RiskTech 100 2021

swiss made software

Payment fraud prevention

The AI risk platform to mitigate payment fraud in real-time

Traditional anti-fraud practices find it impossible to prevent payment fraud in real-time, and efficient manner. But that is what they must do to beat the fraudsters.

As payment channels have multiplied, so have the routes open to fraudsters, pushing up banks' liabilities. In addition, with the introduction of 24/7 banking and instant payments, banks have to process far more transactions and have much less time to review them. For financial institutions worldwide, the challenge is to process and clear payments rapidly and accurately while keeping pace with the ever-increasing number of transactions*.

Most rely on the analysis of static and known fraud schemes. But these fail to detect new fraud patterns and trigger large numbers of false alerts, diminishing operational efficiency and the customer experience. In the payments area, these approaches remain insufficient for banks needing both speed and accuracy in fraud detection and prevention. Further, authentication methods remain inefficient as fraudsters exploit weaknesses in the different methods.

Prevent fraud in real time

NetGuardians' AI risk platform NG|Screener is scalable and analyzes large volumes of transactions per second to identify the fraudulent in real time. Instead of looking for existing fraud schemes, NG|Screener monitors behaviors of bank customers and employees to detect anomalies and identify fraud. NetGuardians' innovative approach enables banks to not only prevent payment fraud in real time, but also detect emerging payment fraud schemes accurately and efficiently.

Compared with a rules-based controlled environment, banks using NG|Screener for payment fraud:

- → Achieve a reduction in the number of false alerts of up to 83%
- → Increase their fraud detection rate by up to 118% (thereby discovering new fraud cases)
- → Spend up to 93% less time investigating alerts

* ACFE, Report to the Nations 2014

Payment fraud prevention

Get it on-premise or cloud

No data-sourcing headache

NG|Screener plugs directly into payment gateways via pre-set connectors. It extracts, enriches, and analyzes data, spotting and stopping payment fraud from day one.

Explainable AI

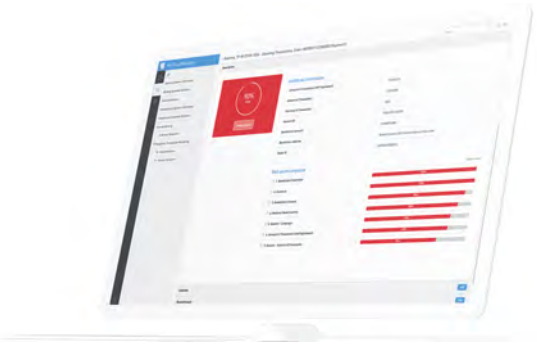
You don't need to be a data scientist to make sense of the AI algorithms' reports. A simple dashboard makes it easy to understand the reason for an alert and gives immediate visibility of the full business context. Powerful forensics using intuitive tools make investigation straightforward.

Ready-to-run AI risk models

Our AI risk models do all the heavy lifting. They monitor the relevant variables to spot and flag anomalies attached to any payment transaction in real time.

Prevent fraudulent payments:

- → Carried out using invoice redirection techniques
- → Carried out using social engineering techniques
- → From compromised corporate treasury systems
- → From various scams (love scams, CEO fraud, etc.)
- → Carried out on the SWIFT network
- → And many more use cases



Tier 1 to Tier 3 banks trust NetGuardians. Some references include:

Retail banking

Private banking

Digital banking

UOB

PICTET

Swissquote

BCN

REYL innovative banking

FirstOntario CREDIT UNION

Santander PRIVATE BANKING

Contact us for more information

For more information on payment fraud prevention, please contact us at sales@netguardians.ch

Headquarters

Y-Parc, Avenue des Sciences 13
1400 Yverdon-les-Bains, Switzerland
+41 24 425 97 60

Africa

The Mirage, Tower 2, Pentfloor,
Waiyaki Way, Westlands, 00101 Nairobi, Kenya
+254 709678 005

Asia

1 Finlayson Green #12-02
Singapore 049246
+65 6224 0987