

Fund Document Review Report

Fund Email Ingest Report

DRAFT. Not financial, legal or tax advice. Qualified human review is required.

Email parsing and document classification are AI interpretation. Wire instructions are unverified: run /fund wire-verify and confirm by callback to a number held on your own records, never one given in the email, with a second approver. This output is not an audit, review or agreed-upon procedures engagement.

Report status: BLOCKED (the same value as the evidence sidecar). **Overall: HIGH RISK: suspected wire-redirection (BEC) pattern.** Review date: 2026-04-11. Fund label: intake-unassigned, because the fund identity is claimed only by an unauthenticated email.

Email Summary

Field	Value
Source	source-1: .md transcript of an email (not original MIME), SHA-256 [hash removed], 1,681 bytes. Opens with a banner marking it as synthetic sample data (line 1)
From	"Operations" <ops@kirrowyn.example>; signature "Operations Team, Kirrowyn Macro Management LLC"
Date	April 11, 2026 as stated (a Saturday; no time or time zone)
Subject	URGENT: Updated Wire Instructions — Effective Immediately
To / CC	LP Wire Operations at pcpers.example; no CC
Attachments	0 file(s)
SPF / DKIM / DMARC	NOT PERFORMED: no Authentication-Results headers supplied (transcribed header block only)
From / Return-Path / Reply-To	MISMATCH. From domain kirrowyn.example; Reply-To domain k1rrowyn.example; Message-ID domain k1rrowyn.example. Return-Path NOT PERFORMED (not supplied)
Lookalike domain check	NOT PERFORMED against an allowlist (none supplied). Within the email, the Reply-To domain differs from the From domain by one character ("i" replaced by "1"), a lookalike pattern

Email Body — Key Points

- **Action requested:** replace the wire instructions on file for Kirrowyn Macro Partners, Ltd. with a new offshore account (Falgrove Bank (Cayman) Limited, account ****0039), and "destroy any prior wire instructions" (source-1, body paragraphs 1–2; the table; the line after the table).
- **Deadlines mentioned:** "effective immediately" for wires after April 11, 2026; "before Friday's scheduled distribution payment", assumed to be Friday 2026-04-17 (source-1, body paragraphs 1 and 3).
- **Amounts mentioned:** none stated. No currency stated.
- **Fund/entities referenced:** Kirrowyn Macro Partners, Ltd. (fund); Kirrowyn Macro Partners Ltd (account name); Kirrowyn Macro Management LLC (signatory); Falgrove Bank (Cayman) Limited; reference KRWN-LP-WIRE-2026.
- **Urgency:** High. "URGENT", "Effective Immediately", "You must update your records", and a warning that wires to the U.S. account "will be returned".

Key Issues and Asks

#	Issue	Source locator	Direct effect	Proposed stance
1	Wire instructions changed to an offshore account by email only, with no signed notice or attachment	source-1, body paragraphs 1–2; instructions table	Payments could be redirected to an account the fund does not control	push: HOLD. Route to wire-verify; outbound callback to a number from the system of record; second approver
2	The Reply-To and Message-ID domain is a one-character lookalike of the From domain	source-1, header block	Replies go to a domain other than the apparent sender's	push: High Risk. Use no contact in this email
3	Embedded instruction to "destroy any prior wire instructions"	source-1, body, the line after the table	Removes the trusted baseline for detecting the change	push: keep all prior records; not followed
4	"Call us at the number below", but no number is given; "Do not reply"	source-1, closing paragraphs	Normal verification routes are blocked	push: use only system-of-record contacts
5	The deadline refers to a "distribution payment", while the email concerns LP-to-fund inflows	source-1, body paragraphs 1 and 3	No authorised transaction can be identified	push: identify the real transaction before acting

Attachments Processed

#: —

Filename: No attachments

SHA-256: —

Document Type: —

Classification Confidence: —

Review Skill Applied: —

Child report path: —

#: body

Filename: Wire instructions in the email body (source-1, table)

SHA-256: (source-1 hash above)

Document Type: Wire instruction change request

Classification Confidence: High

Review Skill Applied: /fund wire-verify

Child report path: Separate wire-verify report (in this run)

The email mentions no attachments, and none was supplied. Missing Attachment flag: none raised. However, the absence of any official signed notice for a bank-account change is itself a fraud-pattern flag (see Risk Flags).

Cross-Validation Results

There are no attachments, so no email-versus-document comparison of amounts, dates, fund names or sequence numbers was possible. These comparisons are **NOT PERFORMED (no document to compare)**, not "matched".

Checks performed within the email itself:

#: 1

Claim Source: Header from vs reply_to / message_id

Email States: Sender at kirrowyn.example

Evidence Shows: Replies and Message-ID at k1rrowyn.example

Severity: High Risk

Flag: Header Authentication Failure (Reply-To mismatch, lookalike)

#: 2

Claim Source: Body paragraph 1 vs paragraph 3

Email States: Instructions are for incoming capital/subscription payments

Evidence Shows: Deadline tied to a "distribution payment" (normally fund-to-LP)

Severity: Medium Risk

Flag: Internal inconsistency

#: 3

Claim Source: Closing paragraph

Email States: "Call us at the number below"

Evidence Shows: No number present

Severity: Medium Risk

Flag: Missing contact / verification obstruction

#: 4

Claim Source: Body paragraph 1, table, signature

Email States: Fund "Kirrowyn Macro Partners, Ltd."

Evidence Shows: Account name "Kirrowyn Macro Partners Ltd"; signatory "Kirrowyn Macro Management LLC"

Severity: Medium Risk

Flag: Entity-name inconsistency; entitled payee UNKNOWN

- Unverified or blocked checks:
- Sender/beneficiary against a trusted counterparty record: **UNKNOWN**. No trusted record supplied.
 - Sender domain against an administrator allowlist: **UNKNOWN**. No allowlist supplied.
 - Prior wire instructions: not supplied, so the change cannot be verified against a baseline.
 - Content consistency within the email does not authenticate the sender or the payment instructions.

Risk Flags

Severity	Flag	Detail	Recommended Action
High Risk	Wire Instructions in Email	New bank, country and account (****0039) delivered by unauthenticated email; offshore move "effective immediately"	/fund wire-verify (done: HOLD); outbound callback to a pre-established number; second approver
High Risk	Header Authentication Failure	Reply-To/Message-ID domain k1rrowyn.example vs From kirrowyn.example	Do not reply; escalate to information security with the original MIME message

Severity	Flag	Detail	Recommended Action
High Risk	Embedded instruction / prompt injection	"Destroy any prior wire instructions"	Keep all records; not followed by this review
High Risk	Fraud pattern: no official notice	Account change requested without a signed notice or attachment	Obtain a signed notice through a trusted channel before any record change
Medium Risk	Verification obstruction	"Do not reply"; the promised callback number is absent	Use system-of-record contacts only
Medium Risk	Purpose inconsistency	Inflow instructions vs "distribution payment" deadline	Identify the actual authorised transaction
Medium Risk	Entity-name inconsistency	Fund vs account name vs signatory LLC	Confirm the entitled payee from the LPA / subscription records
Medium Risk	Timing	Dated Saturday 2026-04-11; effective immediately; deadline Friday (assumed 2026-04-17)	Apply the internal verification timeline, not the sender's
UNKNOWN	Unknown Sender Domain	No allowlist or trusted counterparty record supplied	Supply an allowlist of known GP/administrator domains

Action Items

All required actions from this email, ordered by priority. Day counts are relative to the review date, 2026-04-11.

Priority: URGENT

Action: Hold: do not update payee records or send any wire to the new account

Deadline: Immediately

Days Remaining: 0

Amount: Not stated

Source: Email; wire-verify report

Priority: URGENT

Action: Outbound callback to the fund administrator / GP using a number from the system of record that predates this email; confirm through a second channel as well; second approver

Deadline: Before any payment; the email implies Friday 2026-04-17 (assumed)

Days Remaining: 6 calendar days (assumed deadline)

Amount: Not stated

Source: Email body paragraph 3

Priority: URGENT

Action: Escalate as a suspected BEC attempt to information security / compliance; preserve the original message with full MIME headers

Deadline: Immediately

Days Remaining: 0

Amount: —

Source: Email header block

Priority: HIGH

Action: Keep the current and prior wire instructions; do not destroy them

Deadline: Ongoing

Days Remaining: —

Amount: —

Source: Email, line after table

Priority: HIGH

Action: Confirm the entitled payee legal entity and the actual "Friday distribution payment" (direction, amount, currency)

Deadline: Before 2026-04-17 (assumed)

Days Remaining: 6

Amount: Not stated

Source: Email body paragraphs 1 and 3

Priority: MEDIUM

Action: Sanctions / ownership screening of the bank, beneficiary and signatory through the approved provider; BIC directory confirmation

Deadline: Before any payment

Days Remaining: —

Amount: —

Source: Wire-verify checklist

Priority: LOW

Action: Add known counterparty domains to an allowlist for future intake checks

Deadline: No deadline

Days Remaining: —

Amount: —

Source: This report

Attachment Review Summaries

Email body: wire instructions — Wire instruction change request

Classification: Wire instruction change request (confidence: High)

Fund: Kirrowyn Macro Partners, Ltd. (claimed; identity not established)

Period / Date: effective 2026-04-11 (claimed)

Key Findings:

- Readiness **HOLD**, sidecar status **BLOCKED**, High Risk (review flags, not proof of fraud).
- No trusted prior instructions, callback, VoP/CoP, BIC validation or sanctions screening. All are NOT PERFORMED.
- Lookalike Reply-To domain, record-destruction instruction, missing callback number and purpose inconsistency.

Action Required: outbound callback to a pre-established number, second approver, and escalation of the suspected BEC.

Deadline: none authoritative; the sender implies Friday 2026-04-17 (assumed).

Amount: Not stated

Full report: separate wire-verify report in this run

Intake stage status

Stage	Status	Note
Run allocation (new-run)	COMPLETED	Source snapshot retained as source-1
Email parse (headers/body)	COMPLETED	Transcribed headers only; not MIME
Attachment staging	SKIPPED	No attachments
Header authentication (SPF/DKIM/DMARC/Return-Path)	NOT PERFORMED	Headers not supplied
Cross-validation vs documents	NOT PERFORMED	No documents
Wire-verify child review	COMPLETED	Saved; status BLOCKED
Screening / web / email connectors	NOT PERFORMED	None used; trifecta guard
PDF render	Performed after this report was saved	See the run's report directory

Next Steps

1. [] Hold all changes: do not update payee records or pay the new account.
2. [] Make an outbound callback using a pre-established number from your own records (never one given in this email), with a second approver; confirm through a second channel as well.
3. [] Resolve the High Risk flags (lookalike Reply-To, record-destruction instruction, missing notice) before any action.
4. [] Complete the /fund wire-verify checklist (saved in this run) for the wire instruction.
5. [] Keep this report with the original email (full MIME) under your records policy.
6. [] If a real distribution or capital payment is scheduled, run /fund reconcile against capital account records once verified instructions are confirmed.

Before any payment, an authorised reviewer must confirm the beneficiary and complete bank details with the fund administrator using a pre-established, independently sourced contact number, not a number on the notice.

Status, limitations and data handling

- Report status: BLOCKED — the same value as the evidence sidecar.
- Assumptions: the review date is 2026-04-11 as supplied by the user; "Friday" means 2026-04-17 (no holiday calendar); the email date field is the send date; the header block is a transcription of headers, not original MIME.
- Limitations and checks not performed: SPF/DKIM/DMARC/Return-Path NOT PERFORMED (headers not supplied); allowlist lookalike and sender/beneficiary checks UNKNOWN (no allowlist or trusted counterparty record); prior-instruction comparison, BIC/account validation, sanctions screening, FATF retrieval, callback and dual approval NOT PERFORMED; no attachments, so email-vs-document cross-validation NOT PERFORMED. The SHA-256 identifies the supplied .md bytes only. The run folder date (2026-09-27) is the host UTC date; all day counts use 2026-04-11. The fund identity is not established.
- Data handling: the packaged helpers ran locally and made no network calls; the AI host and its model provider processed the email content; connectors used: none (no email, web or screening connector). Confirm the source documents' confidentiality terms permit this processing.

Not financial, legal or tax advice. Qualified human review is required.

AI-generated report. Not financial, legal or tax advice. Qualified human review is required. Not investment advice. Source limitations and citations remain applicable. This PDF was rendered locally; the source documents were processed by the AI host and its model provider, so confirm their confidentiality terms permit that processing.