricade – fraudsters – whose actions could be generalised by three main motivations:

- anonymise – try to avoid being caught, if you want to make a living off it;
- automate – extract the value from stolen cards as quickly as possible as the Expected Value decreases over time, as well as innovate and experiment;
- modify your conduct to test for thresholds, as the most systems are rule-based, so modifying parameters can expose a system's vulnerability.

We observe a growing trend of cookie hijacking of trusted machines (as an effect of PSD2) and increasing ratio of mobile frauds. That's why we developed mechanisms that monitor cohesion of sessions in all possible domains. We focus on advanced raw behavioural analytics – widely untapped source of additional insights about users, leading to less friction for them, and higher conversion rates for the company.

To reach such accuracy, we leverage machine learning (ML), and we put special effort into making it a 'white-box' and explaining how it works to our clients. Without their trust in ML, we wouldn't have the full buy-in from them.

Can these issues be tackled with unsupervised machine learning? If so, how do you apply this technology to detect real-time fraud?

Unsupervised ML boils down to a robust method of clustering similar events or objects into groups of entities that resemble each other the most, and so that the distinguished groups are as dissimilar from each other as possible. ➔

Nethone

Of course, the concept itself can be used for fraud prevention and we use it, for instance, to distinguish malicious fraudsters from friendly fraudsters. Unsupervised methods are especially helpful while having problems with assigning a reason code for a fraud or a chargeback and more intricate labelling.

However, we believe relying solely on fraud labels is not enough, and supervised ML models are also important. You can teach a model to understand similarities of the session profiles of users and correlate them with the fact that spikes in similarity often point to a fraud attack. Thanks to ML you are able to compare those similarities with 5000+ attributes per each session and compare them to the historical ones in real time, while being able to piece multiple similarities to various parts of past sessions.

What is the best strategy to avoid false positives with unlabelled data, especially when there is little transaction data available?

Start out with blocking transactions that stem for suspicious activity. We provide a list of almost 100 signals (interpretable occurrence of a suspicious activity or characteristics, e.g. 'mobile emulation on a desktop device' or 'connection associated with TOR network') to the client that we set up from day 0. As a next step, we set up models that detect events easy to correlate to fraud – similarity model, industry-based model.

However, we have to remember that unlabelled data leads to a suboptimal situation that we have to deal with, and the reception of labelled data or feedback is something we should strive for. We believe it's important to bring the power of supervised models to reach the pinnacle of performance with a hybrid setup.

What striking facts or anomalies did you discover while applying unsupervised machine learning?

Friendly fraudsters are far more similar in terms of behaviour and data to genuine customers than to malicious fraudsters. A strong difference between these first two groups is that friendly fraudsters seem to have gone through the process many more times than the genuine customers, which is reflected in their raw behaviour (the way they type on the keyboard, how they use the mouse, how they scroll/tap etc.). Also, promo days are more interesting to the fraudsters than to the genuine customers – the ratio between fraud group and other group grows in favour of malicious transactions.

What product developments and services does Nethone have in the pipeline?

We believe that raw behavioural analytics is a great source of knowledge about users. We take account takeover prevention to another level with Nethone ATO, our passive biometrics solution, by providing an end user with the highest possible security, while not compromising their identity privacy.

Nethone is all about transparency – delivering a platform for both merchants and clients and trying to explain the way our ML models work in a clear, visual way. We also look into further automation of manual reviewing process. We want to limit the number of repeatable tasks and, as a result, decrease operational costs of our clients. As ML is being developed to the levels where it's more efficient than humans (e.g. in face recognition), our ambition is to bring such performance to the fraud prevention industry.

About Nethone: The global provider of AI-driven KYU (Know Your Users) solutions that help enterprises from all around the world convert cyberthreats into accurate and profitable decisions. Know Your Users to resolve fraud. Gain more loyal customers, reject only fraudsters. All thanks to proprietary online user profiling (5000+ attributes) and explainable machine learning . In real-time.

www.nethone.com

Click here for the company profile

Company	Nethone
Nethone	Nethone is the global leader in AI-driven KYU (Know Your Users) solutions that help enterprises convert cyberthreats into well-informed, profitable decisions. From world-class fraud prevention, through real-time adaptive customer segmentation tools, up to account takeover detection based on advanced behavioural biometrics, Nethone services protect bottom lines and elevate profits of businesses.
Website	www.nethone.com
Keywords for online profile	fraud prevention, Know Your Users, payments, machine learning, artificial intelligence, profiling
Business model	SaaS
Target market	- Financial institutions - Payment services providers - Web merchants - Other online businesses
Contact	contact@nethone.com
Geographical presence	Global
Active since	2016
Service provider type	Web fraud detection company
Member of industry association and/or initiatives	Yes
Services	
Unique selling points	From the beginning our ML was designed to fight fraud. It provides a combination of plug and play artificial solutions and human intelligence that (combined) ensure the best results. Our proprietary profiler is built through dark web investigation. The light integration and specialisation in the singularity of every business make us stand out on the market.
Core services	Card-not-present fraud prevention, credit-scoring support services, business intelligence
Pricing model	Pricing is per inquiry
Fraud prevention partners	Straal, ERIF (KRUK Group), PZIP (Polish Association of Lending Institutions)
Third party connection	Ekata, Emailage, Maxmind, ExactBINs, Ethoca, Paay, Perseuss
Technology: anti-fraud detection tools available	
Address verification services	N/A
CNP transactions	Yes
Card Verification Value (CVV)	No
Bin lookup	Yes
Geo-location checks	Yes
Device fingerprint	Yes
Chargeback reduction	Yes
Payer authentication	Yes
Velocity rules – purchase limit rules	Yes
White list/black list database	Yes
KYC – Know Your Customer	Yes
Behavioural analysis	Yes
Credit rating	Yes
3D Secure 2.0 – authentication	Yes
Machine learning	Yes
Data analytics	Yes

View company profile in online database

Follow-up action	Real-time recommendations: accept/deny/manual review (optionally), case management, post transaction alerts, post transaction notifications
Other	Profiling, dedicated data scientist
Authentication technology used	
Password/phrase	N/A
One-time password	N/A
Token	N/A
Digital certificates	N/A
Multi-factor authentication	Yes
Biometrics	Yes
Card	N/A
PIN	N/A
Authentication context	
Online	Yes
Mobile	Yes
ATM	N/A
POS	Yes
Call centre	Yes
Other	Offline, agent
Reference data connectivity	
Connectivity to governmental data	N/A
Other databases	Emailage, ExactBINs, Perseuss
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Clients	
Main clients/references	LOT, Azul, ING, Farfetch, eDestinos, eSky, Thales, PKO BP
Future developments	Ecommerce, banks

Nethone

Know Your Users™ to resolve fraud

Gain more loyal customers, reject only fraudsters

Recognize and reject non-human interactions of bots and scripts, suspicious behaviour, anomalous device configuration and fraudulent tools. Use Machine Learning to identify recurring users and prevent ATO.

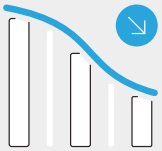
Payment fraud prevention

Exhaustive online user profiling

Passive behavioural ATO protection

Increased sales conversion

Secured end-user experience



Reduced costs of manual verification

Solve your fraud problem more effectively!

Schedule a demo at nethone.com