www.capillarytech.com

Date: October 31, 2026

To,
BSE Limited
Listing Department
Phiroze JeeJeebhoy Towers, Dalal Street Fort, Mumbai -400001
Scrip Code: 544614

To,
National Stock Exchange of India Limited
Listing Department
Exchange Plaza , Bandra Kurla Complex
Bandra (East), Mumbai -4000051
Symbol: CAPILLARY

Dear Sir/Madam,

Subject: Disclosure under Regulation 30 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 read with Para A of Part A of Schedule III –Forensic Audit Report and its summary

Dear Sir/Madam,

This is further to our letter dated July 31, 2026, in which the Company informed you of the initiation of a forensic audit by KPMG in connection with the cyber-enabled banking fraud incident at a step-down subsidiary of the Company.

Pursuant to Regulation 30 read with sub-clause 17(b) of Para A of Part A of Schedule III of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI Listing Regulations"), we wish to inform you that the Company received the forensic report from KPMG on October 30, 2026 and brief summary of the report is:

The forensic investigation by KPMG Česká republika, s.r.o. report establishes that the incident was a fraud carried out by external parties who impersonated a senior executive and an outside lawyer using a look-alike email domain and off-channel communications. Furthermore, the report establishes that there was no traditional email spoofing, forged use of the Company's real domain, malware, endpoint compromise, mailbox compromise, account takeover, or unauthorised access to the Company's systems, devices, or email accounts. It also establishes the absence of questioned employee involvement or wrong doing on their part or any technical compromise, while confirming that the Company has further strengthened its payment controls and is actively pursuing recovery and legal remedies.

This intimation will also be made available on the website of the Company and can be accessed using the below link: https://www.capillarytech.com/investors/shareholder-information/corporate-announcements/2026-27/

We request you to take the above information on records.

Yours faithfully,

For Capillary Technologies India Limited

GIREDDY BHARGAVI REDDY
Digitally signed by GIREDDY BHARGAVI REDDY
Date: 2026.10.31 11:44:20 +05'30'

Gireddy Bhargavi Reddy
Company Secretary and Compliance Officer
Membership No. A17091
Place: Bengaluru

Project Cluewire

Executive Summary and Management Report

Suspected payment-diversion fraud affecting Session M Czech Republic s.r.o.

Prepared for Capillary Technologies India Limited

Classification: KPMG Confidential
Date: October 2026

1. Purpose and reporting basis

This management report distils the principal findings, open matters, business implications and immediate actions arising from the draft forensic report prepared by KPMG Česká republika, s.r.o. The summary is intended for Capillary Technologies India Limited management, Legal, Risk, Finance and Security stakeholders. It does not replace the detailed forensic report, evidence register or technical annexures.

The report concerns four disputed payments totaling EUR 3,041,169.90 executed from Session M Czech Republic s.r.o. between 26 June 2026 and 2 July 2026. The investigation reviewed two forensic laptop images, mailbox and authentication records, communications, transaction documentation, Google Workspace-related logs, Google Takeout exports and open-source intelligence material.

2. Executive incident synopsis

The available evidence is most consistent with a multi-stage payment-diversion fraud based on executive and legal-professional impersonation, social engineering, a lookalike domain and off-channel communications. The communications presented a purported confidential acquisition transaction and were supported by an NDA, invoices, payment requests, beneficiary banking details and payment confirmations.

The reviewed evidence does not support a finding that malware, endpoint compromise, corporate mailbox compromise, successful unauthorized access or traditional email spoofing caused the payments. Relevant emails were sent from an operational lookalike domain, law-ogier.co.uk, rather than through forged infrastructure purporting to be the legitimate ogier.com domain. The use of deepfake voice or video remains an allegation that could neither be substantiated nor refuted because original audio, video, telecommunications metadata and mobile-device artefacts were not available.

3. Key facts for management

Area	Management position
Financial impact	Four disputed foreign payments totalling EUR 3,041,169.90 were identified.
Payment route	Three payments were made to ZZDJB CO LIMITED at HSBC Hong Kong and one payment to ZHONGXIAN TRADING PTE. LTD at UOB Singapore.
Primary mechanism	Executive and external-lawyer impersonation, confidentiality/urgency pressure, WhatsApp and personal email, supported by formal-looking transaction documents.
Endpoints	No incident-related malware, unauthorized remote-access tools, persistence, credential theft utilities or malicious scripts were identified on the two reviewed laptops.
Mailboxes / identity	No evidence of successful unauthorized mailbox access, malicious forwarding, mailbox-rule manipulation or account takeover was identified in the supplied records.
Email infrastructure	No traditional spoofing was identified. The reviewed messages passed available SPF/DKIM checks for the lookalike sending domain.
Deepfake allegation	Not technically determined because original mobile, audio/video, call metadata and telecommunications evidence were unavailable.
Fund tracing	The first-hop payments are evidenced. Ultimate onward movement, beneficial ownership, beneficiary-bank intelligence and recovery are outside the current forensic scope.

4. Hypothesis assessment

Hypothesis	Current assessment	Management interpretation
H1 Deepfake-assisted impersonation	Unable to substantiate or refute	Treat as an unverified allegation; strengthen

		executive verification regardless.
H2 Email impersonation / spoofing	Lookalike-domain impersonation supported; traditional spoofing not identified	Email authentication alone does not establish legitimacy of the underlying sender or business instruction.
H3 Mailbox / account compromise	Not supported by evidence reviewed	No corporate account-compromise root cause identified from supplied records.
H4 Endpoint involvement	Not supported by evidence reviewed	No endpoint-compromise root cause identified on the two reviewed laptops.
H5 Multiple-beneficiary fund diversion	Supported	First-hop fund diversion is established from transaction and banking records; onward tracing requires separate action.

5. Management implications

- Primary business risk is not presently evidenced as technical compromise of corporate endpoints or mailboxes. It is the ability of external personas to exploit authority, secrecy, urgency, non-standard channels and formal-looking documents to induce authorized payment activity.
- The circumstances surrounding the disputed transactions suggest that confidential, time-sensitive transaction requests may warrant enhanced scrutiny and verification. Management may consider assessing whether existing beneficiary-validation, callback, escalation, treasury, and approval processes provide sufficient assurance for high-value transactions involving newly introduced counterparties.
- The use of personal email accounts and WhatsApp reduced organizational visibility and limited the availability of native evidentiary records. Consideration should be given to implementing independent verification procedures for executive payment requests and transaction approvals, particularly where instructions are communicated through personal email accounts, voice or video calls, caller identification, profile images, or messaging platforms outside established corporate channels.
- Information about organizational roles, approval patterns and payment processes may have been obtained through public information, prior interaction, exposed documents or other sources. The present report does not establish the source of that knowledge or insider involvement.
- The absence of identified compromise is limited to the artefacts and records reviewed. It should not be presented as proof that compromise was impossible or never occurred.

6. Critical limitations for management reliance

- No forensic acquisition of the personal mobile device(s) used for WhatsApp communications was undertaken.
- No original audio/video, call-detail records, telecommunications metadata or native call artefacts were available; deepfake use was therefore not technically determined.
- Complete VPN, network, proxy, firewall, packet-capture, memory and some endpoint-security backend telemetry were unavailable.
- Complete bank-portal audit trails, maker-checker records, workflow logs and approval timestamps were unavailable; the end-to-end approval process was not independently validated.
- Slack logs were unavailable; communications occurring solely on unavailable channels could not be assessed.
- OSINT attribution is contextual and not proof of identity, ownership, control or responsibility.
- The financial review established first-hop payments from supplied records, not onward movement, beneficial ownership or recovery status.
- No attribution to a specific individual, group or threat actor was established.
- No statutory audit, legal opinion, compliance certification or criminal-liability assessment was performed.
- Absence of identified compromise is not definitive proof of absence; conclusions remain bounded by the evidence supplied and review period.

7. Recommended management conclusion

Subject to the limitations above, the evidence reviewed is most consistent with a payment-diversion fraud executed through executive and legal-professional impersonation, social engineering, a lookalike domain and off-channel communications. The available evidence does not support a technical-compromise explanation for the two reviewed endpoints or corporate accounts. The potential use of deepfake technology remains unverified due to the absence of native audio, video, and telecommunications evidence. Additionally, a definitive assessment of the effectiveness of payment-governance, beneficiary-validation, and approval-control processes could not be performed because the underlying workflow records, approval logs, and bank-portal audit evidence were not available for review.

8. Use restriction

This summary is prepared for internal management and legal review by Capillary Technologies India Limited. It is derived from the main forensic report and should be read with that report, its evidence register, annexures, assumptions and limitations. It should not be used as a standalone expert report, legal opinion, disciplinary finding, criminal attribution, insurance proof of loss or third-party assurance without approval from the issuing KPMG member firm and relevant legal counsel.



Maroš Holodňák, partner
Proxy holder authorized to act individually