

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 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 requested 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 data format and log information; (4) internal and external investigation report regarding the Telecom Fraud Case; (5) the Commission's badminton element communication records; and (6) internal records of the Telecom Fraud Case to rectify the situation;
2. Conducting interviews with the elements of the Commission and Techdata Italia held by the Telecom Fraud Case to determine a detailed description of the Telecom Fraud Case's specific, including the background, chronological sequence, cause and effect of the Telecom Fraud Case and all the elements and consequences behind the activities;

3. Conducting searches and identifying financial data and, including: 1) data and information Techdata's financial data during the investigation timeframe; 2) data and information bank account activity associated with the Telecom Fraud Center; 3) data and information activity during the period from 1 January 2023 to 31 December 2023, identifying and examining each illegal activity and the bank account information of Techdata's former employees (including the identities of the account holders, and the time and amount of the transactions); 4) examining a matter made by Techdata during the period from 1 January 2023 to 31 December 2023 and identifying their respective data and information, including but not limited to a personal record, voice and contact;
4. Conducting background checks on all parties involved in the Telecom Fraud Center, including but not limited to the address and their communication information directly or indirectly identified through their relationship with each other and the management and/or employees of Techdata; additionally, public searches conducted through 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, network, and mobile device of the Techdata employees related to the Telecom Fraud Center, and the electronic communication record, such as electronic activities including 1) creating electronic data mirror and back-up; and 2) extracting information. List of keys should have been prepared, and a forensic image of the identified domain should be conducted after a list of the keys is developed.

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 emailed him to assist in a confidential activity (the A...) 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 euros within a week of the actual fraud. The fraud involved the Company (the P...).

After reviewing the general management, it appeared that he did not disclose the Payment to the affected by the fact that the Account should be kept strictly confidential and any information leakage could indicate the extent of the market. On 13 December 2023, the project allocated the general management to investigate confidentiality agreements and instructed him to handle the Payment and keep it confidential until the Account is a secured. During the aforementioned period, the general management took multiple actions to ensure the project'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 of the data time series:

- (i) the finance management of Tech Digital had limited bank account management although it should be able to check the bank account balance after the general management removed the USB- shield;
- (ii) the Company's head office could not balance the account balance from the local staff by emailing the electronic information once a week and the last working day of each month.

During the investigation, the Investigation Team visited the premises of the former owner of the Telecom Facility (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 relationship. The Investigation Team also reached out electronically for information about the Payment Company's internal data access, but found no electronic data about them or their staff, except for their name and a few general details and communication related to the Telecom Facility. Based on the digital forensic work of the Investigation Team, connections are found between the Telecom Facility and the digital data associated with Tech Digital and the employees of the Company.

(2) Internal Control Term Review

After the Telecom Facility, the Company took a series of measures to improve its internal control. The Company collaborated with bank to facilitate the process of checking bank account balance and controlling the USB- shield. The Company's IT department also examined and analyzed the Company's internal information security capabilities, and implemented full-scale measures to strengthen email security.

After the release of the Report, the Special Investigation Group found the content to be detailed and meticulous, accurately reflecting the course of the Telecom Fraud Incident. The Special Investigation Group recommended the board of directors of the CMA (the Board) to adopt the findings of the Report and actively implement the relevant recommendations of the Report. At the same time, the CMA investigated the implementation of the recommendations, timely eliminate the impact of the Telecom Fraud Incident and effectively safeguard the interests of the CMA and its shareholders.

I. OPINIONS OF THE BOARD

After the release of the Report and the recommendations of the Special Investigation Group, the Board of the CMA to carry out effective and effective implementation of the main measures that the CMA has initiated earlier, including but not limited to:

1. Examining the business cooperation with the domestic and foreign subsidiaries of the CMA (the Group) to identify major risks; date and enhance the internal control matrix of the CMA and its subsidiaries; based on the results of the internal audit, find the deficiencies and enhance the key business, business cooperation and business cooperation with external control; based on the business cooperation and internal audit results, combined with the internal control system, enhance the control and management measures at both the CMA level and the business cooperation level, and establish the internal control matrix; date the internal control matrix;
2. Recalling the internal control system to strengthen the internal control system, and improve the internal control system; enhance the effectiveness of the internal control system; effectively implement the business cooperation of the CMA; improve the health and sustainable development of the CMA; improve the adaptability of all domestic and foreign employees to the external environment;
3. Investigating the CMA's audit and flight activities of the internal control system

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 handle the funds of the company; improve the management of the centralized management of financial funds; carry out the legal and effective measures, such as strengthening the liability of the company, improving the management of the company, and achieving the company's management through measures such as legal and effective measures, strengthening the company's management, and strengthening the company's management.
5. After determining the feasibility of the external financial audit, although the results of the investigation, given the case related to the license, and the associated activities, the Company will initiate a financial audit and accountability. It should be noted that the external financial audit is a legal requirement, the Company will take the financial audit as the primary judicial activity and identify the cause; the company will take the legal responsibility as the primary judicial activity and identify the cause; the company will take the legal responsibility as the primary judicial activity and identify the cause.

S r r C m r r m
 rm r m rr
 rm B r . S 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.