

Identity verification and anti-fraud protection using the machine learning model factory

Piotr Wojewnik, PhD

Board Member, Digital Fingerprints S.A.,
Data Science Director, BIK S.A.



BIK GROUP



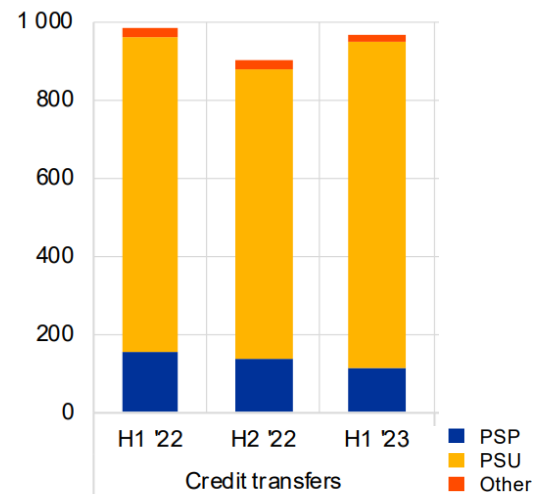
Challenge in Europe

Credit transfers are charged with the **value of the payment fraud up to 1 billion EUR in a half a year** in the financial industry across the EEA.

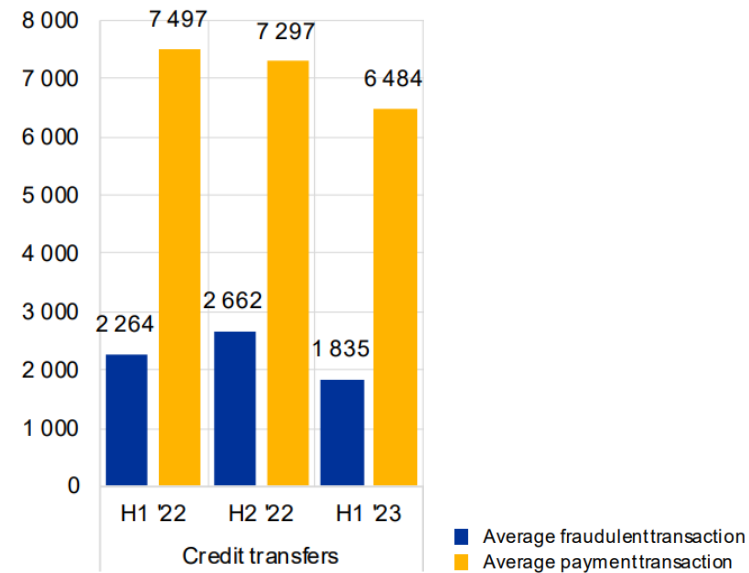
The **typical value** of a single fraudulent transaction is **relatively low**.

The frauds result both from payment **order counterfeiting** but also **payer manipulation**.

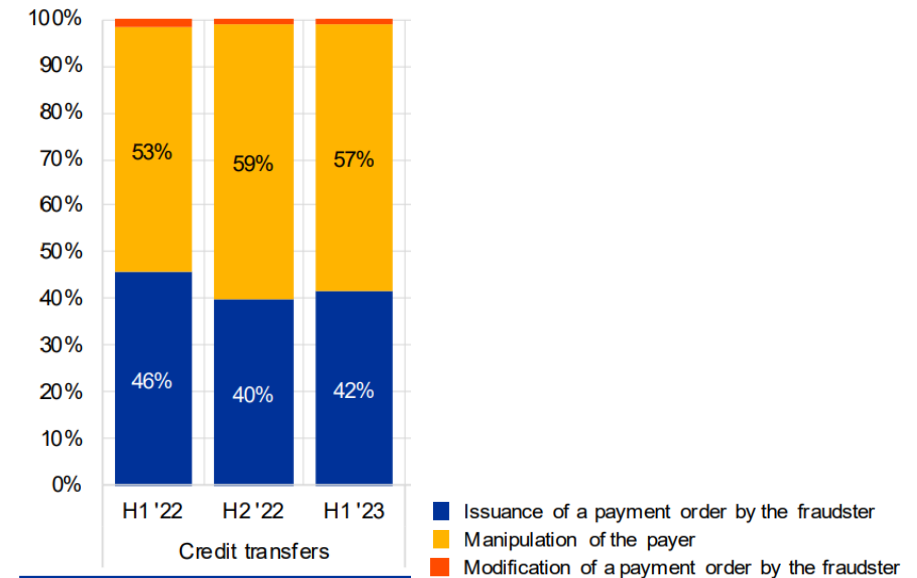
Total **value of reported losses** due to fraud by liability bearer (value of reported losses in million EUR)



Average value of a transaction and a **fraudulent transaction** (average value (EUR))

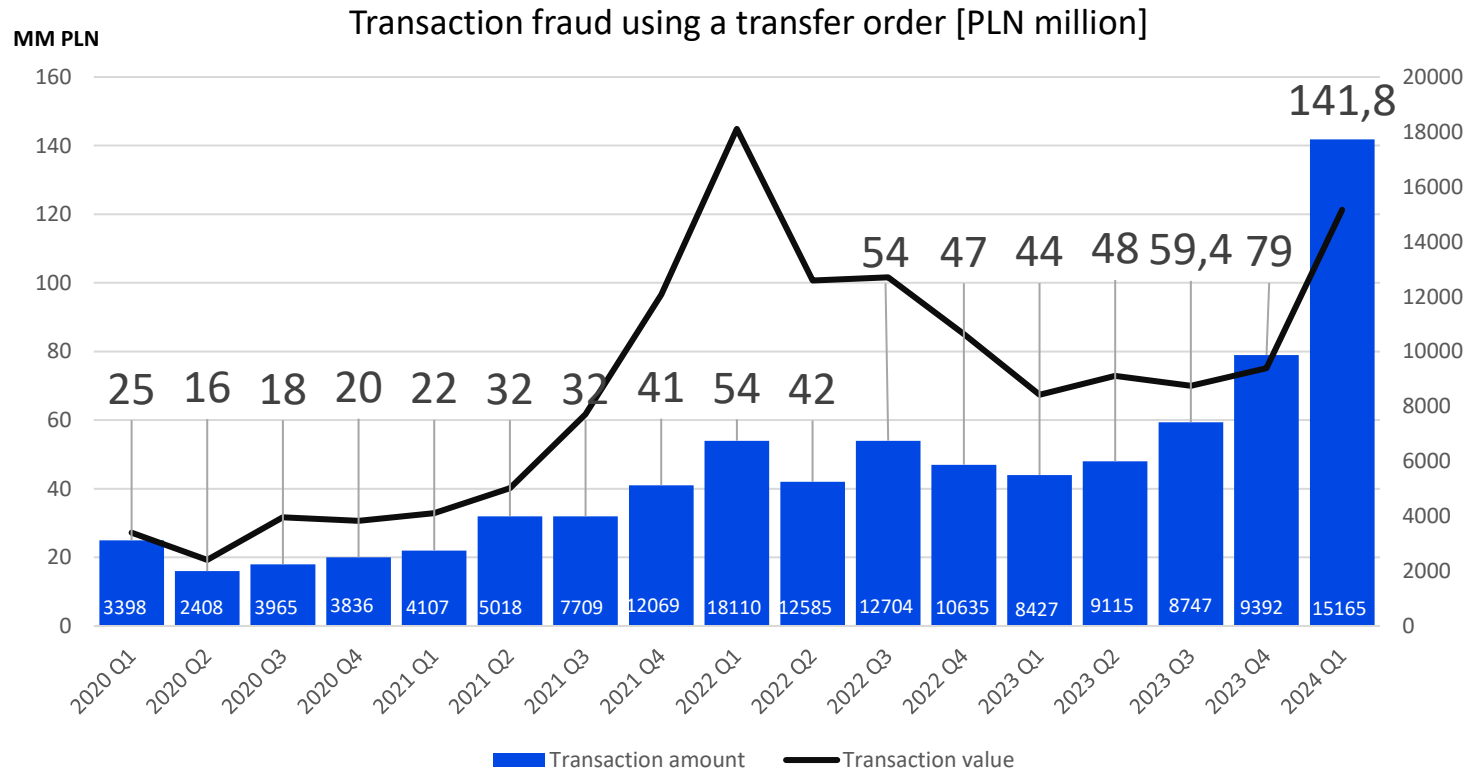


Value of fraudulent transactions by main fraud type in % of the total value of corresponding fraud



Source: 2024 Report On Payment Fraud, European Banking Authority & European Central Bank, August 2024. <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf>

Challenge in Poland



In Q1 2024 for the first time the banks reported the data on fraud resulting from the usage of social engineering. The method was employed against an account holder to manipulate the payment order.

Source: National Bank of Poland

Problem

- **Password theft** is a growing threat, with more than \$3 billion being stolen annually in this way.
- The **takeover of the banking session** is still possible despite the joint efforts of the entire sector.
- There is no perfect method to detect account takeover – **scammers are constantly developing** their methods.
- **Fighting fraud** is a tedious process even for the best-prepared organizations.



Phishing

Criminal groups are more and more often and more boldly pretend authentic transaction platforms of banks. Moreover, advanced phishing kits phish a one-time SMS code, and automatically add a trusted account to the victim's account.



Friendly Frauds

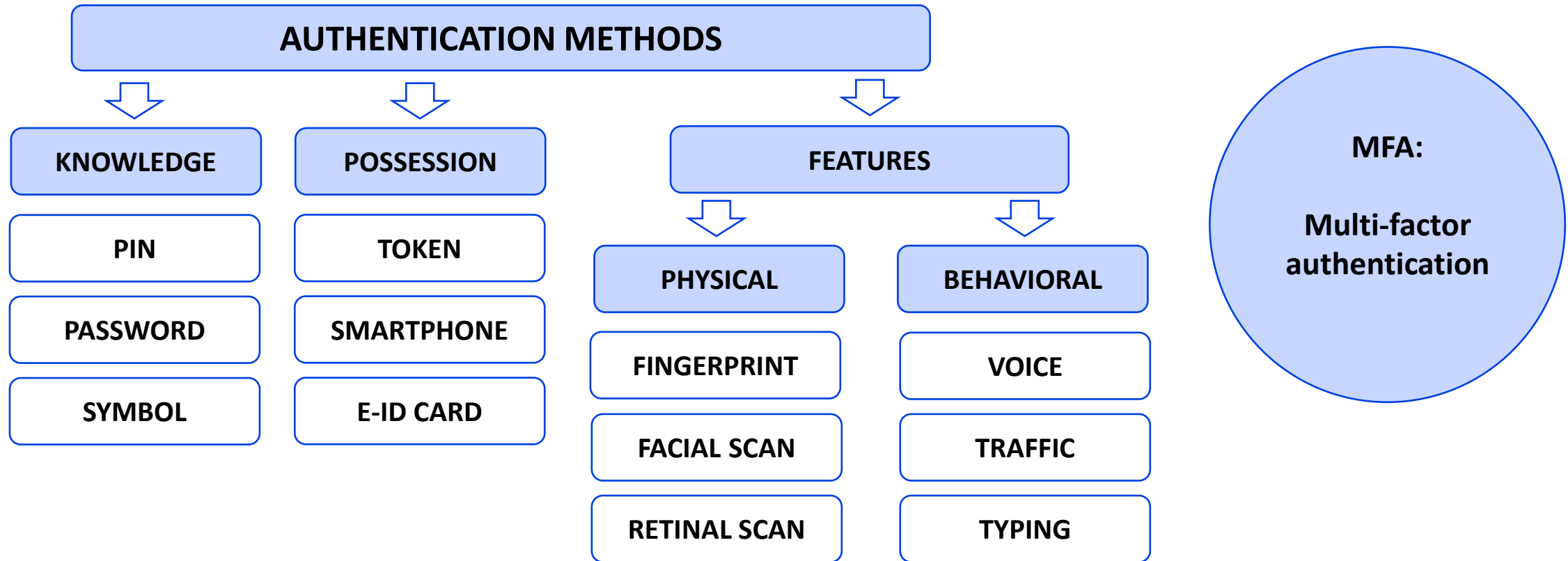
According to the requirements of PSD2, banks are obliged to return funds to the payer within 1 business day if an unauthorized transaction has occurred. This can lead to a situation where account owners start simulating unauthorized transactions in order to obtain compensation.



False investments

Based on the social media pages, the criminals persuade victims to install a remote desktop client – allegedly to make a profitable investment. Then the criminal withdraws funds from the victim's account, often additionally taking loans on their behalf.

Solution: Strong Customer Authentication



Payment Services Directive 2 (PSD2) obligates banks to have a strong verification of the customer's identity. Behavioural Analysis is recognised as a method of SCA by the European Banking Authority.

Biometric patterns = physical characteristics

Biometrics

Analysis of anatomical features:

- Fingerprint,
- Face scan,
- Retinal scan,
- A scan of the blood vessels of the hand.

Biometrics Properties

- Fingerprints repetitive as 1: 64 billion,
- Characteristics that do not change over time,
- Low-intrusive measurement,
- One-time verification,
- Replicable features.



Behavioural verification = behaviour analysis

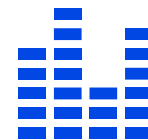
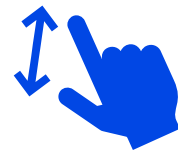
Behavioral analysis

Analysis of human behavior:

- Physical interaction with devices (e.g. smartphone),
- Voice profile,
- Gait.

Properties of Behavioural Verification

- Rarely repeatable features,
- Analysis possible in a continuous mode,
- Low-intrusive measurement,
- Uses standard devices (e.g. camera),
- Features stable over the years,
- Difficult to learn and replicate.



Behavioral analysis

A field that deals with **data analysis and discovery of patterns** in the behaviour of individuals.

Unlike classic biometrics, it **does not analyze physical human characteristics**, such as a fingerprint, a scan of the face or retina of the eye.

Fraud detection



Applications of behavioural analysis

- User identity verification
- Attack detection



After taking over the login and password to the account, the criminal logged into the victim's account. When a criminal tries to log in, the system detects other behaviour.

Example 1



The customer is tricked into a fake investment and installation of a remote desktop. When a criminal enters data for a transfer, the system alerts the Bank.

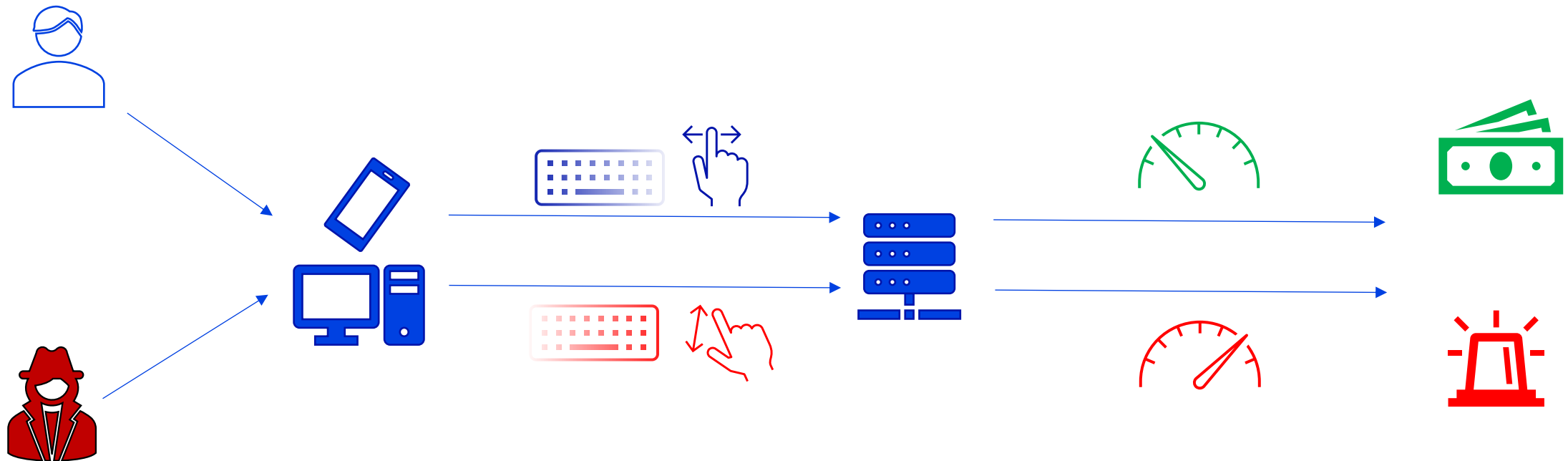
Example 2



The system detects a suspicious transaction. Behavioural analysis confirms that the transaction was entered by the account owner and silences the false alert.

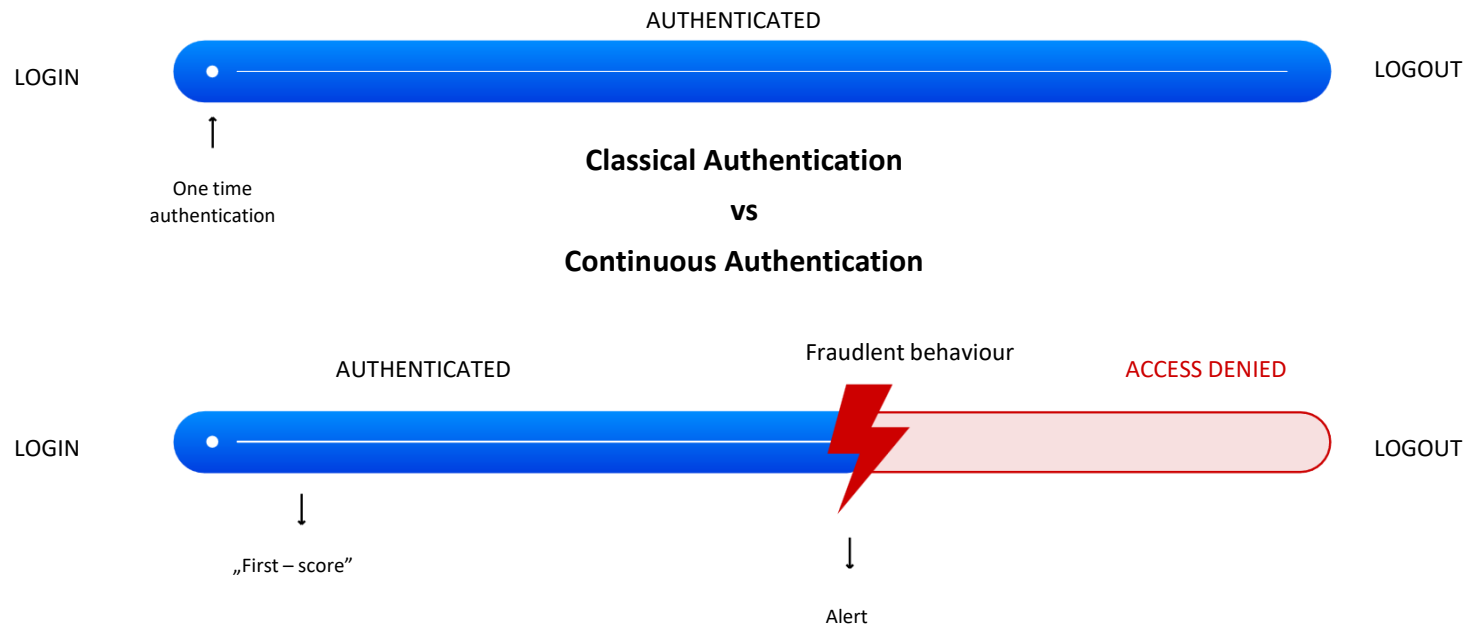
Example 3

How does behavioural verification work?



Continuous authentication

Continuous authentication protects you from the **moment you log in until the end** of your session. Thanks to this, we can **react before** the loss of funds occurs.



Case study

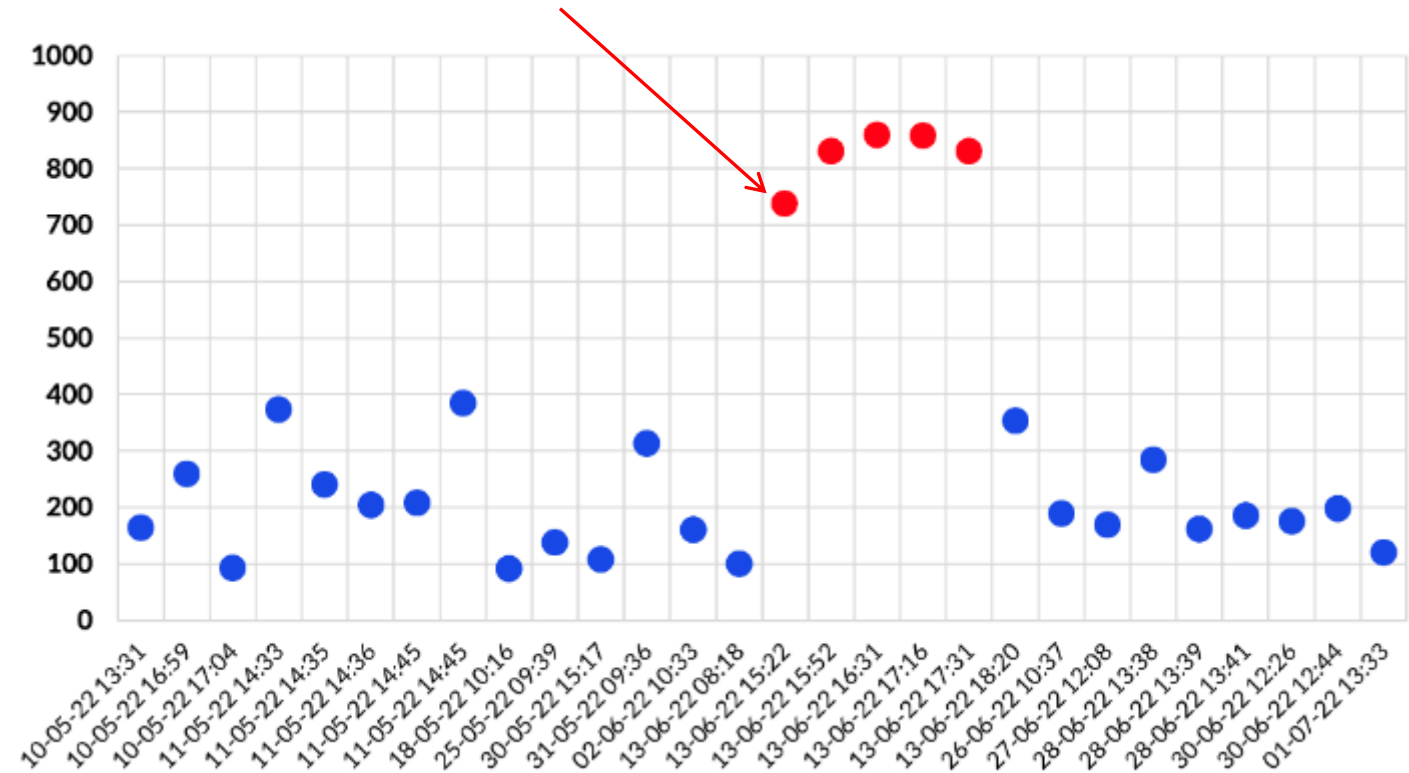
Phishing: Fake bank website

Session start: **score 737**
Fraudster login

In the following steps

The customer receives a link resembling a link to an e-commerce platform with a redirected payment page to a fake banking website - the login and password are stolen.

When a fraudster logs in, behavioural verification alerts the bank with the increased score.



Feature engineering

Which features are analysed?



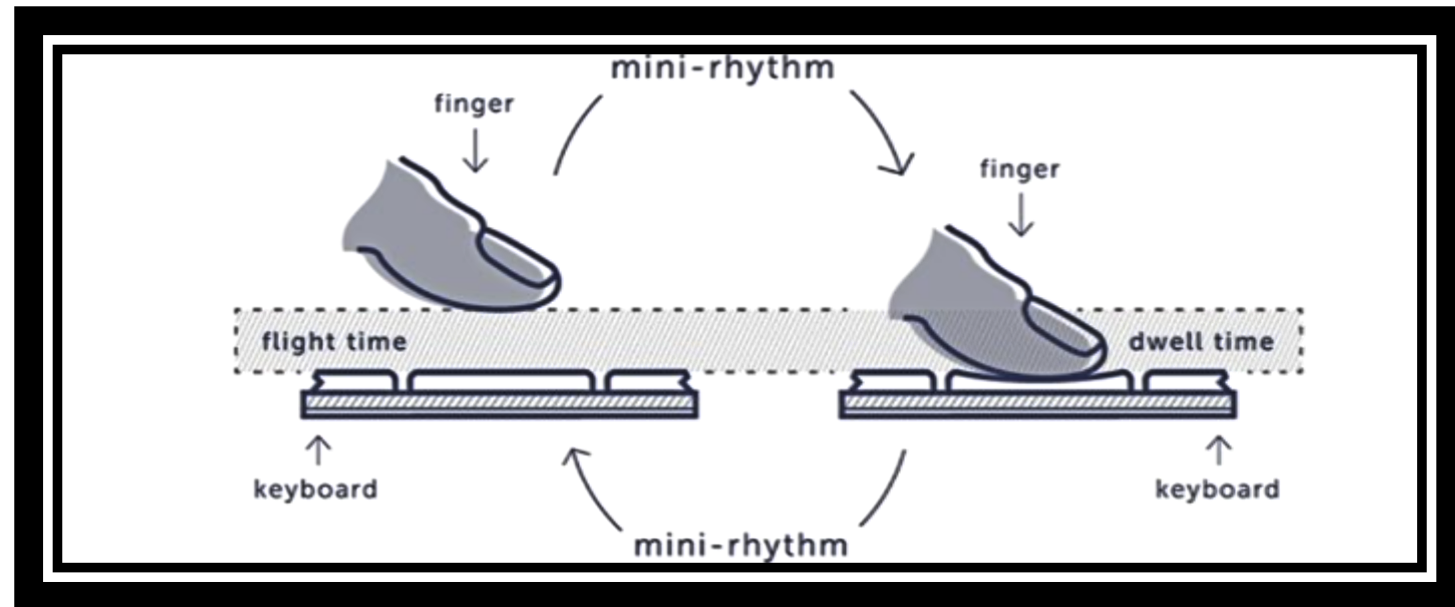
Data characteristics – keyboard

CTRL+C CTRL+V



INTERACTION TIME

KEY TYPE



Data characteristics - mouse



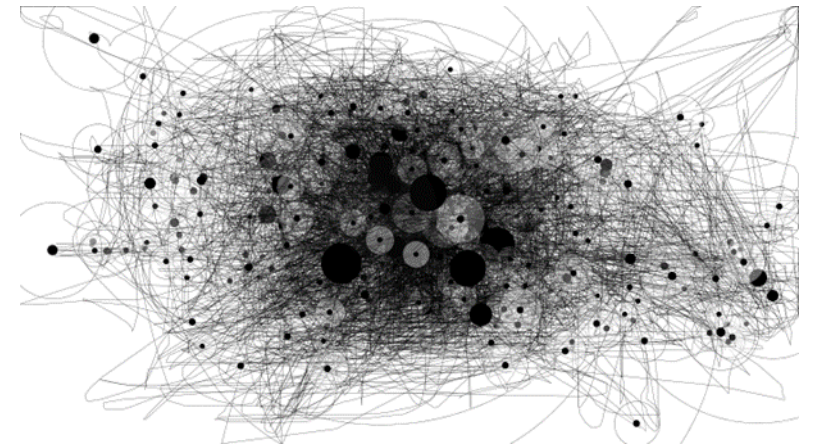
SPEED/ACCELERATION

ANGULAR VELOCITIES

TILT ANGLES

DISTANCE BETWEEN CLICKS

THE SHAPE OF THE MOVEMENT



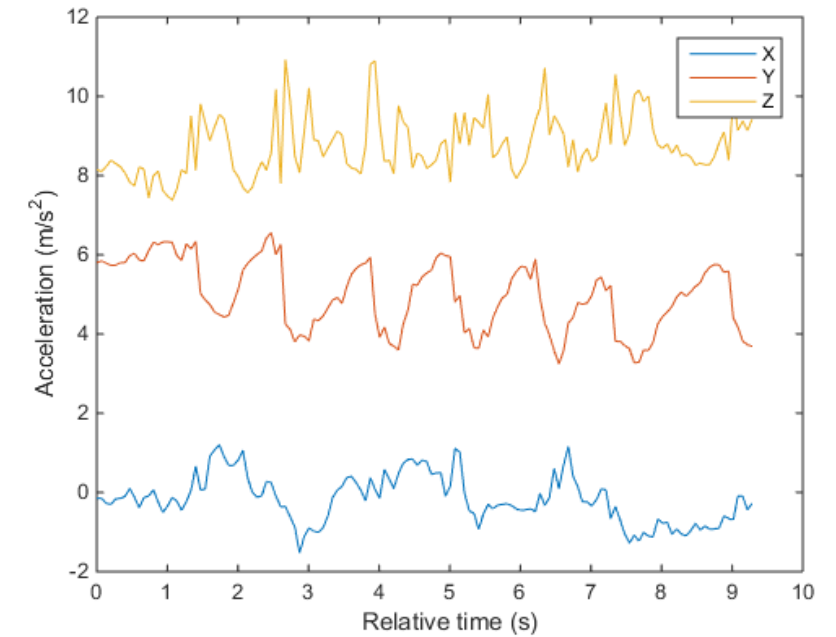
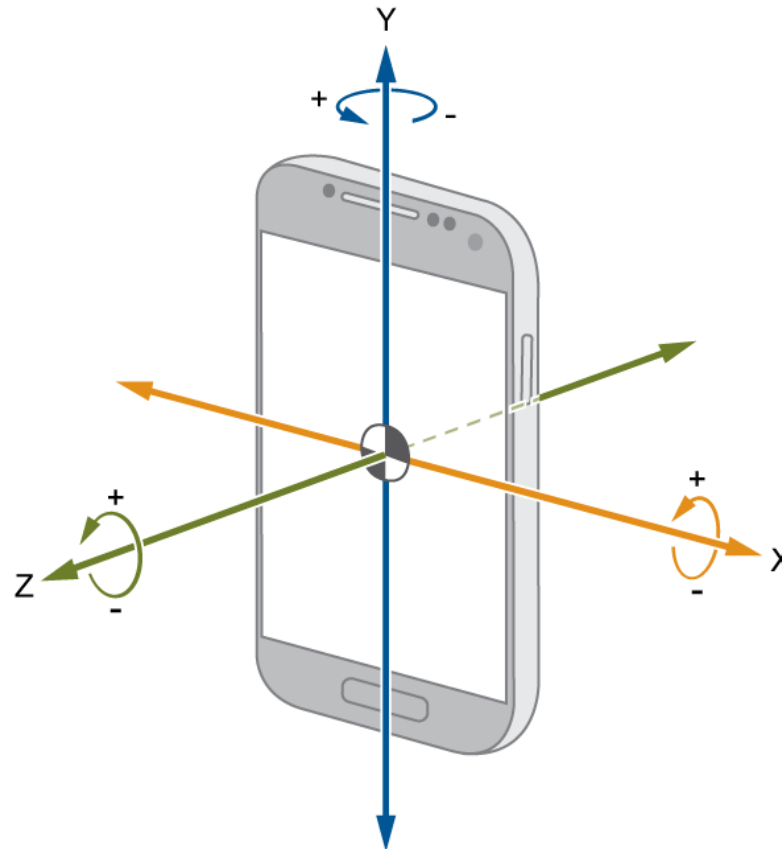
Data characteristics - smartphone



ACCELEROMETER

GYROSCOPE

PRESS TIME



https://www.mathworks.com/help/supportpkg/android/ref/simulinkandroidsupportpackage_galaxys4_gyroscopee0545c3dd6e0d54d37feccea60d134d9.png

https://blogs.mathworks.com/community/files/matlab_mobile_sensors_01.png

Behavioral models: population or individual ?



Fraudster or... Programmer?

Fraudster profile:

- Writes quickly,
- Reacts quickly, does not think long,
- Guides the mouse pointer precisely – knows the application,
- Uses keyboard shortcuts,
- Posses modern, reactive devices.

Approach 1

Let's build a model that includes a **profile of a scammer**.
 A model shared by the entire population, it assesses the level of similarity of the current user to the scammer

Challenge:

The model will alert in the case of the Programmer...

Approach 2

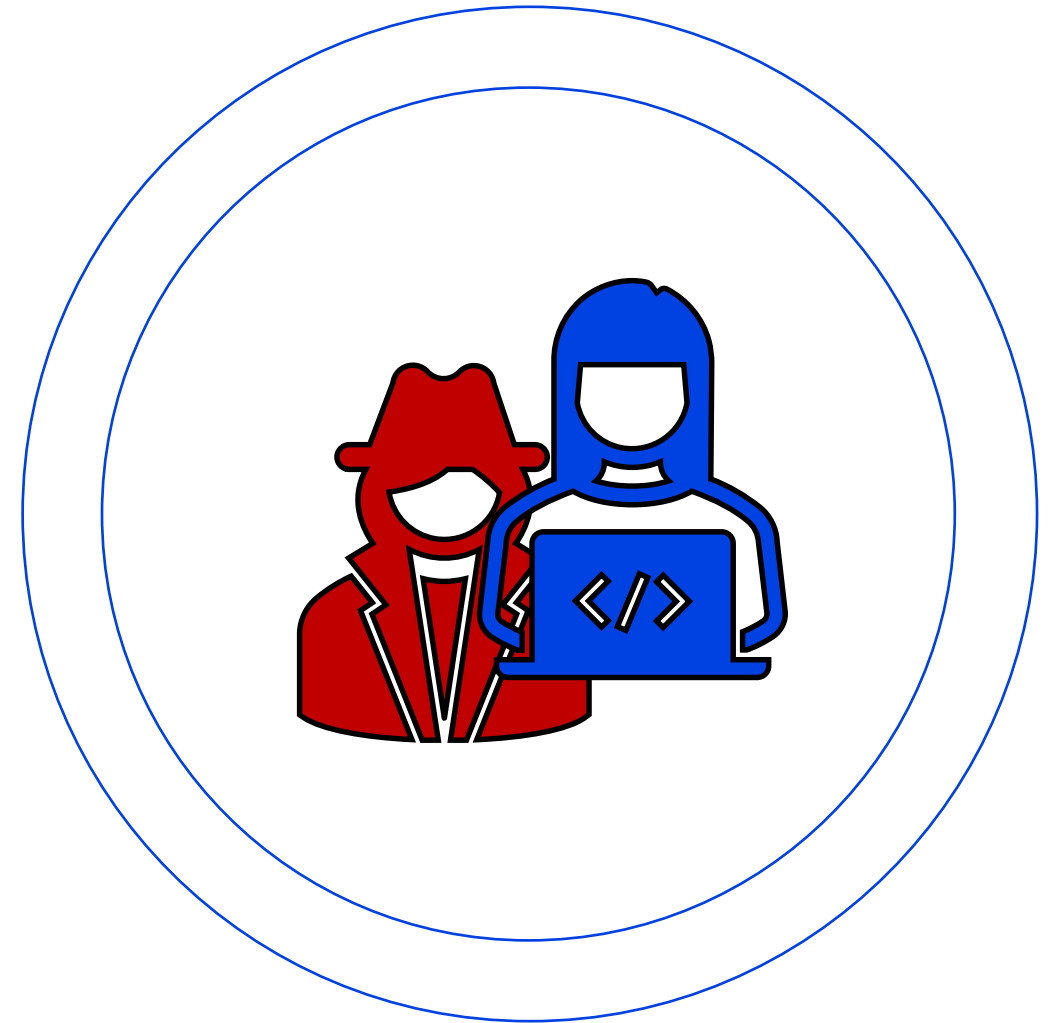
Let's build a model containing the **profile of the account owner**.

Individual model for the owner,

It evaluates the level of similarity of the current user to the owner.

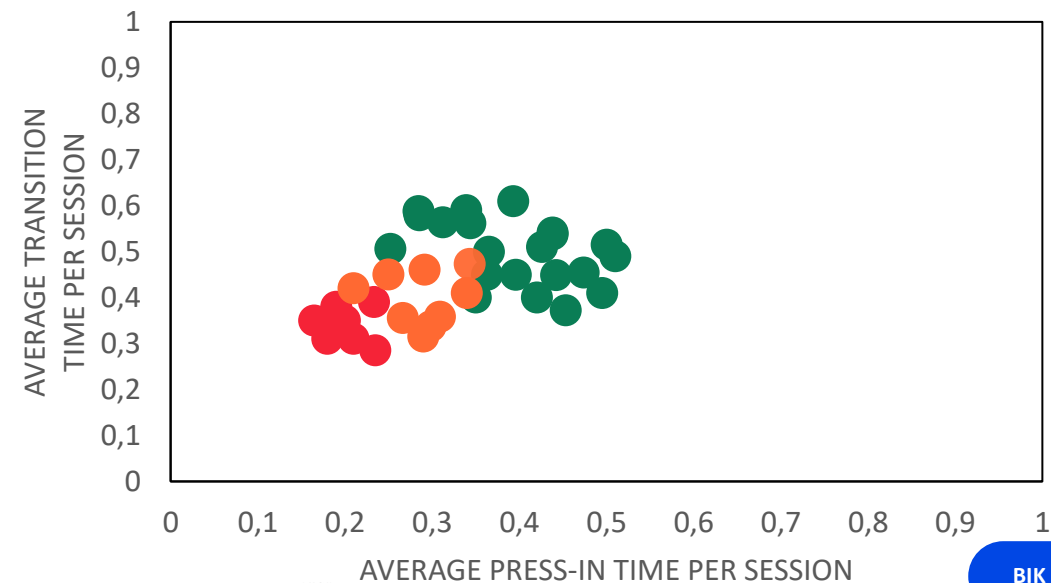
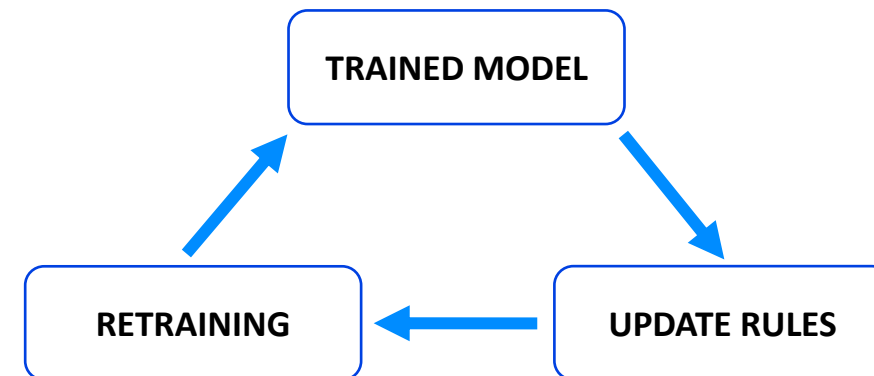
Challenge:

As many models as account owners. How to manage the system ...



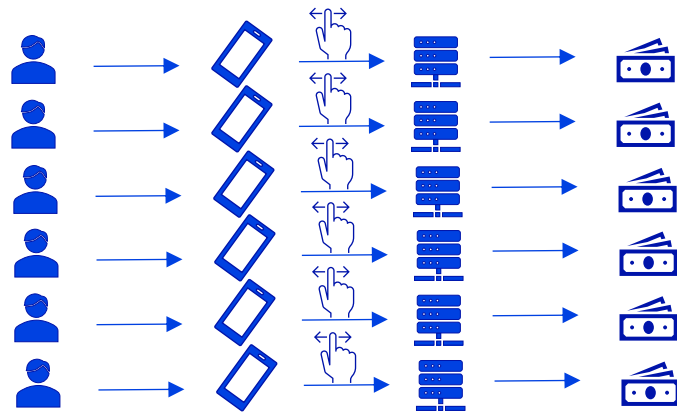
Individual model

- The first generated model can be built after 6-10 user sessions.
- The session must include actual interaction with the device, e.g. logging in from a password manager is not enough.
- Different devices provide different data sets
=> The customer can have several models.
- With the number of sessions, the models gain "power".
- The client changes behavior - data drift.
=> Model lifecycle management needed

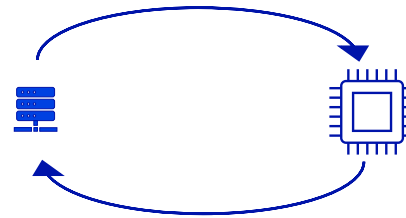


Model Factory

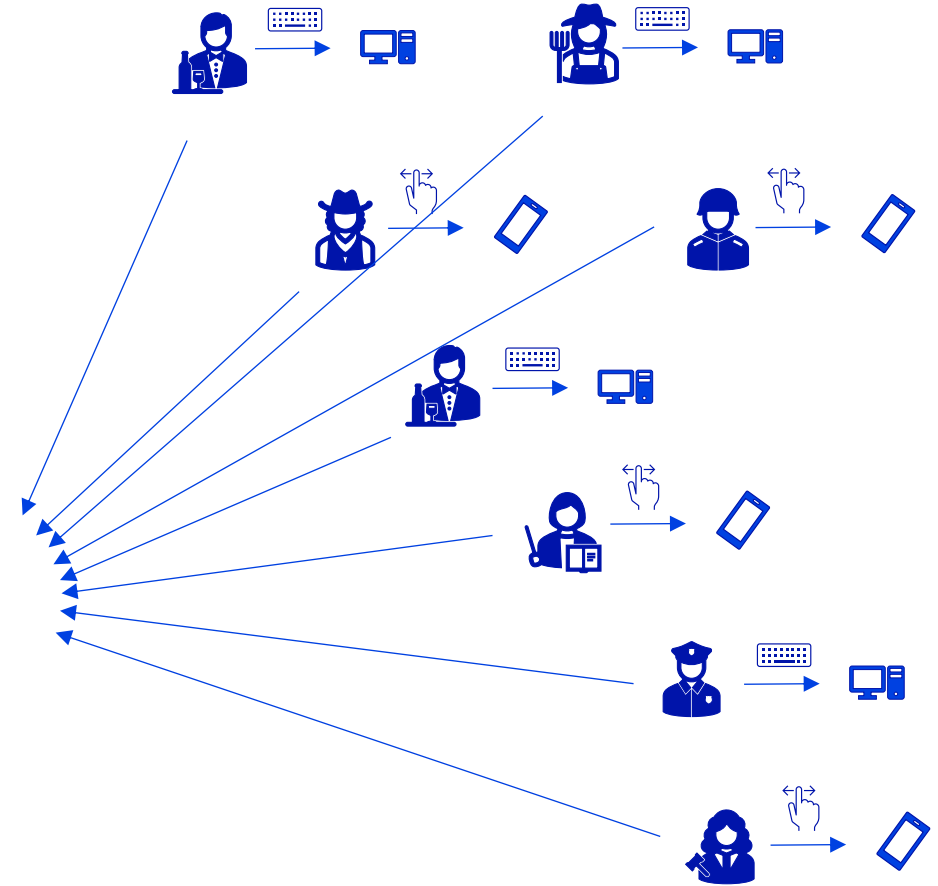
Data collection



Train the model



Session verification



Model Factory Management

- Data transfer from the Bank to the server should be limited
 - balance between process speed and size (value) of data.
- Models must be served quickly to bank by server
 - the balance between the speed of the process and the size (quality) of the model.
- Training models costs money
 - balance between the cost of teaching and the quality of production models.
- Management of the model queue:
 - service of new customers,
 - servicing customers for whom the profile has changed,
 - frequency of device usage.

Sectoral solution

Interbank model/data sharing

- The customer is at the heart of the sectoral solution,
- Behavioral features measured in a consistent manner,
- Behavioral profiles (models) built on shared data,
- Quick process of profiles building,
- Immediate implementation of new customer protection.





BIK GROUP

Summary

Behavioral Verification: Convenient, effective and GDPR-compliant



Behavior analysis seamless to the user.

The analysis refers to HOW the device is used, but DOES NOT explore the CONTENT.



Each user can have several personal models, who constantly adapt to his habits.

Sensitive data is NOT processed: identification, addresses, bank account, age, gender.



Identifying the fraudster before the transaction is completed - preventing losses before they happen.

Historical data about the user's INTERACTION with devices is used.

Thank you

Piotr Wojewnik, PhD

*Biuro Informacji Kredytowej S.A.
Digital Fingerprints S.A.*

piotr.wojewnik@bik.pl



BIK **BIG** **DFP**
InfoMonitor Digital Fingerprints
BIK GROUP

