

Hong Kong Exchanges and Clearing Limited and The Stock Exchange of Hong Kong Limited take no responsibility for the contents of this announcement, make no representation as to its accuracy or completeness and expressly disclaim any liability whatsoever for any loss howsoever arising from or reliance upon the whole or any part of the contents of this announcement.



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 PARTY INVESTIGATION

This announcement is made by Shenzhen Hepalink Pharmaceutical Group Co., Ltd. (the "Company") pursuant to the Independent Information Disclosure Rules of Part XIV 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 records disclosed in the Independent Information Announcement of the Company dated 15 January 2024, 30 January 2024 and 15 March 2024 (the "Telecommunication Records").

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 independent all leading forensic investigation team (the "Independent Team") to conduct an independent forensic investigation, collaboration with a professional legal firm, and the Telecommunication Records to be conducted by the Company's wholly-owned subsidiary Tech Pharma Italia S.R.L. ("Tech Pharma Italia") (the "Independent Team").

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

I. BACKGROUND OF THE INVESTIGATION

According to the information received from the Commission dated 15 January 2024, Techdata Italia received a confidential business information disclosure from a reliable telecom provider, which is a significant amount of approximately 11.7 million. After the Telecom Fraud Case, the Commission referred to the Italian license of the Shenzhen Municipal Public Security Bureau of the Commission's legal risk management team, hired a law firm and established the Special Investigation Group led by the Commission's Deputy Director - Executive Director, which engaged the Investigation Team to conduct the investigation in collaboration with a specialized legal firm.

II. SCOPE OF THE INVESTIGATION

The investigation will include the following categories:

1. Obtain and identify the elements of communication records, including communication records with legal bodies and communication records related to the Telecom Fraud Case; the license related management case of the Commission and Techdata Italia; basic information of the commission employee (such as organizational chart and list of employees); and other activities related to the Telecom Fraud Case, including but not limited to (1) specific bank account held and their activities records; (2) record of financial ledger; (3) annual record of electronic financial management system; (4) internal and external investigation report regarding the Telecom Fraud Case; (5) the Commission's badmote element communication records; and (6) internal records related to the Telecom Fraud Case to rectify the situation;
2. Conducting interviews with the employees of the Commission and Techdata Italia who were involved in the Telecom Fraud Case to get a detailed description of the Telecom Fraud Case's specific, including the background, chronological sequence, cause and effect of the Telecom Fraud Case as well as the employee's conduct and behavior of the all categories;

3. Conducting searches and identifying financial data and, including: 1) data and information Techdata's financial data and the elements investigated timeframe; 2) data and information bank account activities associated with the Telecom Fraud Center; 3) data and information activities and the identified from 1 January 2023 to 31 December 2023, identified and examined each illegal activity and the bank account of Techdata's former employee (including the identification of the amount contributed, and the time and amount of the activities); 4) amount made by Techdata and the identified from 1 January 2023 to 31 December 2023 and identify the charges and the amount of the cost, including but not limited to a total cost, which is a direct cost;
4. Conducting background check on all parties involved in the Telecom Fraud Center, including but not limited to the address and their communication information directly or indirectly identified and the relationship between them and the management and/or employees of Techdata; additionally, public search conducted the name of the email domain used by the subject of the Telecom Fraud Center; and
5. Conducting electronic search of the Company's email account, which is a mobile device of the Techdata employee related to the Telecom Fraud Center, and the elements of all communication records, which for electronic activities include 1) creating electronic data and back up; and 2) extracting information. List of keywords had been used, and a list of identified domain had been conducted after a list of the keywords used.

III. KEY FINDINGS OF THE INVESTIGATION

(1) Criminal Team Profile

According to the interview with the management and received IT data, the general manager of Techdata received an email on 13 December 2023 from a fraud subject who attempted to be hired. The subject requested him to act as a confidential agent (the Agent) and maintain strict confidentiality to prevent information leakage. From 13 December 2023 to 3 January 2024, he received multiple funds totaling approximately 11.7 million USD within a week of the actual funds transferred to the Company (the Payment).

After reviewing the general management, it appeared that he did not disclose the Payment to the appropriate subject that the Account should be kept strictly confidential and any information leakage could indicate the extent of compromise in the market. On 13 December 2023, the subject acknowledged the general management regarding confidentiality agreement and instructed him to handle the Payment and keep it confidential until the Account is successfully closed. During the aforementioned period, the general management took multiple actions to ensure the subject's identity but did not find a red flag.

The Investigation Team identified the main cause of the failure of the management of Tech Digital and the Company to detect the abnormality and raise a timely alarm:

- (i) the finance management of Tech Digital had limited bank account management authority and was unable to check the bank account balance after the general management removed the USB-key;
- (ii) the Company's head office could not obtain the account balance from the local staff by emailing the relevant information once a week and the last working day of each month.

During the investigation, the Investigation Team visited the premises of the former associate in the Telecom Field (the P Company). The Investigation Team conducted background checks on the Payment Company and compared their management's name with the Company's employee list, finding a large gap. The Investigation Team also reached out electronically for key information about the Payment Company regarding their core operating data and, but found relevant data about them through their staff, except for their name and a few general account details and communication related to the Telecom Field. Based on the digital forensic work of the Investigation Team, connections are found between the Telecom Field and the digital data associated with Tech Digital and the employees of the Company.

(2) Immunity of the Company from the Financial

After the Telecom Field, the Company took a series of measures to ensure its technical security. The Company collaborated with bank technical policies for ensuring bank account balance and controlling the USB-key. The Company's IT department also examined and analyzed the Company's confidential information security risks and capabilities, and implemented full-scale measures to strengthen email security.

After reviewing the Report, the Special Investigative Group found the content to be detailed and meticulous, accurately reflecting the course of the Telecommunications Fraud Incident. The Special Investigative Group recommended the Board direct the Commission (the Board) to adopt the findings of the Report and implement the recommendations of the report. At the same time, the Commission assigned the implementation check recommendations, to eliminate the impact of the Telecommunications Fraud Incident and effectively safeguard the interests of the Commission and its shareholders.

I. OPINIONS OF THE BOARD

After reviewing the Report and the recommendations of the Special Investigative Group, the Board gave the Commission its conclusions and effective implementation of the main measures that the Commission has initiated early, and concluded that:

1. Examining the business process with the domestic and foreign subsidiaries of the Commission (the Group) to identify major risks; date and place of the external control matrix of the Commission subsidiaries; based on the results of the internal audit, find the deficiencies and the key business processes and business processes for external control; based on the business process audit and internal control, combined with the financial statement, and place the control and management measures at both the Commission level and the business process level, and establish the date of the external control matrix;
2. Reviewing external control to strengthen the external control, and improve the effectiveness of internal control; effective implementation of external control measures; effective implementation of the external audit of the Commission; strengthening health and safety of the employees of the Commission; improving the adaptability of all domestic and foreign employees to the external environment;
3. Investigating the Commission's audit and flight activities for external control

4. Strength of the centralized management of funds and improving the efficiency of utilization of funds; to implement the fund management system of the Group to achieve centralized management of the financial funds of the Company and its subsidiaries; control and improve the measurement of centralized management of financial funds; carry out regular effect evaluation, strengthen the credit liability of the company, improve the identification of problems and achieve good results in implementation through measures such as regular effect evaluation, key effect evaluation, and evaluation; and
5. After determining the eligibility of the candidates for the directorate through the results of the investigation, according to the case decided with the license and the associated activities, the Company will initiate a regular effect evaluation. Should it be found that any of the independent non-executive directors, the Company will take follow-up actions to the associated judicial activities and identify the cause; if necessary, the relevant regulations are published, the Company will force the resignation of a director against the background of the directorate.

S r r C m r r m
 rm r m rr
 rm B r . S r r r C m r
 r C m .
 B de f the B a d
 S H P rm Gr . C ., L .
 L L
 Chairman

Sh Zh , the PRC
 March 28, 2024

As at the date of this announcement, the executive directors of the Company are Mr. Li Li, Ms. Li Tan, Mr. Shan Yu and Mr. Zhang Ping; and the independent non-executive directors of the Company are Dr. Lu Chuan, Mr. Huang Peng and Mr. Yi Ming.