

Hong Kong Exchange
Limited take no
representation as
whatsoever for a
part of the conte



Hepalink

HEPALINK PHARMACEUTICAL GROUP CO., LTD.
(深圳市海普瑞藥業集團股份有限公司)

(A joint stock company incorporated in the People's Republic of China with limited liability)

(H.K. S.E.C. Code: 9989)

INSIDE INFORMATION ANNOUNCEMENT RESULTS OF INDEPENDENT THIRD PART INVESTIGATION

This announcement is made by Shenzhen Hepalink Pharmaceutical Group Co., Ltd. (the "Company") pursuant to the Independent Information Provisions of Part XIVA of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and Rule 13.09(2)(a) of the Rules Governing the Listing of Securities of The Stock Exchange of Hong Kong Limited.

FORMATION OF SPECIAL INVESTIGATION GROUP

Reference is made to the telecommunication fax dated and disclosed in the independent information announcement of the Company dated 15 January 2024, 30 January 2024 and 15 March 2024 (the "Form F").

The Company established an independent third-party investigation group (the "Special Investigation Group") on 30 January 2024. The Special Investigation Group, led by the Company's independent non-executive director, engaged a reputable and all leading fee independent investigation team (the "Investigation Team") to conduct a independent fee independent investigation, in collaboration with a reputable Italian law firm, in the Telecommunication Fax Disclosure conducted by the Company's wholly-owned subsidiary Techd Pharma Ital S.R.L. ("Techd Pharma Ital") (the "Investigation").

On 26 March 2024, the Investigative Team delivered a investigative report to the Special Investigative Group (the RFR). The elements of the investigation are as follows:

I. BACKGROUND OF THE INVESTIGATION

As disclosed in the information memorandum of the Company dated 15 January 2024, Techdata is a wholly owned subsidiary of the Italian telecommunications giant, with a market value of approximately 11.7 billion euros. After the Telecom Fraud Incident, the Company retained the Italian license of the Shareholding Municipal Public Security Bureau of the Company's legal risk management team, hired a law firm and established the Special Investigative Group led by the Company's independent director-elect, which engaged the Investigative Team to conduct the investigation in collaboration with a consulting firm.

II. SCOPE OF THE INVESTIGATION

The investigation included the following elements:

1. Obtain and review the elements of the records, including communications with legal advisors and related to the Telecom Fraud Incident; the license and related management records of the Company and Techdata; basic information of the company and its subsidiaries (such as organizational chart and list of employees); and the activities related to the Telecom Fraud Incident, including but not limited to (1) specific bank accounts held and their activities records; (2) records of financial ledger; (3) annual records of electronic financial data and logs of transactions; (4) internal deletion of investigation records regarding the Telecom Fraud Incident; (5) the Company's badminton telecommunications records; and (6) the deletion records of the Telecom Fraud Incident records if the latter;
2. Conduct interviews with the employees of the Company and Techdata who were involved in the Telecom Fraud Incident to gain a detailed understanding of the Telecom Fraud Incident's specifics, including the background, chronological sequence of events, causes and the Telecom Fraud Incident's overall impact on the company and its subsidiaries;

3. Conducting checks on the electronic and financial data available, including: 1) data available from Techdata Italia's financial data dig the relevant information timeframe; 2) data available from bank accounts associated with the Telecom Fixed Income; 3) available from dig the eid form 1 June 2023 to 31 December 2023, identifying the employee who registered the bank account of Techdata Italia from the electronic (check the identification of the employee, and the time and amount of the transaction); 4) amount made by Techdata Italia dig the eid form 1 June 2023 to 31 December 2023 and identifying the check amount, including but not limited to the amount, interest and cost;
4. Conducting background checks on all parties involved in the Telecom Fixed Income, including but not limited to the trustee and their company registration information directly or indirectly identifying potential relationships between them and the management and/or employees of Techdata Italia; additionally, investigate the email address of the email domain used by the trustee of the Telecom Fixed Income; and
5. Conducting electronic forensic on the Company's email account, network, and mobile devices of the Techdata Italia employees related to the Telecom Fixed Income, and the relevant electronic communication records, which forensic activities include 1) creating electronic forensic data mirror image and back up; and 2) extracting information. Little known has been revealed, and a forensic investigation of the identified domain has been conducted after a long time period in each.

III. KEY FINDINGS OF THE INVESTIGATION

(1) Criminal Team Profile

According to the interview with the management and recorded IT data, the general manager of Techdata Italia received an email on 13 December 2023 from a fixed trustee who stated to be his employee. The trustee invited him to a virtual confidential meeting (the **Agreement**) and maintain strict confidentiality to prevent information leakage. From 13 December 2023 to 3 January 2024, he received multiple forwarded information from the trustee and aggregated a total of approximately 11.7 million with a weekly average of approximately 1 million from the Company (the **Profile**).

After interviewing the general manager, it was determined that he did not disclose the Paymental information to the effect that the Accountant should be kept strictly confidential and any information leakage could implicate the interest and commitment in the market. On 13 December 2023, the effect allowed the general manager to sign a confidentiality agreement and instructed him to handle the Paymental and keep it confidential until the Accountant was arrested. During the aforementioned period, the general manager took multiple actions to ensure the effect's identity was not discovered.

The Investigation Team identified the main reason for the failure of the management of Tech Digital and the Company to detect the abnormality in financial statements:

- (i) the finance manager of Tech Digital had limited bank account management authority and was unable to check the bank account balance after the general manager removed the USB-key; and
- (ii) the Company's head accountant could not obtain the account balance from the local staff before signing them to email the electronic financial statements a week and the last working day of each month.

During the Investigation, the Investigation Team traced the information of the electronic statements in the Telecom Fraud Incident (the **PTCCM**). The Investigation Team conducted background checks on the Paymental and committed their management's agreement with the Company's employees, finding the relevant information. The Investigation Team also reached electronically for key information about the Paymental information and their electronic data access, but found electronic data about them from their staff, except for their name and signature and the detailed address communication related to the Telecom Fraud Incident. Based on the digital forensic work of the Investigation Team, connections were found between the Telecom Fraud Incident and the individual associated with Tech Digital, the employee of the Company.

(2) Immunity of the Company's Internal Financial Information

After the Telecom Fraud Incident, the Company took a series of measures to improve its internal control. The Company collaborated with bank to enforce strict policies for checking bank account balance and controlling the USB-key. The Company's IT department also implemented a data audit of the Company's internal information security and capabilities, and implemented full-time measures to check the email records.

After reviewing the Report, the Special Investigator Group found the content to be detailed and meticulous, accurately reflecting the course of the Telecom Fraud Incident. The Special Investigator Group recommended the board of directors of the Company (the Board) to adopt the findings of the Report and act effectively to eliminate the legal responsibility of the company. At the same time, the Company should act effectively to check and eliminate the impact of the Telecom Fraud Incident and effectively safeguard the interests of the Company and its shareholders.

VI. OPINIONS OF THE BOARD

After reviewing the Report and the recommendations of the Special Investigator Group, the Board of the Company is satisfied with the effective implementation of the measures that the Company has initiated earlier, including but not limited to:

1. Enriching the business cooperation with the domestic and overseas subsidiaries of the Company (the Group) to identify major risks; date and have the internal control of the Company and its subsidiaries based on the risk of the risk assessment, the definition and effective key business processes and business processes of the internal control; based on the business operation and risk assessment, combined with information technology, have the control of the digital measures at both the Company level and the business level, and establish a data data internal control;
2. Rectify the internal control of the company's internal control, and improve the internal control of the company's internal control; effectively implement the internal control system; effectively improve the internal control of the Company; improve the health and stability of the internal control of the Company; improve the ability of all domestic and overseas employees to effectively deal with risks;
3. Improve the Company's internal control and flight internal control;

