

## CASE STUDY

Client: N° 5 online marketplace  
Solution: Behavioral Biometrics

# Behavioral Biometrics for more security

No. 5 online marketplace successfully combats ATO  
using behavioral biometrics

→ How our client succeeded in preventing 2.000 ATO per day,  
reduced its losses due to fraud by EUR 1.2 million and increased its  
conversion while maintaining security at the highest level.

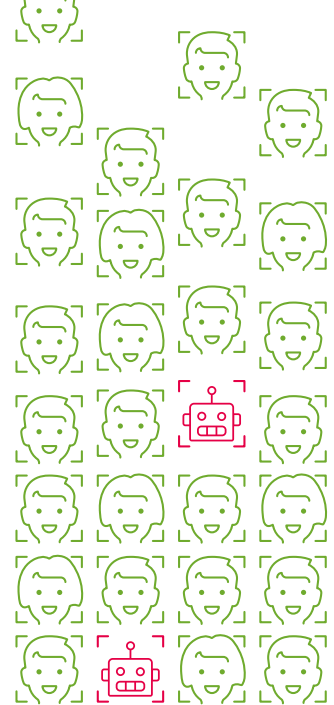


**FRAUDSTER OR  
GOOD USER?**

## 01

### Our client

Since 2018, we have been able to call one of the top five online marketplaces one of our clients. The company runs a native iOS and Android app with over 9 million app downloads and a web-based platform. The company is steadily growing, but the number of account take-overs is also increasing exponentially. In order to reduce the reputational damages and costs arising from fraud, a solution had to be found.



## 02

### Initial situation

The client had to deal with countless account take-overs (ATO) every day, which needed to be investigated using costly, manual order reviews and were strongly dependent on the rule set. The standard approach of the fraudsters: gain access to accounts of legitimate users, place orders and have them sent to the desired address, which is usually a post office collection point. The consequence: a relatively high rate of chargebacks that increases the need of the online merchant to take action.

In short:

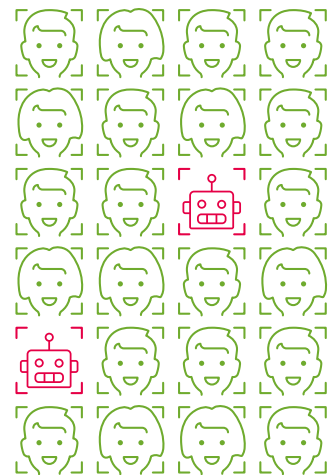
↘ reputation  
↘ effective operating processes

↗ chargebacks  
↗ manual order reviews  
↗ chargeback handling

## 03

### The challenge

- **Security without side effects:** Establishing high security standard without impacting on the customer journey and conversions.
- **Detection, not monitoring:** Identify users with fraudulent intent, bots or emulators when attempting fraud to prevent consequential damages.
- **Security without a loss of performance:** Implement a scalable fraud solution with a minimal technical footprint to keep site performance high.



Request business insight now:  
[„Harnessing the power of Behavioral Biometrics“](#)

## 04

### Our solution

Detecting fraud before it occurs. The use of behavioral biometrics helps to recognize fraudulent activity at an early stage.

- Recognizing legitimate users based on behavioral biometrics data and device anomalies through machine learning.
- Creating a trust score in real time to distinguish legitimate users from fraudulent, non-human users and to stop orders.
- Continuously and invisibly analyzing user data and account activities within a website or app.

## 05

### The result

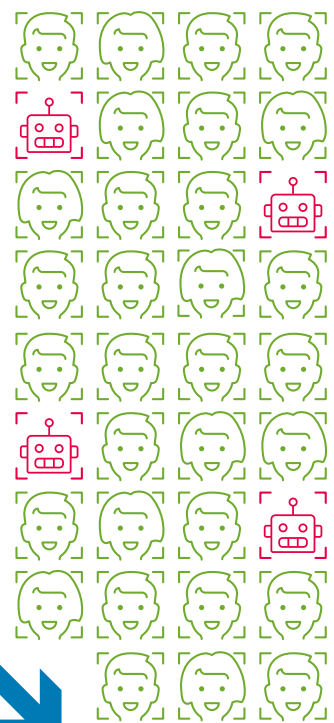
- Reducing the costs of fraud by more than €1,200,000
- Preventing over 2,000 ATO per day
- Improved customer experience for loyal customers due to fewer security hurdles
- Reducing internal costs arising from automation of manual orders
- Successfully handling constantly increasing transactions

## 06

### Statement by the Head of Risk

N° 5 online marketplace

The solution has successfully met our initial requirements, and soon after the straightforward implementation we were already able to measure a significant decline in the rate of fraud, chargebacks and refund requests. We are delighted to have found a solution that detects ATO prior to the transactions, without having a negative impact on the customer experience and hence inevitably on conversion.



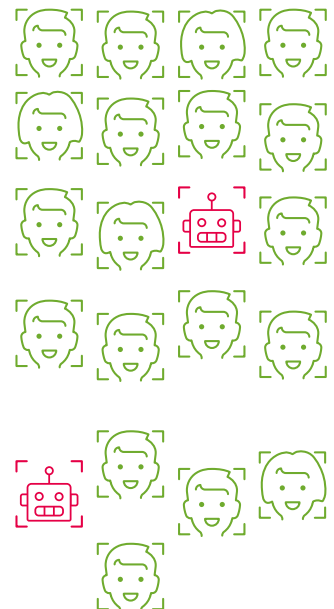
Reduce

- financial losses
- fraud rate
- internal costs



Increase

- customer experience
- legitimate transactions



Request business insight now:  
„Harnessing the power of Behavioral Biometrics“