Fraud Prevention Policy

Purpose of this Document

As a payment service provider, Roark Holdings Ltd. (the Firm) will face the threat of fraud (both internal and external) which will need to be addressed.

This policy details how the Firm will approach identifying the fraud risks that it faces, when delivering its payment service, and implementing the necessary controls to mitigate them.

Review of Policy

This policy will be reviewed regularly, at least once a year, and amended as considered necessary by the Firm's Management Body in the event of changing circumstances or regulations.

Risk Assessment

All Fraud risks will be identified using a fraud risk assessment, which has been appended to this document.
The risk assessment will provide details of the following:

- Details of Internal and External Fraud risks the Firm faces.
- The controls in place to mitigate those risks.
- The policies that have been developed to implement the controls.
- Details of how the policies are monitored.

4 Fraud Risks

The Firm has identified the following risks relating to fraud:

4.1 Internal Fraud

Employees acting in a fraudulent manner, resulting in either:

- Financial loss, from either the company or a customer.
- Identity fraud, resulting in a customer's data being compromised.

4.2 External Fraud

External threats have been identified in the following areas:

- Clients acting fraudulently.
- Fraudsters posing as potential clients.
- Email fraud; emails from 3rd parties purporting to be clients/staff.
- Cheque fraud.

5 Controls to mitigate the risks

The Firm has implemented the following controls, which will mitigate the risks identified above:

5.1 Controls for Internal Fraud

The Firm has implemented the following controls:

- Identity checks as part of the employment process, which will include a DBS check.
- Data visibility restriction by department, which is governed by an Access Rights Policy.
- Access to internal systems and trading platforms governed by an Access Rights Policy.
- The Firm also uses pro-active anti-cyber fraud mailers to our client base to promote awareness and vigilance.

5.2 Specific Policies to implement the controls

The following policies have been implemented by the Firm, which will enable these controls to be implemented:

- Access Right Policy.

5.3 Controls for External Fraud

The Firm has implemented the following controls in relation to the external fraud risks

- KYC checks during on-boarding.
- As part of this policy, the Firm has made the decision not to accept cheques.
- Staff training to be aware of fraud trends.
- Operational process to confirm all new beneficiary details with clients to avoid client email fraud/interception – see appendix 2.

5.4 Specific Policies to implement the controls

The following additional policies and checks have been implemented by the Firm, which will enable these controls to be implemented:

- AML Policies and Procedures.
- Daily checks to prevent cheques being paid in to our client accounts.

6 Issue Monitoring and Resolution

The controls outlined in this policy have been designed to prevent a fraud related issue from occurring. Where an issue does occur, details of how it will be monitored and resolved are outlined in the Operational and Security Incident Reporting Process.

7 Compliance Monitoring

This policy will be monitored through the compliance monitoring plan.

8 Breaches of Fraud Policy

Any breaches of the Fraud policy will be recorded on the Firm's breach log in conjunction with its Regulatory Breach policy.

Appendix 1: Risk Assessment

Factor	Area	Details of focal point	Risks	Controls	Policy	Monitor
Fraud	Internal Fraud	Staff members	There are several types of fraud that we address in our various preventative measures. Some examples of fraud are as follows: · Social engineering: Someone can convince an employee that they are supposed to be let into the office building, or they can convince someone over the phone or via e-mail that they're supposed to receive certain	· All employees, regardless of job responsibilities, are made aware of the potential incident identifiers and who to notify in these situations. · Identity checks as part of employment pro-cess. · Data visibility restriction by depart-	· Access Rights Policy · Fraud Policy · Security Policy	· Control measures are continuously monitored and improved when a problem is detected. · Issue Resolution Policy · Compliance Monitoring Plan – Including annual policy updates

			information. · Careless disposal of documents: Employees who aren't careful when throwing away papers containing sensitive information may make secret data available to those who check the company's trash/bins. · False pretences: Someone with the intent to steal corporate information can get a job with a cleaning company or other vendor specifically to gain legitimate access to the office building. · Financial fraud · Identity			

			fraud (client data)			
	External Fraud	· Fraudsters posing as potential clients · Email fraud · Clients	· Computer viruses: With every click on the internet, a company's systems are open to the risk of being infected with nefarious software that is set up to harvest information from the company servers. · Identity fraud · Cheque fraud · Email fraud from 3rd parties purporting to be clients/staff.	· KYC checks during onboarding. · Daily checks to prevent cheques being paid into our client accounts. · Staff training to be aware of fraud trends. · Phone calls to confirm all new beneficiary details with clients. · Operational process to confirm all new beneficiary details with clients to avoid client email fraud / interception. · Policy not to accept cheques as payment.	· AML policies and procedures ·Fraud policy	· Issue Resolution Policy · Compliance Monitoring Plan – Including annual policy updates

Appendix 2:

Operational process to confirm all new beneficiary details with clients to avoid client email fraud/interception

To protect the Firm and its clients, this policy has been developed to increase both client awareness of fraud and to increase operational robustness throughout the payment process.

All new beneficiaries requested by clients will be confirmed verbally by the Firm operations team using the following process.

1. **As new beneficiary details are emailed to operations team by client (or the Firm's dealer), the team member responsible for inputting the 1st stage of the new beneficiary in Roark Holdings Ltd is responsible for calling the client.**
2. **The client will be phoned on the number provided during on-boarding,**
3. **If client in question would prefer to call us back they can do so. When clients are calling us they should then confirm date of birth/1st line of address and postcode prior to beneficiary authorisation.**
4. **Wording required:**

Hi.....

As part of an additional fraud prevention check that Roark Holdings Ltd carry out, we would just like to verbally verify your new beneficiary details requested today(yesterday etc).

Please can you clarify:

1. New beneficiary name
2. Last 4 digits of new account no. / IBAN
3. When verbal confirmation gained successfully from client, notes detailing confirmation call to be added within notes section of trade in BOS.

New beneficiaries are exempt from this process if they are added by the client using our online platform.