PAYSOS

Sensitive Payment Data Policy

1 Introduction

Roark Holdings Ltd. (the Firm) has been providing Payment Services since [Date]. The Firm ensures sensitive payment data, as defined in the Payment Services Regulations 2017 (PSR 2017), is protected, monitored and stored appropriately to comply with the PSR 201.

2 Purpose of this Document

The purpose of this document is to detail the Firm's approach to sensitive payment data across the business.

3 Sensitive Payment Data

The Firm defines sensitive payment data as information, including personalised security credentials which could be used to carry out fraud. The Firm collects transaction and KYC information from clients that can be classified as sensitive payment data. The following information is collected:

Sensitive Payment Data	Use of collected data
- First name, last name, date of birth, address, phone number, beneficiary details (first name, last name, bank account details for bank transfers, address and phone number).	KYC information
- Basic details, transaction amount and date of payment receipt from customer, unique transaction reference number, date of payment made to beneficiary, method of payment.	Transaction information

4 Sensitive Payment Data Flows

A diagram outlining how the data flows through the infrastructure of the Firm is in Appendix 1. The following systems store sensitive payment data during the day to day activities of the Firm.

- The client wants to replenish the account with a bank transfer, for this he creates a withdrawal transaction with the bank indicating the details for replenishing the account with a financial company.
- The bank sends a message about the incoming transfer.
- The **transaction is created** in the back office through the API or manually (manual creation / loading of statement).
- The system checks if the transaction needs to be confirmed by the financial controller:

4.1 Financial controller **approves** the transaction, the transaction goes through an AML **check** (*paragraph 5.2.*).
4.2 Financial controller doesn't approve the transaction. Transaction will be **Closed** (*paragraph 11*).

The platform checks for matches to identify the recipient (name, comment, link number, etc.).

5.1 **Receiver is not found** automatically
5.1.1Transaction will be reviewed by the manager to identify the receiver of the funds.
5.1.2 In case the **receiver is not found** the transaction goes through **AML check for the sender** of the funds.
If the sender was not approved by the AML the transaction will be **canceled** and funds will be **returned** back (*paragraph 11*).
If the **sender has been verified** the transaction will be holded for 30 days.

6.1 If the receiver will not be found the transaction will be **canceled** and funds **returned** (*paragraph 11*).
6.2 If the receiver of the funds will be **found,**the transaction will be redirected to **AML check** (*paragraph 5.2*).
6.2.1 If a **receiver is found**, the transaction will be redirected to **AML check** (*paragraph 5.2*).
6.3 **Receiver found** automatically
6.3.1 If a match is found, the transaction goes through **AML check**.

7. Transaction is not approved by compliance.
7.1 Transaction will be **canceled** and funds **returned** (*paragraph 11*).

8. Transaction is approved by compliance.
8.1 The platform checks whether a **fee settlement** is required. If necessary, the system sends a message to the bank after which the bank transfers the fee from an account with customer funds to a company account.
8.2 The funds credited to the client's account and a **notification** is sent to him.
8.3 The system checks the outgoing payment.

9. Transaction completed.
9.1 The client received a notification and transaction details.
9.2 Client creates the request for a refund to the sender.
9.3 The system has received a **refund request**.
10. Transaction will be **closed** (paragraph 11).
10.1 Cancel incoming transactions and **return funds**. Sending a refund notification to the bank.

5 Sensitive Payment Data Access

The Firm restricts access to sensitive payment data through its Access Rights Policy. The Access Rights Policy is based on the principle of least privilege i.e. access is granted based on the minimum amount of access needed to fulfill a role. The Access Rights Policy provides further detail on how sensitive payment data is accessed, who decides the levels of access, and the process for changing levels of access.

5.1 Access Monitoring

The Firm monitors access to Sensitive Payment Data automatically through the its system. Through automatic monitoring the Firm is able to record and track any changes to sensitive payment data and identify access outside of expected job requirements. The automatic monitoring assists in producing the audit trail of changes and access to sensitive payment data. The Firm performs an annual review of access rights, as well as a review following a change in role, to ensure access remains specific to job requirements. The Firm also performs a monthly review of access logs and raises any issues with senior management.

5.2 Sensitive payment data access for customers (if applicable)

The Firm's online platform is accessible for customers using a preassigned ID and password, as outlined in the Access Rights policy. The password policy in place clearly defines the parameters for a password to be suitable. The sensitive payment data that is accessible via the web portal includes only sender and recipient names.

6 Use of Collected Data

The Firm collects sensitive payment data in order to perform transactions, maintain records for transaction monitoring and fraud reporting purposes, and to perform KYC as a fraud prevention method.

6.1 External use of Collected Data (if applicable)

No external parties are allowed to access any sensitive payment data of Roark Holdings Ltd. (the firm)

Provided below is a table that includes all external parties with access to sensitive payment provided to The Firm, the purpose of their access and with whom the relationship responsibility lies internally. The firms are aware of their responsibilities regarding the security of sensitive payment data and have adequate controls in place.

7 Security Measures

The Firm's Security Policy ensures Sensitive payment data is protected and access is restricted. The Firm's Security Policy provides detail on the technical security measures that have been applied to the Firm systems to ensure sensitive payment data is adequately protected. The Firm will detect breaches through the systems in place in the Security Policy. These breaches will be alerted to the Firm and it will be responsible for handling the breach. The Firm will then present mitigation measures to the Senior Management body to ensure further breaches can be prevented.

8 Annual Internal Control Program

The Firm operates internal control programs regarding the safety of IT systems and the storage of sensitive payment data. The Sensitive payment data policy is reviewed annually, the Access rights policy is reviewed annually and the Security policy is reviewed annually. Any updates are added accordingly, with all relevant parties made aware of the updates and reports provided to the management body.