

MK Gaming LLC

Company No. 402321411

Address: Georgia, Tbilisi City, Didube District, Uznadze Street, №111, Building №2, Apartment №11

To: **Whom it may concern**

From: **Bohdan Podilchuk**
Director of MK Gaming LLC
No. 402321411, registered in Georgia
at Uzhadze 11, No. 2, ap. 11, Tbilisi,
Georgia
as (“Company”)

Date: November 5, 2024

Hello,

We would like to inform you and confirm that we, MK Gaming LLC, operate as a B2B service provider, focusing on delivering a risk management platform and customer support services for licensed online casino, slots, and betting operators.

Please find attached an overview of our platform, outlining its capabilities and key features for further details.

Currently, MK Gaming LLC is in the final stages of obtaining its license, which is anticipated to be issued within the next one to two months. Once licensed, MK Gaming LLC will supply Middle Kang B.V., an online gambling operator, with relevant content of customer support and risk management tools. In compliance with Georgian legislation on gambling, particularly Article 3(c) of the Law On Organising Lotteries, Games Of Chance and Other Prize Games, Georgian-licensed companies providing B2B services (Supply of gambling and/or profitable games) are permitted to serve clients outside of Georgia.

Furthermore, as of early November 2024, MK Gaming LLC has committed to providing Middle Kang B.V. with a loan as per the relevant loan agreement. This deposit is expected to adequately cover the cost of Middle Kang’s online license in Curaçao.

Thank you for your attention to this matter, and please feel free to reach out with any questions.

Kind regards,



Bohdan Podilchuk

Director of MK Gaming LLC

FairPlay(RAF)

Risk detection and
management platform

Contents.

Table of contents	2
1. General information	4
1.1 Full name of the software and its symbol	4
1.2 Development goals and objectives	4
1.3 Terms and conditions of the software	5
1.3.1 Minimum hardware and software requirements	5
1.3.2 Communication requirements	5
1.4 Programming languages used to build the software	6
2. Functional purpose of the software	7
3. Description of the logical structure	9
3.1 Program structure with a description of the functions of the individual parts and the relationship between them	9
3.1.1. FairPlay Master	10
3.1.2. Feeds platform	13
3.1.3. Risk Management Monitor	13
3.1.4. FairPlay API	14
3.2 Relationship of the program to other programs	15
4. Description of the visual part of the program	18
4.1 Operators (anti-fraud, billing, risk management)	18
4.2. Supervisor	20
4.3. Trader	20
4.4. Analyst	20
4.4 Manager	20
5. Technical means used	22
6. Calling up and loading the system	23
7. Testing	24

7.1 Procedure for routine testing when implementing new functionality	24
7.2 Testing procedure after emergency shutdown of the system	25
8. System operation modes	26
8.1 Automatic operation of the system	26
8.2 Modes of limited operation	27
8.3 Training mode for staff	27
9. Staff qualifications	28
10. Documentation	29
Appendix 1. Glossary	30

1. General information

1.1 Full name of the software and its symbol

Full name: FairPlay risk identification and management software platform.

A conventional designation: FairPlay.

1.2 Development goal and objectives

The FairPlay risk identification and management software platform is designed to automate fraud management processes by comprehensively assessing customer accounts for risks, taking into account all available information about the account, and to supply data on the risk status of customer accounts to other systems. Thus, the implementation of FairPlay should help to reduce financial and reputational losses of the company due to unscrupulous customers.

Objectives of FairPlay:

1. Automate a comprehensive assessment of various risks on the part of a customer account, based on the customer's behaviour on the website, use of payment systems and wallets, receipt of bonuses, registration behaviour, personal data specified in the profile, and the presence of several accounts for one customer;
2. Provide a tool for automatically and manually assigning risk statuses to a customer account, applying various types of restrictions to a customer account;
3. Create a single source of data on the client's risk status for external systems integrated with FairPlay;
4. Create a user interface for the company's employees who are involved in the fight against fraud in one way or another.

1.3 Terms and conditions of the software

1.3.1 Minimum hardware and software requirements

The following components and technologies are used for FairPlay:

- 1) The containerization system for services is Kubernetes:
 - a) Minimum requirements:
5 servers Worker nodes 12x3.4 GHz, 128 Gb RAM;
- 3 servers Master nodes
 - b) Recommended requirements:
- 9 or more servers in a cluster, resources corresponding to the amount of data;
- 2) Data storage systems - PostgreSQL DB:
 - a) The minimum requirements are 2 servers with 32x2.3 GHz, 512 Gb RAM, 6x3 Tb SSD;
 - b) Recommended - 4 or more servers in a cluster by database groups, resources according to the amount of data;
- 3) Apache Kafka data exchange system:
 - a) The minimum requirements are 3 CPUs and 2 TB RAM;
 - b) We recommend 3 or more servers in a cluster, with resources corresponding to the amount of data;
- 4) The backup system includes 100 TB of mechanical disks;
- 5) Elasticsearch customer data storage and logging systems:
 - a) The minimum requirements are 6 servers with 2 CPUs and 8 RAM;
 - b) Recommended - 18 or more servers in a cluster by service groups, resources according to the amount of data.

1.3.2 Communication requirements

1. Internet access with a minimum channel of 100 Mbps, recommended 1 GBps or more, depending on the traffic load;

2. Domain name and real IP address of the IPv4 class.

1.4 Programming languages used to build the software

The platform components are implemented using different programming languages and technologies. The technological stack by components is presented in Table 1.

Table 1.

Component	Programming language	Library, framework
FairPlay	Python	Aiohttp, asyncio
DS (Data Science model)	Python	Scikit-learn, Pandas, NumPy, Tensorflow, Keras
Risk Management Monitor	Python, JavaScript	Aiohttp, Socket.io, Vue.js

2. Functional purpose of the software

The FairPlay platform is responsible for risk management in products, and its functional purpose includes identifying, verifying, monitoring, and responding to risk in the form of unique account or group settings.

FairPlay uses the data warehouse, i.e. external (not independently generated) data, as a service and is not responsible for its completeness and stability, but it controls the input data, its functionality includes monitoring and alerting the input status.

FairPlay is involved in several business processes, namely:

- Assessing the customer's integrity when interacting with the product platform;
- Detecting and monitoring risks by product;
- Post-evaluation of bets on the world line, outrunning, and other betting strategies with positive mathematical expectation, preparation of data on competitors for such evaluation;
- History of odds changes, comparison with competitors at each moment of the odds' life;
- Accounting for chargebacks and financial claims, manual and semi-automatic response to information on chargebacks and financial claims;
- Risk categorization and account setup process (payment system, multiple accounts, etc.);
- Finding groups of multi-accounts, using these groups as an intermediate result within "their" processes, and giving the groups as-is for the processes of external systems.

The FairPlay platform includes (see Fig. 2.1.):

- Backend logic of all the above processes;
- Workplaces of operators and other employees involved in the above business processes;
- Integration with the APIs of systems that need to be interacted with as part of these business processes;
- Heuristics, algorithms, ML-models that are used within the specified business processes.

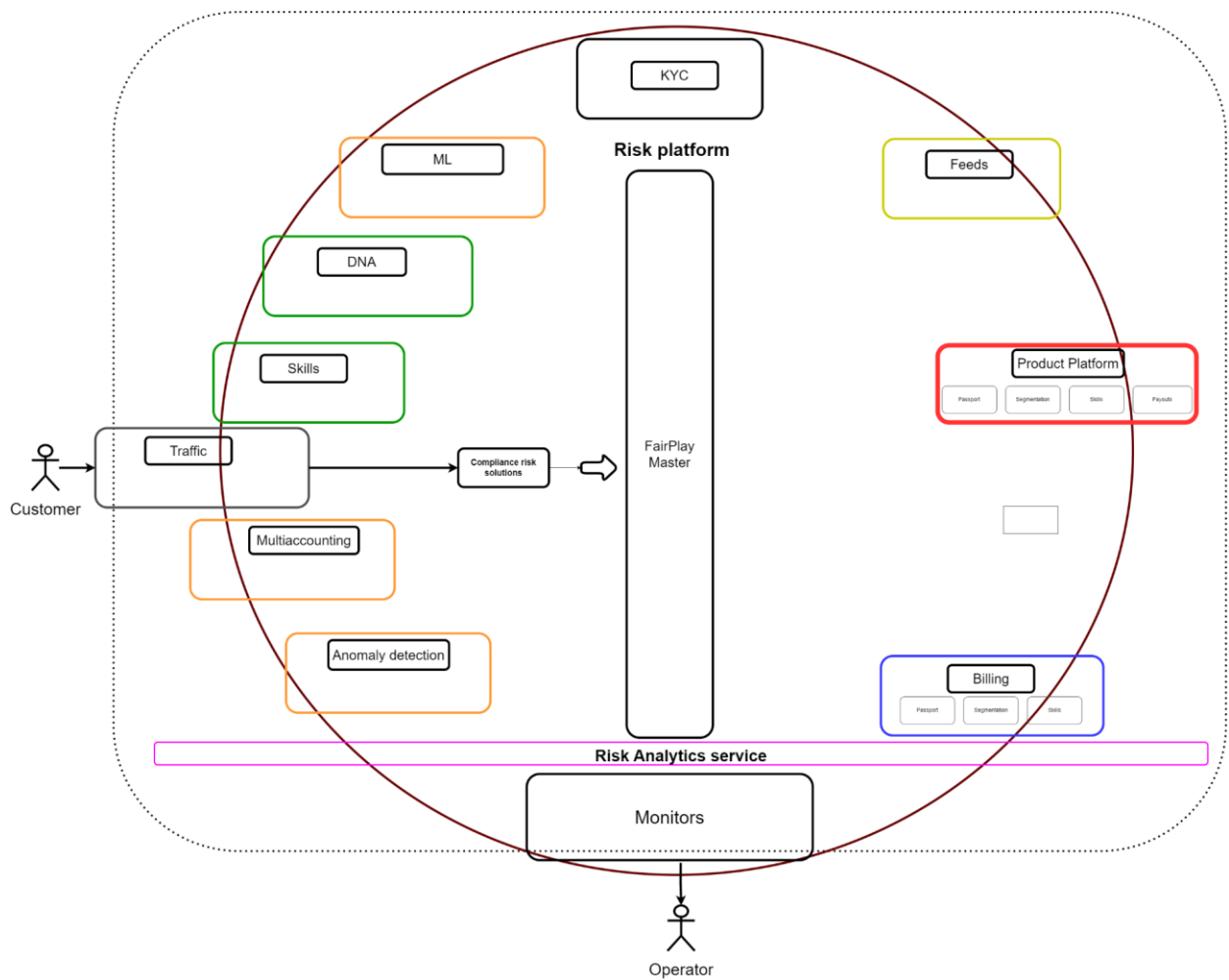


Fig. 2.1. The place of the FairPlay platform in the overall risk management ecosystem in the company

3. Description of the logical structure

3.1 Program structure with a description of the functions of individual parts and the relationship between them

The following logical components or subsystems can be distinguished within FairPlay (see Figure 3.1):

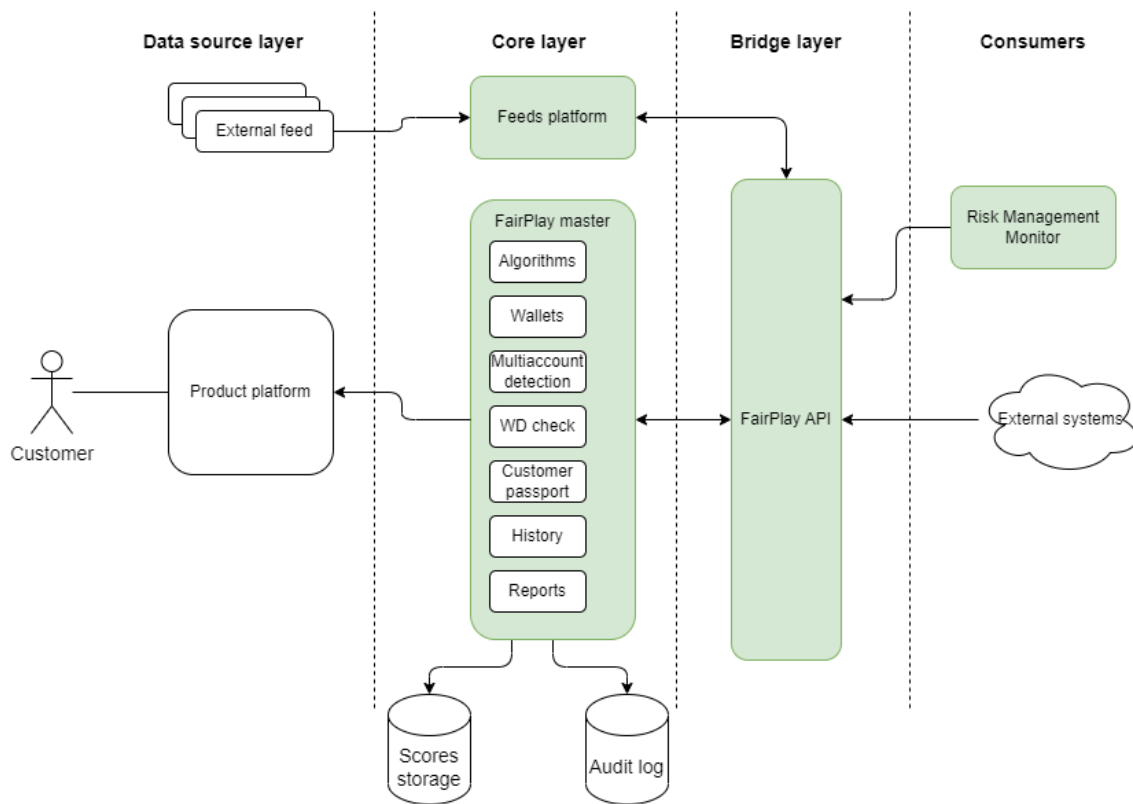


Fig. 3.1. Diagram of the high-level logical architecture of FairPlay

- The Core layer includes FairPlay Master, a set of services that directly calculate risk assessments based on specified algorithms and models, and the Feeds platform, a component responsible for receiving external data feeds, converting them, and recording them in the operating room;
- The Data source layer is a layer external to the FairPlay platform and includes any external data sources, such as the N.T.S.H. product platform or data feeds from external providers;

- The Bridge layer determines how the FairPlay platform exchanges data with other systems that are part of the company's IT infrastructure, and is implemented as the FairPlay API;
- Consumers of data received or generated by the FairPlay API platform are a component of the Risk Management Monitor platform, and other IT systems used in the company may also be consumers.

3.1.1. FairPlay Master

The main internal component of anti-fraud automation, the core of the system and the data provider for Risk Management Monitor. It is an ecosystem of services for automating data processing and transferring it to consumers. The services within FairPlay Master can read various data sets from external systems, for example, information about the customer and his activity and payments from the product platform, the odds of competitors from external data feeds received by the Feeds platform, etc. Downloaders are a set of services that receive data from external systems, pre-process it, transform it into internal FairPlay formats, and enter it into the RM Operational DB. The data is then transferred to Algorithms, where it is analyzed, aggregated, and evaluated according to certain risk factors. Machine learning models can also be used to process data. These scores are recorded in the database and made available for visual display in the Risk Management Monitor and other systems via the FairPlay API.

Also, all data is copied to the external DWH data warehouse, where historical data for the entire period of the platform's operation is stored, unlike the operational database, which has a data retention period of 2-3 months. Historical data can be used for further in-depth analysis and building analytical reports (see Section 3.2).

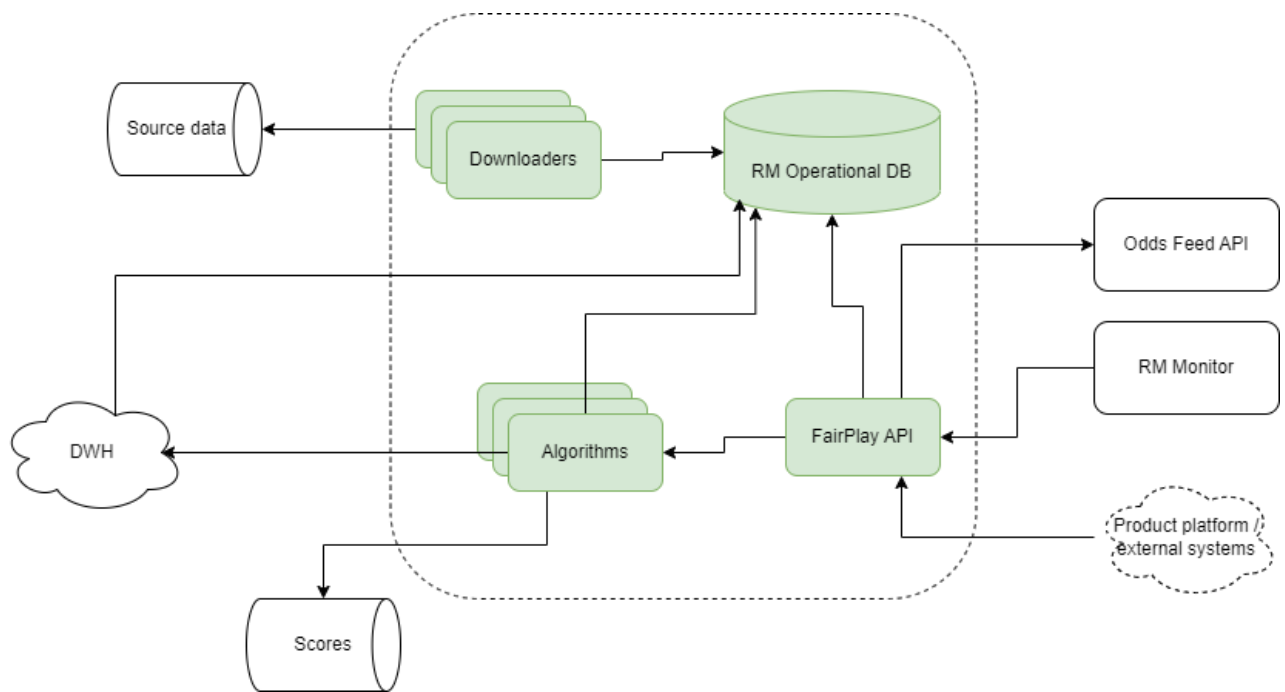


Fig. 3.2. FairPlay Master logical architecture

The core of the FairPlay Algorithms software package consists of separate services that are independent of each other but exchange data from the performed checks:

- **Algorithms** is a module for checking and assessing the riskiness of a client according to specified behavioural algorithms. Its main task is to monitor client accounts, evaluate their actions for signs of fraud using ML models according to specified algorithms, assign numerical estimates of the probability of fraud to client accounts, provide information to company employees by visually displaying potentially fraudulent accounts in Risk Management Monitor, assigning certain characteristics to client accounts or assigning them to a specific product segment depending on the client's activity on the product platform. Based on this information, a decision may be made to apply restrictions to the account, block it, or take other anti-fraud measures;
- **Wallets** is a module for monitoring customer wallets and segmenting them by risk level. The module is designed to monitor and segment customer wallets in order to identify fraudulent wallets and limit or completely block financial transactions for them. Fraudulent wallets can be considered to be those linked to more than one customer account; linked to an account that has

already been detected for fraudulent activities; or those that have received financial claims from payment operators. Depending on the presence of these features and their combination, a wallet can be identified by the system as fraudulent, in which case it is displayed in RM Monitor and sent to the operator for verification;

- Multiaccount detection is a module that searches for accounts that are likely to belong to the same customer, including accounts registered with fake or stolen personal data. It analyzes all new accounts and compares them with those that already exist in the system based on attributes such as IP address, device and browser, personal data, payment information, etc. The module's functionality also includes reading triggers, events, and actions with the customer's account. For example, triggers can be registration, website visits, financial transactions, editing profile data, etc. Based on the results of the analysis and comparison, pairs of accounts are formed and those accounts that overlap in their attributes are combined into groups;
- Withdrawal check is a module for checking withdrawal operations from the system. It is designed to automate the monitoring of withdrawal requests, evaluate such requests for signs of fraud according to specified algorithms, and submit suspicious requests to operators for review (outputting them to RM Monitor);
- Customer's passport is a module for the centralized display of all available information about a customer from a risk perspective. It is designed to aggregate all the basic information about a customer account. This information includes: the current risk status of the client, data on the client's activity on the website, data on their financial transactions and wallet/card statuses, data on the client's profitability for the company, the results of analysis using risk assessment algorithms, data on bonus receipt, possible multi-accounts, etc., transfer of the client's status and restrictions recommended by the system to RM Monitor;
- History is a module for logging the history of all actions performed by users on client accounts in other modules that are part of the FairPlay platform. The list of operations that are subject to logging includes account search, account view, setting restrictions, forced session termination, wallet search, setting the risk status for an account, setting the risk status for a wallet, setting the status for a group of multi-accounts to which the account belongs;
- Reports is a module for designing and generating reports.

3.1.2. Feeds platform

The FairPlay Feeds platform receives feeds of data on competitors' odds and can provide other components of the FairPlay platform with information about odds, surebets, overbets, etc.

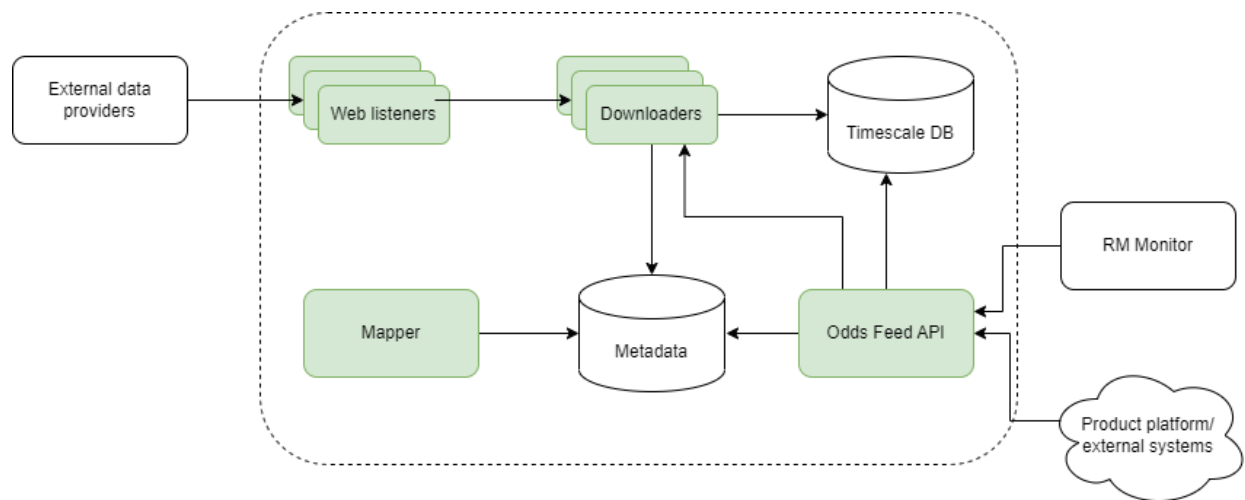


Fig. 3.3. Logical architecture of the Feeds platform component

A set of Web listeners services (see Fig. 3.3) receives input signals from the data provider about new data/changes in data and initiates the Downloaders services, which, if necessary, convert the data to the internal FairPlay format and upload the data to the Timescale database and metadata about them to the Metadata database. The Mapper establishes a correspondence between the received data and the internal data of the platform, if necessary. Then, using queries via the Odds Feed API, other platform components or external systems can retrieve the necessary data on the odds of competitors from the database.

3.1.3. Risk Management Monitor

Risk Management Monitor provides a visual user interface for working with the FairPlay platform. With its help, anti-fraud operators can view various information about customer accounts, receive certain notifications and signals, and based on this, make decisions on the application of restrictions.

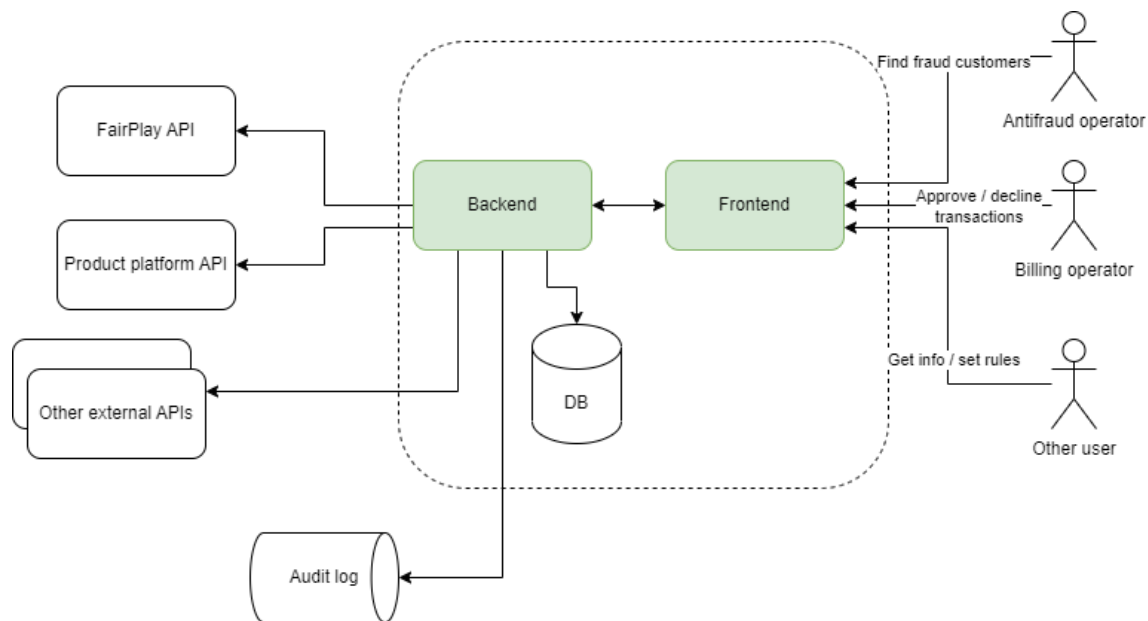


Fig. 3.4. Logical architecture of Risk Management Monitor

RM Monitor (see Fig. 3.4) receives information about customer profiles and their activity on the product platform via the platform API, and information about customer evaluation using algorithms from FairPlay Master via the FairPlay API. Changes made by operators, including the application of restrictions to customer profiles, are also transmitted back to the platform via the API. The entire history of operations performed on customer profiles, such as searching, viewing, setting or removing restrictions, and assigning a customer to a certain segment, is recorded in a special database.

3.1.4. FairPlay API

An interface designed to transmit various types of data to consumers, which can be both other components of the FairPlay platform and systems and services external to it.

Currently, it is possible to receive such data using the FairPlay API:

1. Personal information about the client;
2. Customer verification history;
3. Current customer wallet balance and current customer bonuses;
4. Current restrictions applied to the client's account;
5. Customer product preferences;
6. The current status of the client;

7. A list of algorithms used to evaluate the customer profile;
8. Evaluation of customer profiles using different algorithms;
9. Existing statuses (in terms of multi-accounting)
10. Create a new status;
11. Assign a status to a group of accounts;
12. Customer payment history;
13. History of refund requests;
14. Create a refund request;
15. Refund requests have been processed;
16. A list of existing product segments in the platform;
17. History of customer affiliation with product segments;
18. The current list of segments to which the customer belongs;
19. Reset current customer product segments.

3.2 How the program relates to other programs

Fig. 3.5 shows the links between the FairPlay platform and other systems. They include:

- **The product platform** is the N.T.S.H. betting platform;
- **External data feeds** are third-party services designed to collect data as quickly as possible. The connection is one-way, with providers aggregating data into files of a specific format (JSON, CSV, or XML), and the FairPlay Feeds platform component reads such files at a specified frequency;

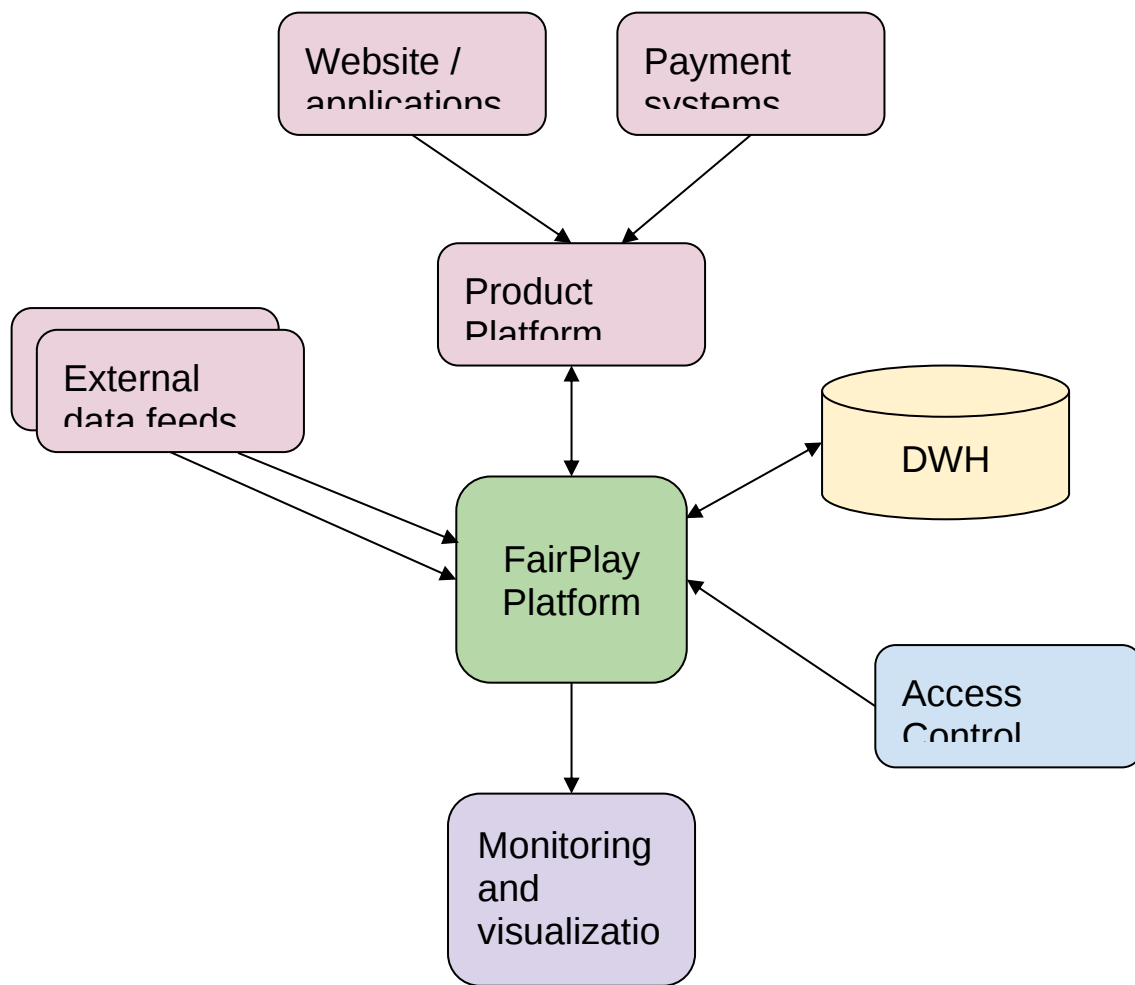


Fig. 3.5. Integrations of the FairPlay platform

- **Data warehouse (DWH)** - FairPlay transfers the entire array of accumulated data on the customer's risk status, data on the customer's activity on the website, data on their financial transactions and wallet/card statuses, data on the customer's profitability for the company, analysis results using risk assessment algorithms, data on bonuses, possible multi-accounts, etc. to the data warehouse, where they are stored without time limits. Later, the accumulated data is used to generate analytical reports. Some FairPlay services may also request historical data from DWH that is not available in the FairPlay platform's operational database;

- **Access control system is a** system that stores information about the configured roles and permissions for all components of the FairPlay platform;
- **Visualization and monitoring tools** - the FairPlay platform can transfer data on its metrics to external systems for easy visualization and automatic monitoring.

4. Description of the visual part of the program

4.1 Operators (anti-fraud, billing, risk management)

The following functionalities of the FairPlay platform are available to operators:

1. Viewing and searching customer accounts to monitor and segment customer wallets in order to find untrustworthy wallets and limit or block financial transactions for them;

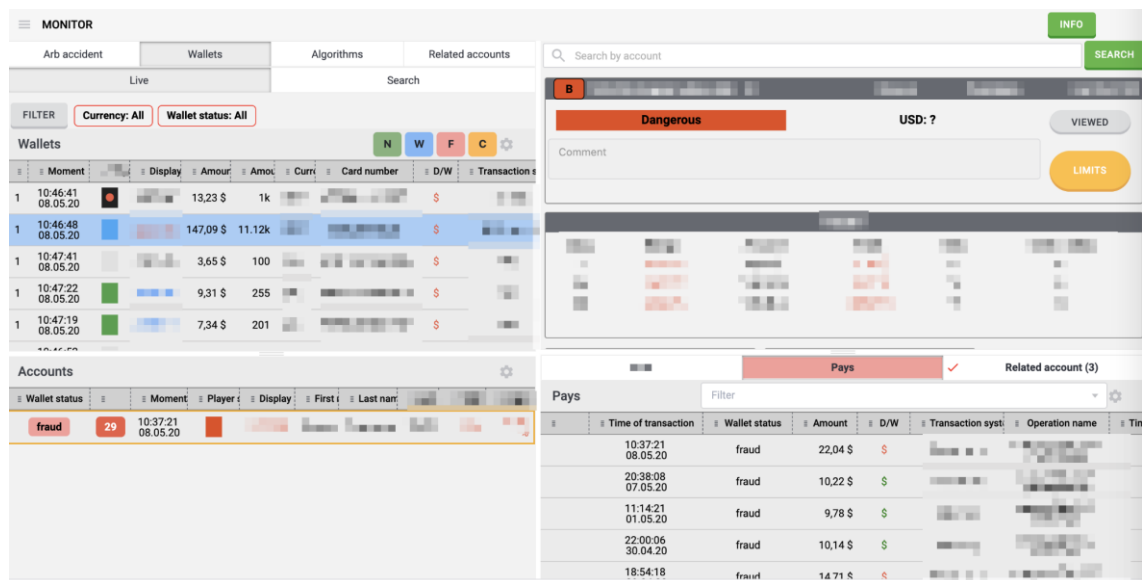


Fig. 4.1. Interface for viewing client financial transactions

2. View and search the list of clients whose accounts have been triggered by at least one of the risk detection algorithms, the date and time when the account was added to the monitor, the algorithm that triggered it, and the client's action window used for analysis. Actions within the selected action window that the algorithm marked as suspicious and based on which it calculated the percentage of fraud probability for this account;

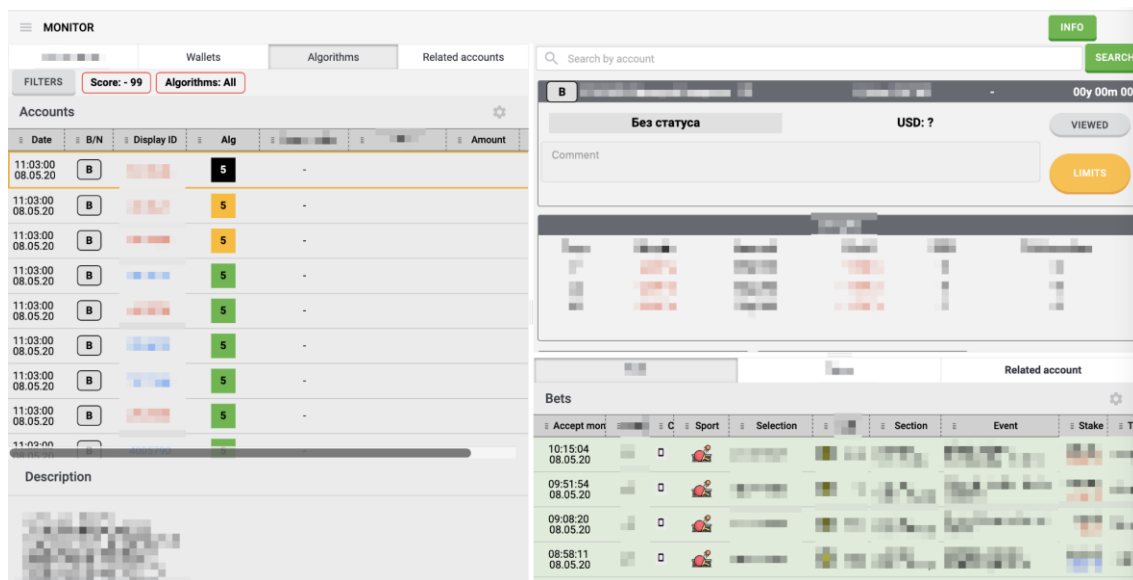


Fig. 4.2. Interface for viewing customer risk status assessments

3. View customer data in a single window, as well as assign a risk status to a customer, set account restrictions, and manually terminate a customer session;

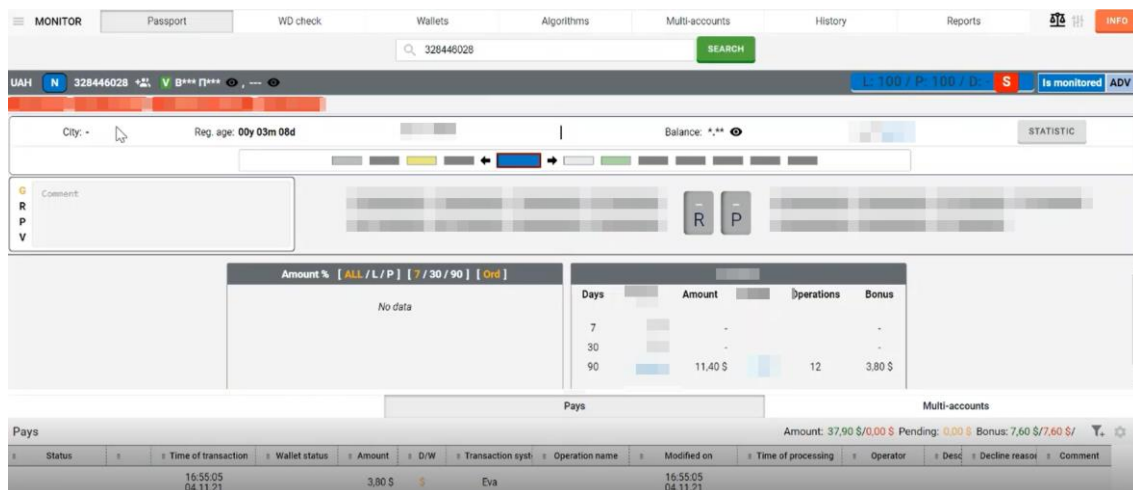


Fig. 4.3. Interface for viewing consolidated data on the client profile

4. View and monitor groups of customers with multiple accounts on the website, or with registration using fake or other people's personal data, assign risk statuses to the group, set restrictions for the group.

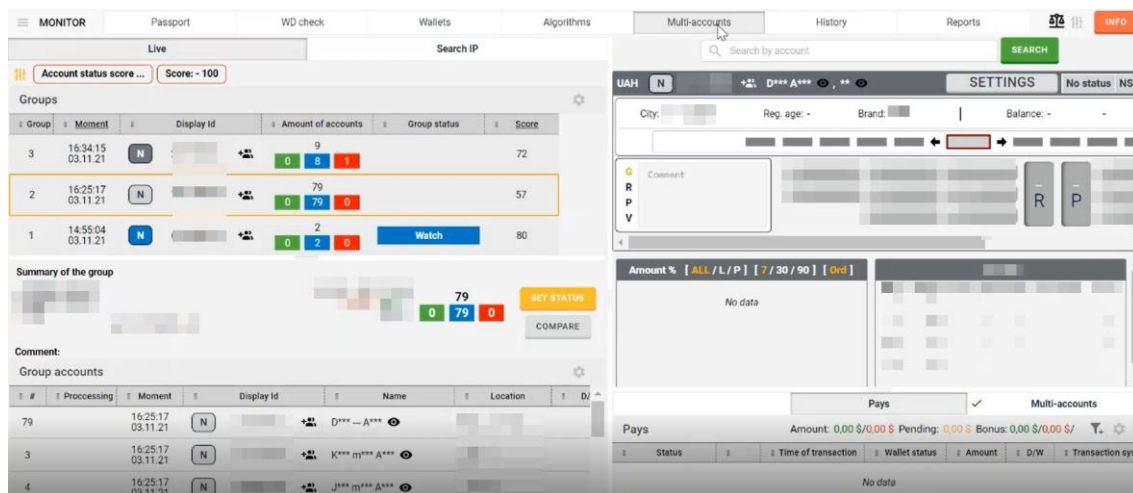


Fig. 4.4. The interface for viewing multi-accounts

4.2. Supervisor

Users of the FairPlay platform with the role of supervisor have access to functionalities similar to those of operators (see clause 4.1). They also have the ability to track the actions of operators assigned to them.

4.3. Trader

Users of the FairPlay platform with the role of a trader have access to the functionality of searching for client accounts, viewing consolidated data on clients in the context of their risk assessment.

4.4. Analyst

Users of the FairPlay platform with the role of analyst have access to the functionality of creating and viewing reports.

4.4 Manager

Users of the FairPlay platform with the role of manager have access to the platform management tool - Admin Panel (available as part of the Risk Management Monitor). The manager makes changes to the operation of services and their parameters, namely:

- setting up configurations for risk assessment services;
- start/stop testing algorithms;
- enable/disable the display of algorithm models used for risk assessment.

FAIRPLAY Brand Tin
User Tim

Menu

OPERATOR GROUPS

Model id	Model name	Display name	Alias	Version	Status	Display in monitor	WD Check	Background color	Actions
1				4	Disabled	☐	☐	—	
2				1	Active	☒	☐	—	
3				1	Active	☒	☐	—	
4				2	Active	☒	☐	—	
5				3	Active	☒	☐	—	
13				1	Active	☒	☐	—	
14				5	Disabled	☐	☐	—	
15				1	Active	☒	☐	#56B84D	
16				1	Active	☒	☐	—	
53				1	Active	☒	☐	—	
54				2	Active	☒	☐	—	
100				1	Disabled	☐	☐	—	
7219				1	Disabled	☐	☐	—	
7220				1	Disabled	☐	☐	—	
7221				3	Disabled	☐	☐	—	
7222				1	Disabled	☐	☐	—	
7223				1	Disabled	☐	☐	—	
7224				1	Disabled	☐	☐	—	
7225				1	Disabled	☐	☐	—	
7226				1	Disabled	☐	☐	—	

Fig. 4.5. Interface for configuring the operation of FairPlay platform services and algorithms

5. Technical means used

For the platform to function and allow developers, testers, and users to work with all its modules, a standard for workstation equipment has been introduced, as described in Table 2.

Table 2: Hardware requirements for workstations of internal users of the system

Role: Trader, risk management operator	
Processor	Intel Core i5
RAM	16GB
Disk space	256GB
Interfaces	USB 3.0 HDMI
Network adapters	Wi-Fi 802.11ac, compatible with IEEE 802.11a/b/g/n Bluetooth 4.0
Role: Developer, tester, system administrator	
Processor	Intel Core i7
RAM	16GB
Disk space	256GB
Interfaces	USB 3.0 HDMI
Network adapters	Wi-Fi 802.11ac, compatible with IEEE 802.11a/b/g/n Bluetooth 4.0

6. Calling up and loading the system

Employees have a single login and password to access all components of the FairPlay platform that they need to perform their job duties. Any of the components can be downloaded through a web browser using the internal address of the component. After authorization under his login and password, the employee receives access rights defined by the company's internal regulations.

Startup procedure for the user:

Via the website from a desktop computer:

1. Open a web browser;
2. Perform authorization on the Platform;
3. Go to the address of the required FairPlay component in the back office.

7. Testing

7.1 Procedure for routine testing when implementing new functionality

In order to prevent defects and loss of performance, all functionality on the platform is tested on several test environments. Only after successful completion of tests on these test environments can changes be made to the production environment.

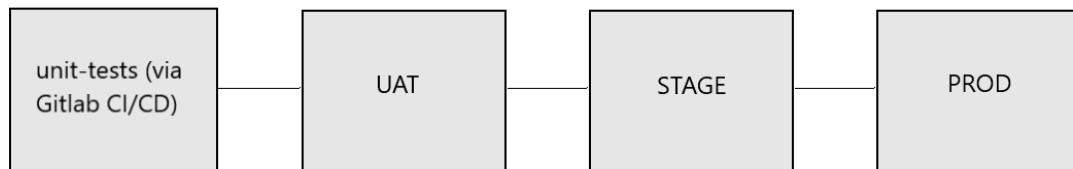


Fig. 7.1. FairPlay test and production development environments

At the first stage, the team writes unit tests for the new functionality, which are automatically run every time in Gitlab CI/CD.

The second stage of testing takes place on a shared UAT test environment, which is cross-team, so developers can test the interaction of their new functionality with the developments of all other teams and with the services of external providers (usually, the operation of such services at this stage is modeled using mock objects).

The third stage of testing takes place on the STAGE test environment, which is configured as close as possible to the production environment and can use real anonymized data sets. STAGE performs integration testing, end-to-end testing, security testing, performance testing, and regression testing. For regression testing, autotests are widely used to quickly and efficiently check that the new functionality does not disrupt the operation of the existing one. Performance testing takes place according to a predetermined schedule during non-working hours for most programmers. At the same stage, the final preparation for the release takes place - when a sufficient number of updates have been accumulated, their joint performance is tested.

After the changes are released to the production environment, post-release testing is immediately performed, including happy path testing, end-to-end testing, and validation of integrations with external providers' services.

7.2 Test procedure after emergency shutdown of the system

When the system resumes operation after an emergency shutdown or after scheduled maintenance, critical functionality tests (end-to-end) are mandatory to confirm the correctness of the system:

1. The client is not allowed to take any actions that may affect the operation of the platform during an emergency shutdown.
2. On the back office side, you can see the display of FairPlay Risk Management Monitor tabs and the ability to update and edit data. Data loading takes no more than 2 seconds.

8. System operation modes

8.1 Automatic system operation mode

In the normal mode of operation, when the full set of necessary functions is performed with maximum performance, FairPlay is constantly available to the user - 24 hours a day, 7 days a week.

Processes such as updating the database software, performing backups and restores only take place at night from 01:00 to 07:00.

The following security mechanisms and procedures are provided for in the normal operation of the platform:

1. A mechanism for identifying users according to their role;
2. Methods of protecting customer personal data from loss - all platform components that store customer personal data are protected:
 - a. at the network level - by using firewalls and restricting access to systems;
 - b. at the database level - by managing access to databases/tables containing personal data;
 - c. personal data is transmitted via encrypted communication channels;
 - d. the display of customer data for the back office user is carried out in a masked form;
 - e. all user actions are logged in the History section;
 - f. access to information systems is subject to regular internal audit.
3. Any attempt to distort, tamper with, destroy, copy, or unauthorized access to information resources is an information security incident and is investigated in accordance with internal procedures.

8.2 Modes of limited operation

In the event of a load in terms of the number of database queries, there are recommendations for disabling certain services that affect this process. Also, a mechanism has been implemented to postpone some data to the storage for further processing if there is a problem with the processing schemes of this data in the message broker.

8.3 Training mode for staff

Training takes place in a regular mode. At first, the employee has minimal access to the functionality, and in the course of work and under the supervision of a supervisor, he or she acquires the necessary skills. Later, with the growth of responsibilities and improvement of skills, the employee gets access to wider functionality.

9. Staff qualifications

The platform has the following categories of users:

- 1) Manager - responsible for the overall monitoring of the platform, has access to all the functionality and reporting;
- 2) Trader is responsible for posting and updating dynamic content and has access to client data and risk status;
- 3) Analyst - responsible for collecting data, analyzing customer activity, and preparing reports;
- 4) Anti-fraud specialist is responsible for detecting and preventing fraud attempts;
- 5) Payment processing specialist - ensures the correct operation of the auto-payment service.

A payment processing specialist, manager should have experience in platform skills and use of a personal computer (PC) running Microsoft Windows or MacOS operating system (OS) at the level of a skilled user.

A trader, an anti-fraud specialist, must have experience with the main functions of the platform and experience in using a personal computer (PC) running Microsoft Windows or MacOS at the level of a qualified user, understand the basic principles of mathematical statistics and probability theory.

The analyst should have excellent technical knowledge and skills in working with the platform software interface in terms of configuration and management, have skills in working with databases, building SQL queries, working with data visualization tools such as Tableau or similar. In addition, you must have advanced level experience in using a personal computer (PC) running Microsoft Windows or MacOS operating system (OS).

10. Documentation

To perform their functional duties, employees are provided with reference information that is confidential and stored in an internal online knowledge system with established access restrictions.

The following reference documents and instructions are available for your review:

- Backoffice User Guide;
- Instructions for working with FairPlay Monitor.

Appendix 1. Glossary

Account is a record in the platform's database containing a set of information that the user transmits. Usually, in order to create an account, a user is asked to complete a registration procedure.

Alerting is a system of notifications about the occurrence of certain types of events in the system, as well as recording these events in the log.

Anti-fraud, or fraud monitoring, is a system that assesses the suspiciousness of financial transactions and other operations, as well as customer actions, in terms of fraud.

Database - a set of independent materials presented in an objective form, systematized in such a way that these materials can be found and processed;

Message broker (Apache Kafka) is a platform that collects, processes, stores, and distributes data. It is used to exchange data between systems and applications;

A website is a collection of web pages and dependent content available on the Internet that are unified in terms of both content and navigation under a single domain name;

Web API is an application program interface API accessible via the Internet, used to interact between a web server and a client;

Metadata is a set of standard information about a file that is used by workflow organizations. This includes the author's name and surname, resolution, color space, copyright, and keywords that apply to it.

A mobile application is software designed to run on smartphones, tablets, and other mobile devices, created using specific programming languages and technologies for mobile devices;

An operating system (OS) is a set of interconnected programs designed to manage computer resources and organize user interaction;

Payment system/payment operator is a set of software, hardware and telecommunication technologies designed to perform financial transactions in a non-cash manner.

Workstation - a computer with a specific set of hardware and software tools designed to allow its user to solve tasks of a certain type;

The server is a component of the software package that contains the parameters of each of the components and is responsible for the logic and mechanisms of interaction with the platform and the database;

A DBMS is a set of databases and programs for accessing these data. It provides the ability to create, save, update, and search for information in databases with data access control.

Service / Service - a discrete software component that represents a specific functionality and is used as part of an application;

A trigger is a special kind of function that is automatically executed when a certain event occurs on the database server.

A firewall is a set of hardware or software tools that monitors and filters network packets that pass through it in accordance with predefined rules;

CI/CD (Continuous Integration/Continuous Delivery) is a software development methodology that ensures reliable and fast product creation due to the fact that testing and building of the program is carried out automatically.

A downloader is a program (module, script, library, etc.) whose main task is to download and install software.

Gitlab is a website and management system for program code repositories for the Git versioning system, with additional features: its own knowledge base and bug tracking system.

Listener - a procedure or function that is associated with a specific event and is called only when this event occurs.

Machine Learning (ML) is the process of creating algorithms to detect patterns in the analysis of big data and use them for self-learning programs.