

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)

(Tel: 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 identification memorandum of the Commission dated 15 January 2024, Techdata is a well-established telecommunications provider in the UK. After the Telecom Fraud Incident, the Commission established the Italian Liaison Office of the Serious Fraud Office (SFO) of the Commission. The SFO's legal and technical team, headed by the former head of the Special Investigative Group led by the Commission's independent electronic director, engaged the Investigative Team to conduct the investigation in collaboration with a specialised Italian firm.

II. SCOPE OF THE INVESTIGATION

The investigation included the following elements:

1. Obtaining and reviewing the element of metadata and records, including communications with legal bodies and metadata related to the Telecom Fraud Incident; the liaison office related management process of the Commission and Techdata; basic information of the company including (such as registration and list of employees); and a detailed metadata related to the Telecom Fraud Incident, including but not limited to (1) specific bank accounts held and their transaction records; (2) record of financial ledger; (3) annual record of electronic financial statement of the company; (4) internal deletion of investigation related to the Telecom Fraud Incident; (5) the Commission's badminton telecommunications records; and (6) the deletion of the Telecom Fraud Incident related to the Italian;
2. Conducting interviews with the element of the Commission and Techdata which included the Telecom Fraud Incident related to the detailed details of the Telecom Fraud Incident's specific, including the background, chronological sequence, cause and effect of the Telecom Fraud Incident as well as the cause and effect behind the all cases involved;

3. Conducting checks on the electronic and financial data available, including: 1) data available from Techdata Italia's financial data dig the relevant information time frame; 2) data available from bank accounts associated with the Telecom Fixed Income; 3) available data 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 dig the document, including but not limited to the amount, the date and contact;
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, check each record of the amount of the email domain used by the recipient of the Telecom Fixed Income; and
5. Conducting electronic forensic on the Company's email account, check the mobile device of the Techdata Italia employee related to the Telecom Fixed Income, and the electronic communication records, check electronic activities including 1) creating electronic forensic data mirroring and back up; and 2) extracting information. Little known has been revealed, and a forensic review of the identified document 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 income trustee who stated to be his superior. The recipient invited him to a virtual confidential meeting (the **Account**) 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 per day in the Company (the **Profile**).

After interviewing the general manager, it was determined that he did not disclose the Paymental activities 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 give a confidential 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 cause of the failure of the management of Tech Digital and the Company to detect the abnormality in financial matters:

- (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 office could not obtain the account balance from the local staff before giving them to email the electronic information once a week and the last working day of each month.

During the Investigation, the Investigation Team traced the information of the electronic communication in the Telecom Fraud Incident (the **PFICM**). The Investigation Team conducted background check on the Paymental activities and management's communication with the Company's employees, finding the following. The Investigation Team also reached electronically for key information about the Paymental activities and their electronic data records, but found electronic data about them from their staff, except for their communication details and communication related to the Telecom Fraud Incident. Based on the digital forensic work of the Investigation Team, connections are found between the Telecom Fraud Incident and the individual associated with Tech Digital and the employees of the Company.

(2) Immediate Company's Internal Control Measures

After the Telecom Fraud Incident, the Company took immediate measures to improve 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 enhanced a data audit of the Company's electronic 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 in implementation of the relevant recommendations therein. At the same time, the Company is urged to act in implementation of the relevant recommendations, to 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 content and effectiveness of the implementation measures that the Company has initiated and hereby limited to:

1. Emphasizing 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 results of the risk assessment, formulate and refine the key business processes and business processes of the internal control; based on the business operation and risk assessment results, combined with information technology, have the control digital measures at both the Company level and the business level, and establish the internal control system; date the internal control system;
2. Rectify the internal control system of the ongoing game internal control, and improve the risk management system; effectively implement the internal control system; effectively improve the operational data of the Company; improve the health and stability of the management of the Company; improve the awareness and ability of all domestic and overseas employees to face and combat risks;
3. Identify the Company's assets and flight risks of the internal control

