Momentum Solutions S.A.

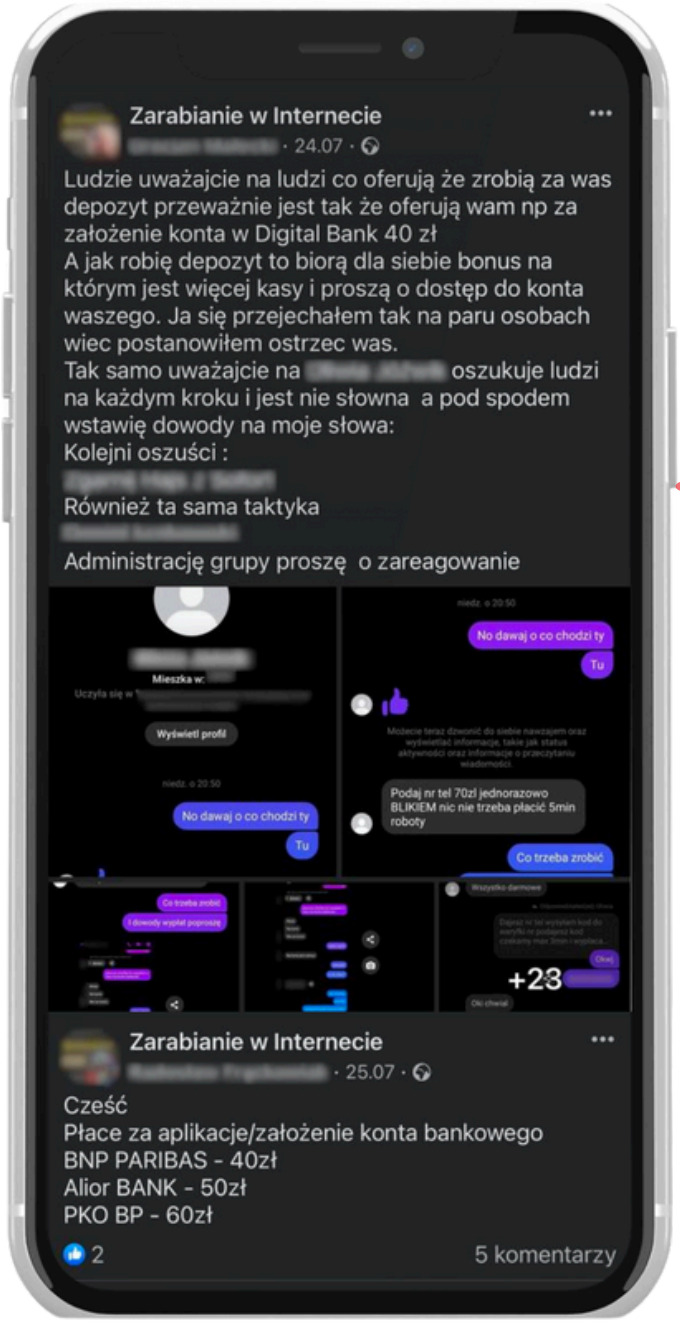
KAIROS™ FRAUD DETECTOR

Decision Support System in the Area of Web Service Access Security

Momentum Solutions S.A.

momentumsolutions.pl

Uncontrolled trading of bank accounts - use case



On the Internet - especially on social media platforms - there is an increasing trend of illegal trading in bank accounts. The same practice applies to the accounts of entities operating payment accounts under MIP or KIP licenses.

Example of the problem:

Bank accounts (both private and corporate) "without debt seizure" can be purchased for as little as 5 Euros!

Why are bank accounts traded?

1. **Fraudulent acquisition of bank bonuses**

   Banks offer a bonus for opening an account online or through a courier. The "account sellers" capture these bonuses, leading to a suboptimal allocation of marketing funds by the bank. In extreme cases, this may result in disabling the online account opening option during an active campaign.

2. **Legalization of illicit funds**

   A "purchased" account facilitates the legitimization of illegally obtained funds, which violates AML procedures and exposes banks to liability.

3. **Cryptocurrency transactions**

   The anonymity of cryptocurrency transactions, combined with the use of someone else's account, is used to obscure the origin of funds and circumvent regulations.

4. **Identity Verification**

   Some individuals use "purchased" accounts to exploit someone else's data and obtain a seemingly valid identity verification.

5. **Financial fraud**

   Loans, credits, and fraudulent sales on e-commerce platforms (Allegro, OLX) - such operations are easier when using an account that isn't your own but a purchased one.

Conclusions from the analysis of the banking system's resilience to fraud

Based on the conducted research, the following conclusions emerge:

•Lack of Ability to Determine the Ultimate Beneficiary

Customers knowingly share their login credentials, which results in the bank being unable to determine who is actually using the account.

•AML Procedures vs. the Scale of the Phenomenon

Due to the magnitude of the issue, current AML procedures prove insufficient. Fraudsters can easily bypass standard safeguards.

•Risk of Losses That Are Difficult to Estimate

Banks may incur significant financial and reputational losses due to such abuses.

•The Importance of Detecting Fraud at an Early Stage

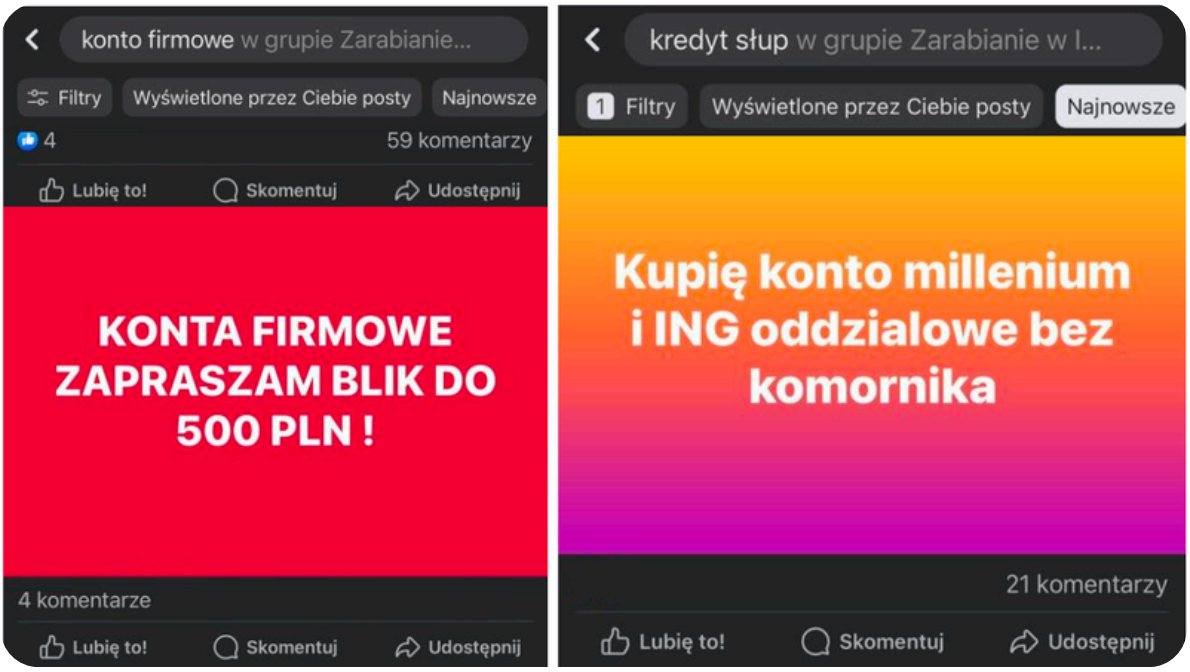
It is crucial to recognize that fraud has begun at its inception, in order to immediately block further operations and prevent losses.

Source of Data:

Dozens of public Facebook groups (including "Zarabianie w Internecie"), each with membership ranging from a dozen to several tens of thousands. Analysts at Momentum Solutions S.A. have identified a range of diverse characteristics of these frauds, enabling their categorization and precise identification in banking systems.

Lack of effective preventive tools.

Trading in login credentials for banking applications is conducted on a massive scale, and there are currently no technological solutions available to prevent such activities. Existing systems do not provide a means of stopping the described fraud because it relies on genuine data and the voluntary sharing of login credentials.



This phenomenon particularly affects accounts opened via mobile applications, such as “selfie” accounts. One of the fraud schemes, in a simplified form, can be described as follows: the person selling the account opens it using a mobile application, providing their real personal details but using a phone number and email address that belong to the “fraudster.” After successful identity verification and logging into the application, the seller hands over the login credentials in exchange for an agreed-upon payment. The person purchasing the account then logs in on their own mobile device, changes the password, and takes control of the bank account for the purposes described in this document.

Kairos Fraud Detector – an Advanced Decision Support System

Kairos Fraud Detector is a decision support system based on an analytical engine developed using a Big Data architecture, featuring stream analysis components—analyzing data in real time as it arrives—and algorithms that embed knowledge about fraud activity models.

The architecture of the Kairos System allows for the real-time identification of potential violation events—within milliseconds of receiving an incoming event. This means that Kairos can detect fraud ex-ante, i.e., before it is committed, enabling the system to block fraudulent activity before it occurs.

The system was developed based on the years of expertise of a team of programmers and analysts who create IT tools to combat organized crime, as well as on experience from advanced fraud systems related to scams in the transportation of excisable goods and goods of special value or significance.

Real-time fraud detection based on a multi-criteria analysis of user behavior. The data is analyzed using data quality algorithms—assessing the quality of information originating from various types of mobile devices, which enables the correct classification of the circumstances affecting the accurate identification of a fraud event. The application of multi-criteria analytics includes, among other factors, data about the user's device, its operating parameters, and its environment. It utilizes advanced algorithms that examine the sequence and dynamics of detected changes in application performance attributes. The detection of so-called breach clusters is achieved through correlation analysis and clustering of user behavior patterns. The entire process concludes with the assignment of an event classification, in accordance with the KAIROS_FRAUD_STAMP methodology.

In addition to integration with an anomaly detection module and ex-ante fraud event logic, the system also features an ex-post analysis module for defining new functionalities and algorithms utilizing machine learning.

Our experience

A team with implementation experience in Big Data based on stream processing with real-time analytics in critical infrastructure systems. Our experience includes creating systems for processing streaming data acquired, among others, from smartphone-class mobile devices. Thanks to our involvement in co-developing mobile applications that transmit telematics data, we possess extensive knowledge regarding the imperfections of various hardware classes available on the market and methods for optimizing the occurrence of anomalies in data sent by these devices at the software level.

Innovation

• Event analytics in the "incoming stream"

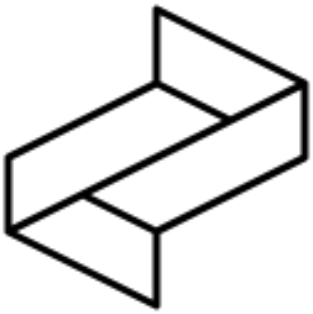
• System reaction time to the detection of a violation/anomaly at the millisecond level, enabling real-time fraud detection and, consequently, the prevention of fraud before it occurs.

Effectiveness

Issuing alerts or control directives to the service provider's systems on suspicion of fraud before it occurs.

Continuous Development

- Identification of fraud patterns and continuous development of algorithms.
- The ability to implement changes without affecting the continuity of the main data stream processing.
- High availability and system flexibility in terms of integration with service provider systems.



About us

Momentum Solutions S.A. is a technology company specializing in fraud prevention systems. We offer products such as Kairos Fraud Detector for the financial industry and Kairos Inspector for the transportation sector.

We also modernize critical infrastructure systems for the Polish Ministry of Finance.

Our team co-developed one of Europe's largest anti-fraud systems – the Ministry of Finance's critical infrastructure system used for monitoring goods of special significance.

We serve entities operating within the framework of the Polish National Health Fund by providing a platform that automates the process of managing coordinated care.

We are also developing an innovative passporting and recycling process management system, as well as a system for automating the bidding process in the construction industry.

[Stay in touch]

Momentum Solutions S.A.

TOMASZ ZYGMAŃSKI
CEO

+48 601 888 007
biuro@momentumsolutions.pl

WWW.MOMENTUMSOLUTIONS.PL