BIK GROUP

Behavioural Verification

The best way to secure banking customers

Piotr Wojewnik, PhD

Data Science Director, BIK
Board Member, DFP

ACCIS Conference

Market Leader in Polish data ecosystem

BIK Platform **Anti-fraud**

Detects fraud related to **APPLICATIONS** for credit, credit cards, limits, as well as loans, leasing & factoring.
Based on present & historical application data & **fraud markups**.

- 39 Participants
- Savings: over 262 MM Euro (since 2017)

BIK Platform **Cyber-Fraud Detection**

Comprehensive tool for protecting the online channel and exchange of data on **COMPROMISED DEVICES** between participants .
Devices identified by parameters **determined passively** & **actively**.

- 34 participants
- 4,5 MM events analysed per month

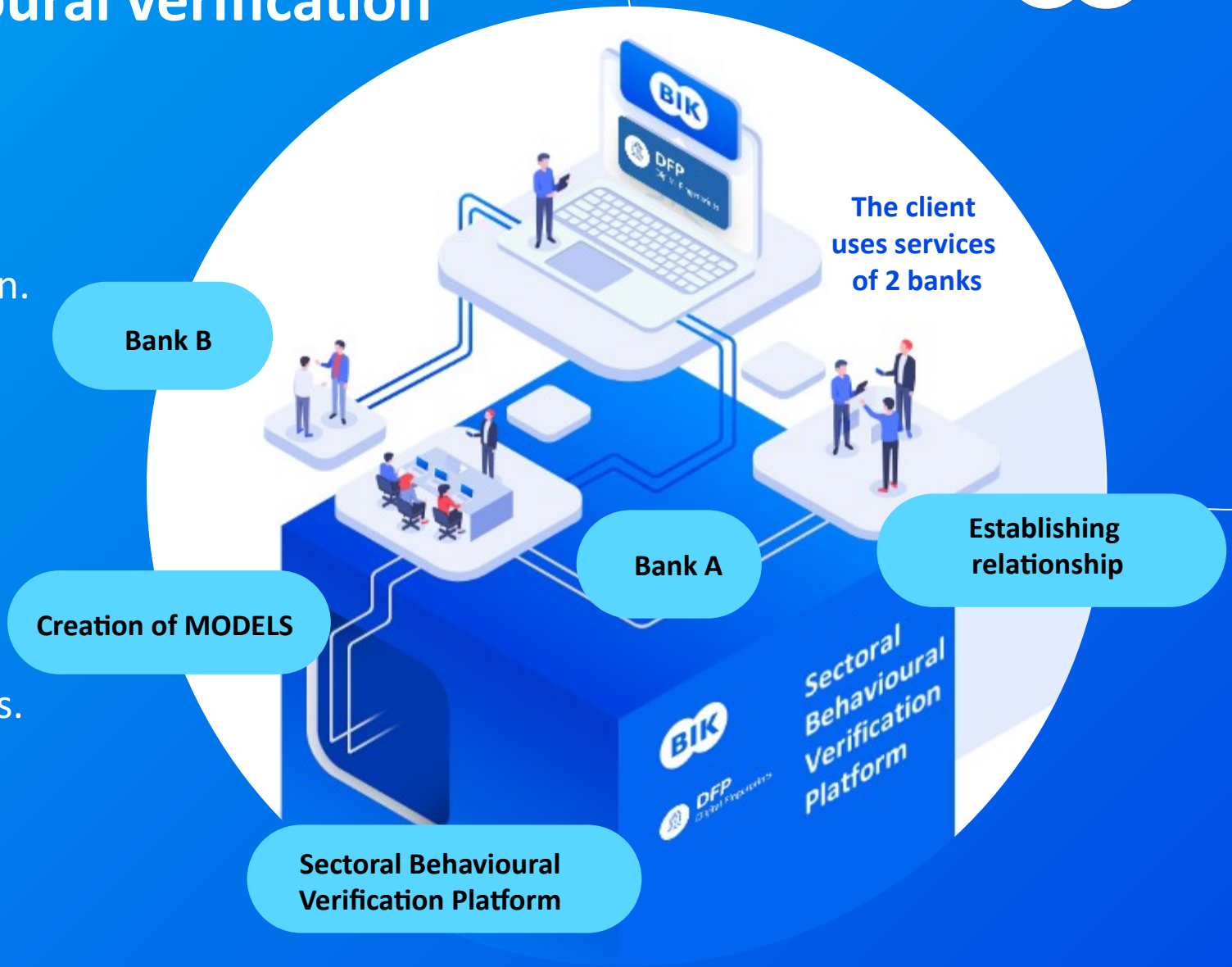
BIK Platform **Behavioural Verification**

Anomaly detection based on **USER-DEVICE INTERACTIONS**.
Enables real-time fraud identificaiton and reaction of the financial institution still **during transaction**.

- *8 Participants , 1 software integrator*
- *over 6 MM customers*

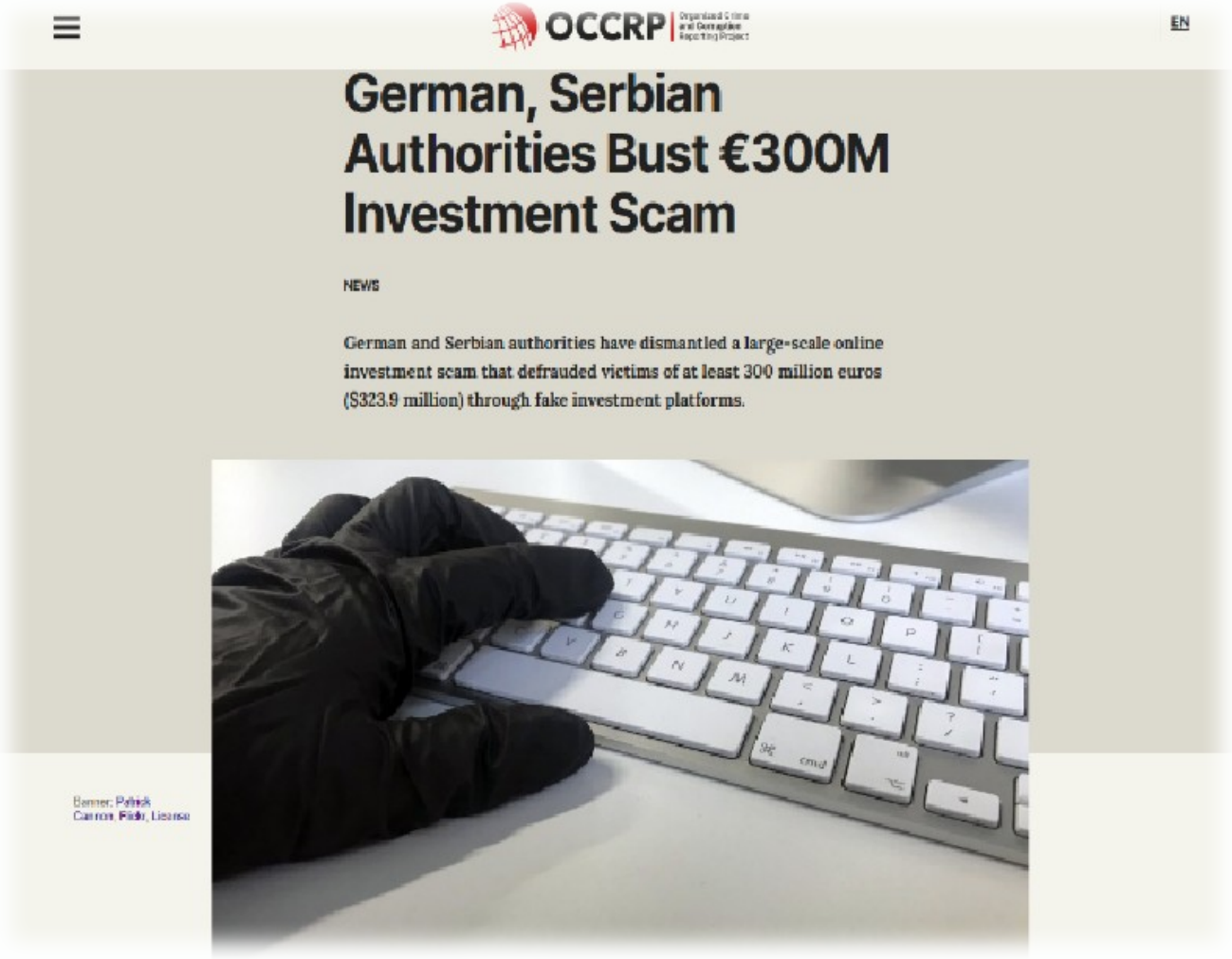
Benefits of sectoral behavioural verification

- The customer at the heart of the solution.
- Fast & CONSISTENT assessment of customer behaviour.
- MODELS co-creation & sharing.
- No DATA exchange between banks.
- Immediate protection of NEW customers.



Fraud –
Challenge to banks and customers

Popular fraud scenario – false investment



Scenario

- **Designed websites** promissed high returns on investments.
- Little or no return observed.
- Victims' personal data and bank account details used to create **fake customer accounts** & lending creditworthiness.

Status

- First complaints in June 2020. Investigation by Dresden Prosecution & Chemnitz Police.
- Ca. **120 victims** have been identified **in Germany** alone, with losses estimated at **EUR 12M**.
- Mastermind arrested in Cyprus. Authorities searched 22 locations across Cyprus and Serbia, seizing computers, hard drives & mobiles.
- **Eurojust** (European Union Agency for Criminal Justice Cooperation): the victims worldwide ca at **EUR 0,5B**.

German, Serbian Authorities Bust €300M Investment Scam | OCCRP

Most popular fraud scenarios in Europe

Online Shopping Fraud

ID Theft
(BankID)

Phishing
(Gaming/Streaming accounts hijacking to get access to financial data)

Smishing/Phishing
(public services providers)

House rental
(not existing/
already booked houses)

Vishing
(police officer scam)

Job offers
(false initial training / hardware payments)

Smishing
(false SMS about tickets)

Phishing
(overdue payments)

Loan/Leasing/Invoicing Fraud

Easy Money
(crypto, false investments)

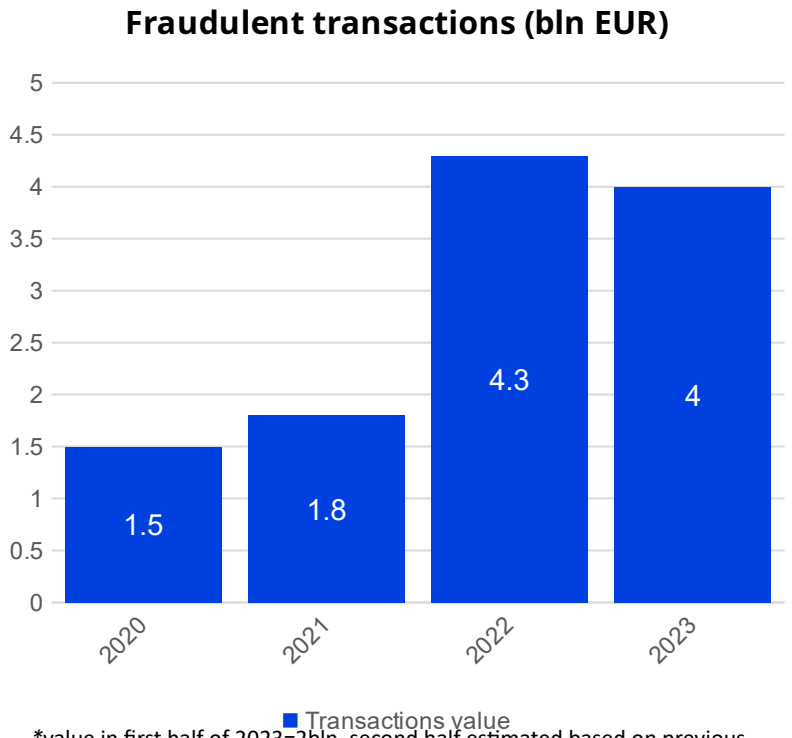
Fake charities

Government subsidies
(false assistant witch proceeding subsidies)

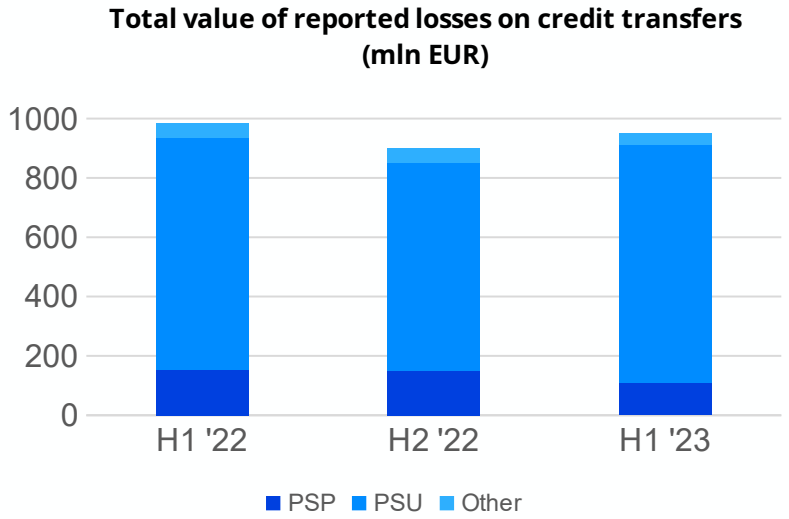
Social network
(false assistance with digital wallets)

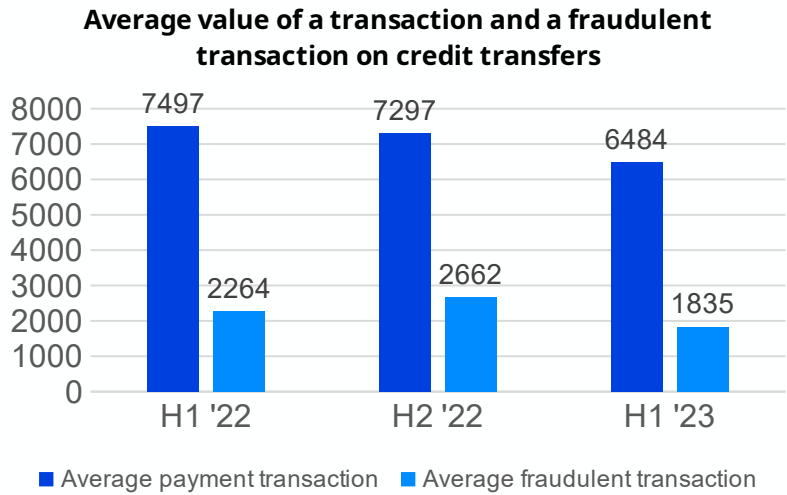
Love Story
(pretending to be someone else)

Challenges in Europe (EEA) - key figures



*value in first half of 2023=2bln, second half estimated based on previous years





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

Behavioural verification by BIK/DFP –

Key features and benefits

Solution: Behavioural Verification

Each individual has a **unique way of interacting** with device: typing, navigation with the mouse or touchpad, and usage of smartphone.

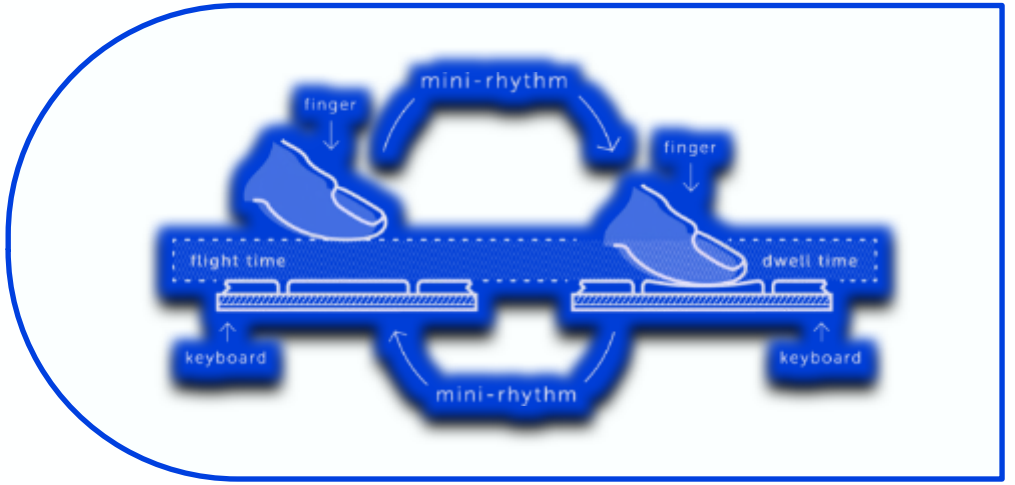
This diversity can be attributed to various factors such as our **muscle memory** or the **anatomy** of our hands.

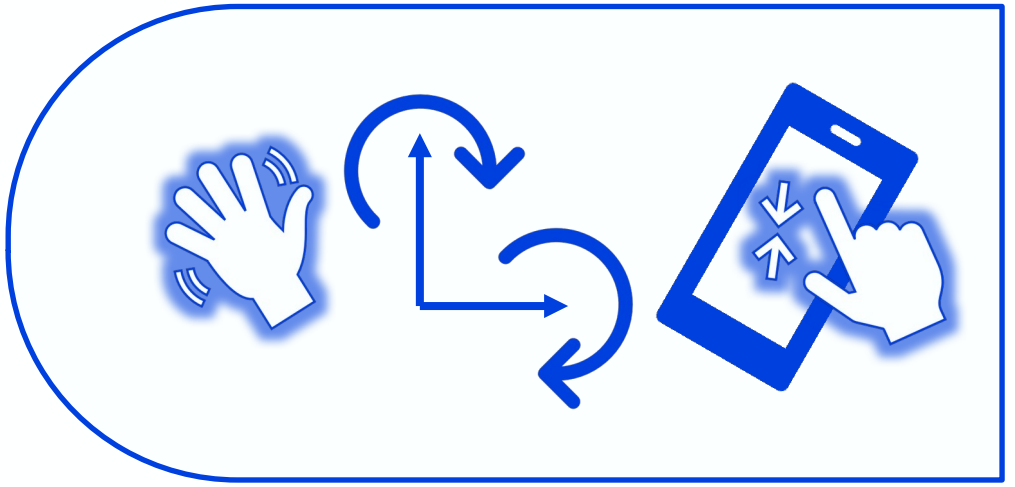
Behavioural verification is an approach:

- to study these unique patterns of behaviour and
- to establishe a **behavioural profile – MODEL unique** to each individual.

Behavioural Verification is recognized as a method of **Strong Customer Authorization** by the *European Banking Authority.*

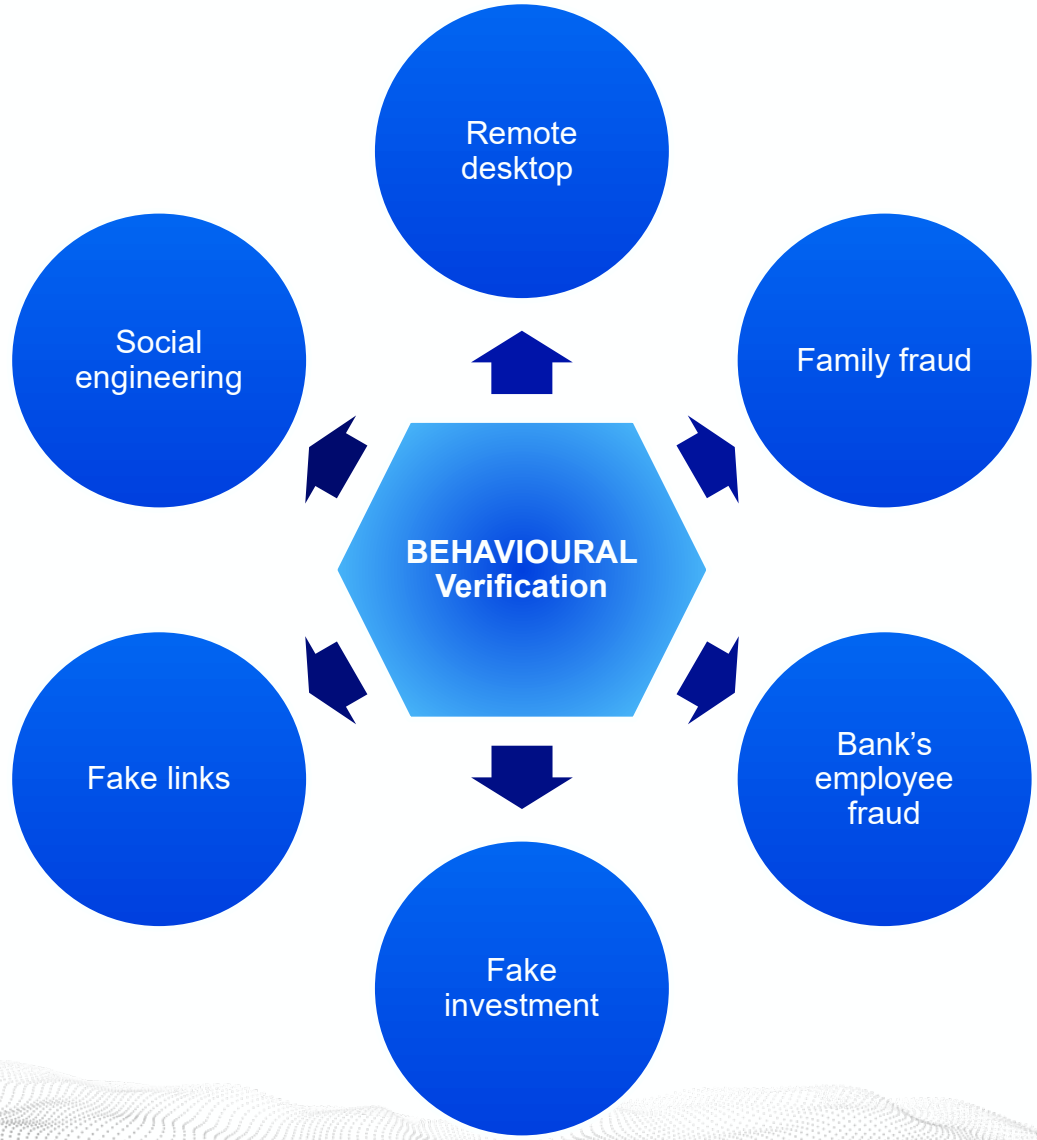
Question ID: 2020_5620 to Legal act: Directive 2015/2366/EU (PSD2)
2020_5620 Use of behavioural data for SCA | European Banking Authority





*…"The EBA gave examples of factors which constitute inherence, including fingerprint and face scanning, **keystroke dynamics** and the **angle at which a user holds the device**, adding that these **could be used to authenticate PSUs** provided the implemented approaches have a 'very low probability of an unauthorised party being authenticated as the payer'…"*

Fraud Types identified by Behavioural Verification – feedback from BIK platform Users



CASE 1

Hijacking the login and password to the account

#1 During login, the system detects an anomaly in the user's behavior and alerts the bank.

CASE 2

Remote desktop

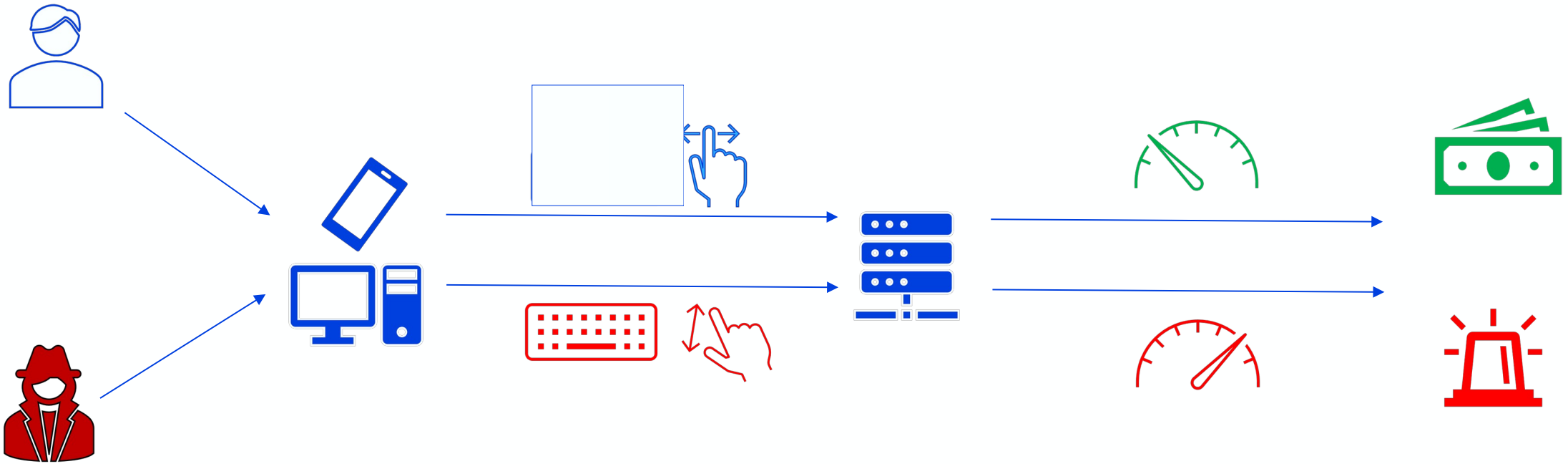
#1 - During the session, the user is asked to install remote desktop.
#2 The fraudster takes over the session.
#3 The system detects an anomaly in the user's behavior and alerts the bank.

CASE 3

Reducing alerts

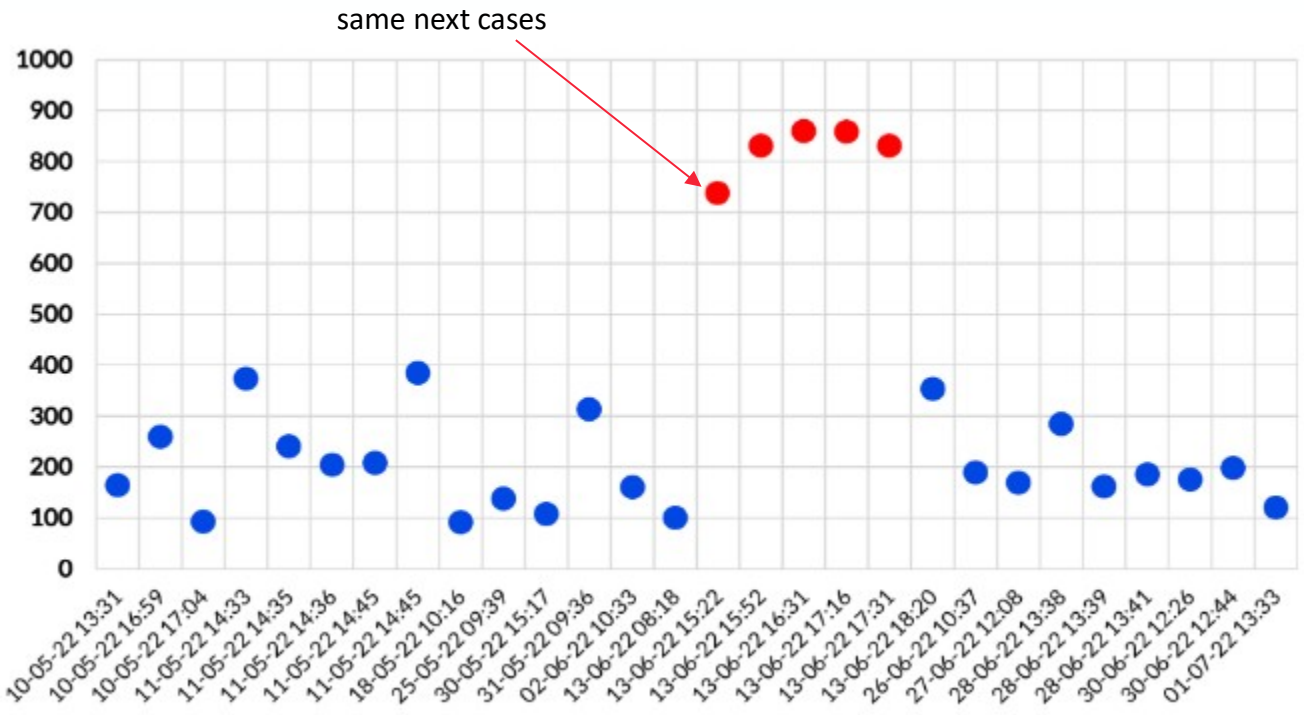
#1 The system identifies authorized and unauthorized user sessions by comparing behavioral patterns.
#2 The system determines whether a session exhibits signs of fraud.
#3 The system minimizes false alerts.

How does Behavioural Verification work?



Behavioural Verification Platform case study

Phishing: **Fake bank website**



The customer receives a link looks like link to e-commerce platform with payment redirected to a fake bank website - the login and password are stolen.

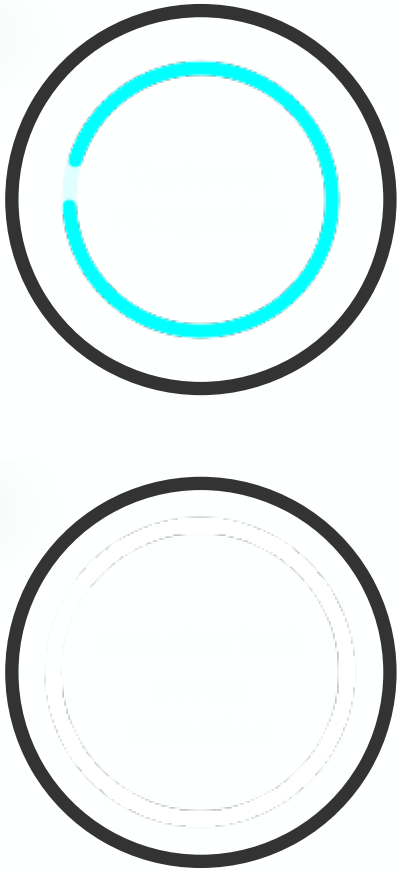
When criminals log in, the Behavioural Verification system alerts them to an increased score.

Can Behavioural Verification fix fraud?

We collect user behaviour unnoticed
Behavioural Verification works in browser and mobile (IOS and Android) without impacting the user.

We learn user behaviour
Each user has more than one personal model being constantly updated according to his/her habits.

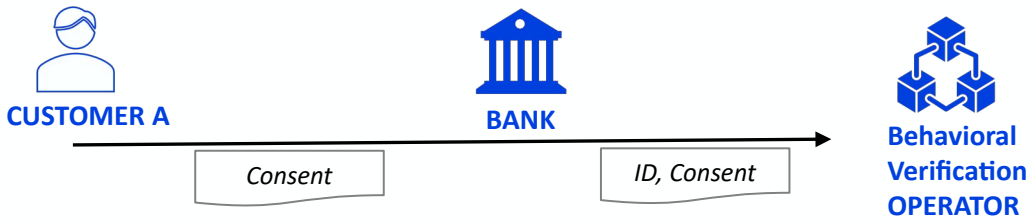
We react in real time
If the behaviour is inconsistent with the model,
we notify bank via a PUSH message.



Data transferred under Behavioural Verification

Data collection

Consent collection process



- Consent collection

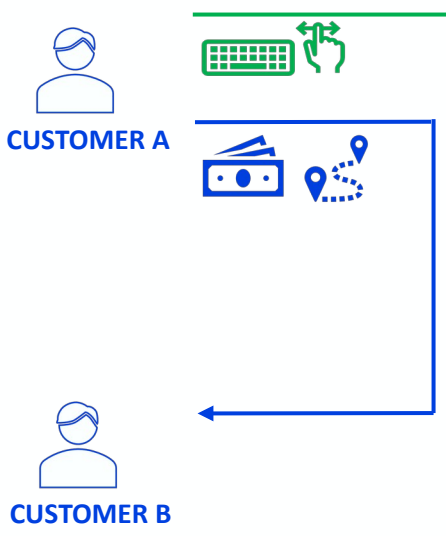
Model building process

- Consent verification
- Behavioural data collection
- Model Building

Data transferred under Behavioural Verification

Client verification – stand-alone version

Bank transfer

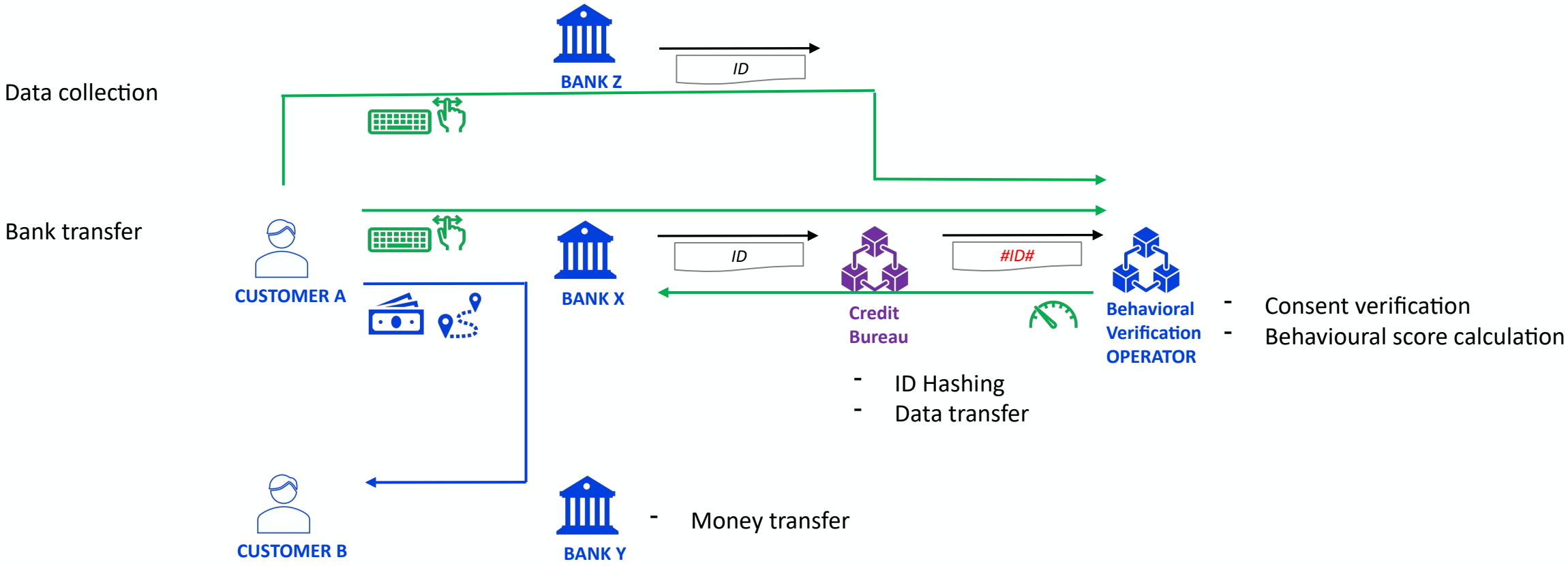


- Consent verification
- Behavioural score calculation

- Money transfer

Data transferred under Behavioural Verification

Client verification – sectoral version



Local Credit Bureau as a Country Operator of behavioural verification

BENEFITS FOR CREDIT BURAEU

- Own Branding – BIK solution as a **white label**
- Extended offering to the banks
- Increased loyalty

Product

- **Modern**, verified technology
- Continous R&D by BIK
- SaaS – complementary to running soultions

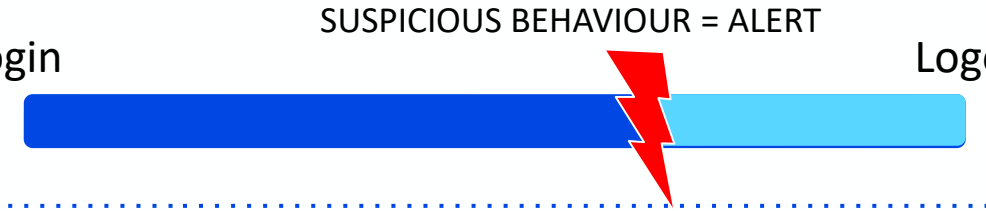
Technology

- **No upfront** payment
- Attractive, degressive pricing
- Revenue share model

Revenue

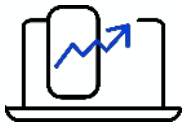
Behavioural Verification Platform overview

CONTINUOUS ANTENTHICATION



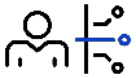
PROCESS **POWERED BY AI**

MULTI DEVICE



INDIVIDUAL BUILD-UP

SECTORAL REPOSITORY



BIK Behavioural Verification Platform

- Behavioural **profiles shared** between sectoral participants
- **AntiFraud Council** (BIK + Users): establishes standards; initiative & opinion to new legal acts; experience sharing
- **Anonymised** behaviour: **no personal/ no context data**, no logging text
- **Machine Learning** embedded, custom models for individuals, models re-trained automatically
- **Subject experts** support onboarding, adjust algorithms based on feedback
- CSR & Edu: **alerts to customers**; media campaigns

USERS of BIK Behavioural Verification Platform

Emerging Standard in Polish market (6 of TOP 10 Banks)

PKO Bank Polski
11,5M pers.

PL TOP3
6,8M pers.

ING
4,6M pers.

mBank
5,7M pers.

BNP PARIBAS
4,0M pers.

VELO BANK
1,0M pers.

KASA STEFCZYKA
Zawsze u siebie
0,9M pers.

Bank Pocztowy
0,7M pers.

NOVUM
Cooperative Banks

Key success factors of fraud prevention schemes

01.

TECHNOLOGY

Top class technology solutions

02.

SECTORAL

Centralised data architecture

03.

CROSS PLATFORM CONVERGENCE

Maximise efficiency by x-platform and x-sector alerting

„To go fast, go alone.

To go far, go together.”

African proverb

BIK BIG InfoMonitor DFP Digital Fingerprints

BIK GROUP

Piotr Wojewnik PhD

Data Science Director, BIK
Board Member, DFP

piotr.wojewnik@bik.pl
linkedin.com/in/piotr-wojewnik