CLIENT SCHEDULE

Security Procedures Schedule

How we check that instructions and payment-detail changes are genuinely yours, your choices, and who bears a loss.

Issued by	Flumen Pay LLC, trading as Lydiam Group
Version and date	Version 1.0 · 28 October 2026
Owner	Ayaz Khan, Chief Executive Officer
Status	Issued for use (v1.0)
Document reference	D07 (part of the Client Portal Terms of Use)
Applies to	Every client; provided with the Client Portal Terms of Use and every Client Agreement; any opt-out signed

1. About this Schedule

1.1 This Security Procedures Schedule forms part of the Client Portal Terms of Use and of every Client Agreement of Flumen Pay LLC, trading as Lydiam Group (the "Company", "we" or "us"). Capitalised terms have the meanings given in the Common Definitions Schedule.

1.2 As the Common Definitions Schedule provides, the "Security Procedures" are the security procedures set out in this Schedule, as accepted by the Client or varied by its written opt-out. In this Schedule, "Mandate" means the Client's Authorised Signatory and Authorised User Mandate, which registers its Authorised Users and their telephone numbers, email addresses and messaging accounts.

1.3 The Security Procedures are designed to check that an instruction, or a change to payment details, genuinely comes from the Client. They are not designed to detect errors in the content of an instruction, such as a wrong account number or amount given by the Client.

2. Channels

2.1 Instructions are accepted only from Authorised Users, through the Portal or the Company's designated channels: dealing@lydiamgroup.com and the telephone numbers and WhatsApp and Telegram accounts listed in the Portal.

2.2 The Company does not act on an instruction received on any other channel, number or account, even if it appears to come from the Client.

2.3 The Company's own payment details for the Client are shown and changed only in the Portal. The Company never sends new payment details by email, chat or phone, and never asks the Client to pay anyone other than Flumen Pay LLC.

2.4 The Company never asks for a password, a two-factor authentication code, a private key or a seed phrase, on any channel.

2.5 A payment received for the Client that the Company cannot explain is returned only to the account it came from.

2.6 The Client uses only the telephone numbers, email addresses and messaging accounts registered in the Mandate, and does not use disappearing or auto-deleting messages with the Company.

2.7 The Company may refuse or delay an instruction given through a VPN, proxy or anonymising network, or in other circumstances that indicate fraud, and tells the Client promptly in the Portal or by email, with the reason where it lawfully can.

3. The Security Procedures

The following procedures apply unless the Client has varied an item marked "Variable" by a written opt-out under section 4.

No.	Procedure	Variable?
1	**Portal login with two-factor authentication.** Every Authorised User signs in to the Portal with their own login and two-factor authentication using an authenticator app, or another method the Company approves that is at least as secure. SMS codes are never used as the second factor for individual clients.	No
2	**Authorised Users only.** Instructions are accepted only from Authorised Users, on the telephone numbers, email addresses and messaging accounts registered in the Mandate.	No
3	**New beneficiaries and changes to bank or wallet details.** These are accepted only through the Portal or after a call-back by the Company to a telephone number in the Mandate, and are confirmed on a different channel from the one on which the request was made, never on the same one. A request made in the Portal is confirmed by call-back; a request made by email or messaging app is confirmed in the Portal or by call-back; a request made by phone is confirmed in the Portal.	Yes: same-channel or faster confirmation

No.	Procedure	Variable?
4	**Call-back on larger instructions outside the Portal.** Before acting on any instruction given outside the Portal (WhatsApp, Telegram, email or phone) that, together with other such instructions to the same payee in the previous 24 hours, exceeds USD 50,000 (or its equivalent), the Company calls back a telephone number in the Mandate.	Yes: same-channel confirmation
5	**Wallet cooling-off.** Before the first use of a new Registered Wallet: 2 hours if nothing in the account's security details (for example Authorised Users, registered numbers or emails, messaging accounts or two-factor authentication devices) changed in the previous 7 days; otherwise 24 hours.	Yes: shorter cooling-off
6	**Notification.** Every Authorised User is notified of a new beneficiary or a change to bank or wallet details, and can block it. For an individual Client aged 60 or over who has nominated a Trusted Contact, the Trusted Contact is told too. A Trusted Contact has no authority over the account.	No
7	**Changes to Authorised Users and registered details.** A change of Authorised Users, registered telephone numbers, email addresses or messaging accounts needs a signed update to the Mandate, a call-back to the previously registered number, and a 24-hour hold before it takes effect.	No
8	**Wallet controls and risk checks.** Every wallet address is screened with blockchain analytics before the first withdrawal to it, and the Client may be asked to prove control of a wallet it holds itself (by a signed message or a small test payment). There are no standard test-payment or dual-approval requirements. The Company may apply an extra check, hold, test or second approval to a particular instruction where its risk controls require it.	No

3.1 **How a call-back works.** The Company calls a telephone number registered in the Mandate, never a number given in the request, and asks the Authorised User to confirm the instruction or change. It never asks for a password, code or key. If it cannot complete the call-back, it does not act. A call-back may delay an instruction, and the Company is not responsible for that delay.

3.2 **Enterprise Firms.** Where an Enterprise Firm acts for the Client under an Operator Authority, a new beneficiary proposed by the Firm takes effect only after the Client approves it itself in the Portal and the Company completes a call-back to the Client's own registered number, never the Firm's.

3.3 **Scam-prevention steps.** Where the Company is concerned that an instruction may be the result of a scam, it may pause it, contact the Client, give a warning or ask questions before acting. For a Vulnerable Client, the pause is at least 24 hours and may be extended to 72 hours.

3.4 **Trading API.** Instructions given through the Trading API must also meet the security requirements in the API Terms. For the purposes of procedure 4, an instruction given through the Trading API is an instruction given outside the Portal.

4. The Client's choices: written opt-out

4.1 The Company has offered the Client the Security Procedures in the Security Procedures Schedule. The Client may opt, in writing, for confirmation on the same channel or for faster confirmation than those procedures provide. If it does, the Client bears the risk of any loss that the procedure it declined would have prevented.

4.2 An opt-out may vary only the items marked "Variable" in section 3. It is made on the form in the Annex, signed by an authorised signatory (or by the Client, if an individual), and takes effect when the Company confirms it in writing. The Client may withdraw an opt-out at any time by written notice. The Company may decline an opt-out, or end one on notice, where it considers it unsafe.

4.3 **Instructions bound by an opt-out.** If the Client opts out under this section, it expressly agrees to be bound by any instruction, whether or not it authorised it, that the Company accepts in good faith and in compliance with the procedure the Client chose.

4.4 The Annex records which procedures the Client accepted and any written opt-out. If no variation is recorded, every procedure in section 3 applies.

5. Authorisation and losses

5.1 **Commercial reasonableness.** The Client agrees that the Security Procedures, as accepted by it or varied by its written opt-out, are commercially reasonable for it, having regard to the size, type and frequency of its instructions.

5.2 **Deemed authorisation.** An instruction given through the Portal after login with two-factor authentication is treated as authorised by the Client if the Company acted on it in good faith and in compliance with the Security Procedures, whether or not the Client in fact authorised it, unless the Client proves that it was not caused, directly or indirectly, by a person entrusted by the Client or a person who obtained access to the Client's devices, credentials or channels.

5.3 Deemed authorisation never covers a loss caused by the Company's own systems.

5.3A An instruction given through the Trading API is treated as authorised by the Client as set out in the API Terms.

5.4 **Who bears a loss.** For a loss caused by an instruction or change that the Client did not authorise, or that the Client was tricked into authorising, the Company is responsible only where (a) the Company did not follow the Security Procedures or a scam-prevention step it had triggered, or (b) the Company's own systems or staff caused the loss. Otherwise the Client bears it.

5.5 If the Client is tricked into authorising a payment, the Company will try to recall it and will not charge a recall fee. A recall cannot be guaranteed.

5.6 If the Client is an individual, nothing in this Schedule removes or limits the Client's Mandatory Rights.

6. The Client's responsibilities

6.1 The Client must tell the Company at once if it suspects that any device, credential, email or messaging account used with the Services has been compromised.

6.2 The Client must:

(a) make sure that each Authorised User keeps their login, authenticator device and any API credentials to themselves, and never shares them, including with an Enterprise Firm;

(b) keep its devices, email and messaging accounts secure, and keep the Mandate up to date;

(c) remove an Authorised User's access on the day they leave or no longer need it;

(d) check every notification of a new beneficiary or changed details, and block any it does not recognise at once; and

(e) check a new or changed payee on a separate, known channel before paying it.

7. Changes

7.1 The Company may change these Security Procedures on the notice set out in the Client Agreement. It may strengthen them with immediate effect where security requires, and tells the Client as soon as it can.

Annex: Record of Security Procedures and written opt-out

Client	[CLIENT LEGAL NAME]
Client reference	[CLIENT REFERENCE]
Date	[DATE]

No.	Procedure	Default accepted	Variation requested (Variable items only)
1	Portal login with two-factor authentication	☒ Applies	Not variable
2	Authorised Users only	☒ Applies	Not variable
3	Different-channel confirmation of new beneficiaries and changed details	☐ Accepted	☐ Same-channel confirmation ☐ Faster confirmation: _____
4	Call-back on instructions outside the Portal over USD 50,000 per payee in 24 hours	☐ Accepted	☐ Same-channel confirmation
5	Wallet cooling-off (2 hours, or 24 hours after a security change)	☐ Accepted	☐ Shorter cooling-off: _____
6	Notification to Authorised Users (and any Trusted Contact)	☒ Applies	Not variable
7	Changes to Authorised Users and registered details	☒ Applies	Not variable
8	Wallet controls and risk checks	☒ Applies	Not variable

> **If you request any variation:** "The Company has offered the Client the Security Procedures in the Security Procedures Schedule. The Client may opt, in writing, for confirmation on the same channel or for faster confirmation than those procedures provide. If it does, the Client bears the risk of any loss that the procedure it declined would have prevented." The Client expressly agrees to be bound by any instruction, whether or not it authorised it, that the Company accepts in good faith and in compliance with the procedure the Client chose. The Client also agrees that the Security Procedures, as varied by this opt-out, are commercially reasonable for it, having regard to the size, type and frequency of its instructions.

For the Client

Name: _____

Title (companies): _____

Signature: _____

Date: _____

Confirmed for Flumen Pay LLC, trading as Lydiam Group

Name: [NAME]

Role: [ROLE]

Date: [DATE]

Opt-out effective from: [DATE]