Fraud and Cybercrime In the Age of Digitization

Applying Machine Learning and AI in Enterprise Fraud Detection

Timothy Choon
FICO
Sophisticated, organized fraudsters equipped to exploit byproducts of payment technology innovation

Physical theft
Sale of fake and stolen payment cards
Identity theft and application fraud

A brief history of fraud
Phishing, social engineering and mass data compromises
Organized fraud rings using advanced analytics and cyber attacks
“The trajectory of fraud attacks on the financial value chain is rising on a number of fronts. Data breaches abound, putting an unprecedented quantity of payment card data, personally identifiable information (PII) and stolen credentials in the hands of organized crime rings.”

Julie Conroy, Research Director at Aite Group
Automated discovery of patterns across large volumes of streaming transactions

Thousands of computations to be accurately performed in milliseconds

How FAST Is Payment Fraud Detection?

200 MILLISECONDS
GOOGLE SEARCH

185 MILLISECONDS
HELICOPTER ROTOR ROTATION

60–80 MILLISECONDS
AIRBAG INFLATION

300 MILLISECONDS
BLINK OF AN EYE

200 160 120 80 40
SLOWER FASTER

240 200 120 80
20 MILLISECONDS
REAL-TIME ANALYSIS OF FRAUD RISK

15,000
CALCULATIONS IN MILLISECONDS

Calculations are performed in milliseconds by FICO® Falcon® Platform to detect fraud whenever a credit card is used or a payment is made.
Applying Machine Learning to Enterprise Financial Crime and Fraud

- Integrating supervised and unsupervised AI models in strategy
- Distinguishing specialized from generic behavioral analytics
- Applying behavioral profiling analytics
- Adaptive analytics and self learning
- Leveraging large datasets in model development & training
### FICO Techniques – Profiling System, Neural Networks and Consortium

<table>
<thead>
<tr>
<th>Profile Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction profiles</td>
<td>Behavioral Machine Learning profiles for each consumer’s financial and non-financial activity. Updated in real-time with each transaction, across all channels.</td>
</tr>
<tr>
<td>Collaborative profiles</td>
<td>Improves risk sensitivity by identifying behaviors that differ from typical behaviors within individuals’ peer groups.</td>
</tr>
<tr>
<td>Behavior sorted lists</td>
<td>Deep learning behavioral analytics that identify and rank recurrent activities that are unique to each individual, such as favorite merchants, ATMs or destination accounts, in order to significantly reduce false positives.</td>
</tr>
<tr>
<td>Merchant profiles</td>
<td>Aggregated transactions at merchant-level to form behavioral metrics for a more comprehensive view of risk.</td>
</tr>
<tr>
<td>Multi-layered self-calibrating profiles</td>
<td>Detects behavioral outliers in real time even with limited or no data to train the model and automatically adjusts to accommodate new behavioral patterns. Advanced instances use deep learning to further improve pattern recognition.</td>
</tr>
<tr>
<td>User-defined profiles</td>
<td>Flexible, custom-defined profiles for entities such as devices or IP addresses.</td>
</tr>
<tr>
<td>Global intelligent profiles</td>
<td>Real-time adaptive risk ranking to monitor and respond to the riskiest profiles for improved fraud assessment.</td>
</tr>
</tbody>
</table>
Thank You

Timothy Choon
FICO