

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



Hepalink

SHENZHEN HEPA LINK 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 PARTY INVESTIGATION

This announcement is made by Shenzhen Hepalink Pharmaceutical Group Co., Ltd. (the "Company") pursuant to the Independent Information Publication Policy 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 facilities disclosed in the Independent Information Announcement of the Company dated 15 January 2024, 30 January 2024 and 15 March 2024 (the "Three Facilities").

The Company established a dedicated 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 team of all leading forensic investigation team (the "Independent Team") to conduct a dedicated forensic investigation, collaboration with a dedicated external law firm, and the Telecommunication Facilities conducted by the Company's wholly-owned subsidiary Techdata Pharmaceutical S.R.L. ("Techdata") (the "Independent Team").

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

I. BACKGROUND OF THE INVESTIGATION

According to the identification materials submitted by the CMA dated 15 January 2024, Techdata Italy has established a commercial network of telecommunications, including a total of approximately 11.7 million. After the Telecommunications Fraud Case, the CMA requested the Italian license of the Shanghai Municipal Public Security Bureau of the Ministry of the CMA's legal risk management team, hired a law firm and established the Special Investigation Group led by the CMA's deputy director - executive director, which engaged the Investigation Team to conduct the investigation in collaboration with a dedicated technical law firm.

II. SCOPE OF THE INVESTIGATION

The Investigation Team followed the following procedures:

1. Obtaining and identifying the relevant communications records, including communications with legal bodies and communications related to the Telecommunications Fraud Case; the license related management case of the CMA and Techdata Italy; basic information of the company including legal representation (such as organizational chart and list of employees); and its actual control related to the Telecommunications Fraud Case, including but not limited to (1) specific bank account information and their actual use records; (2) record of financial ledger; (3) actual record of electronic financial management system operation; (4) internal and external investigation report regarding the Telecommunications Fraud Case; (5) the CMA's badminton telecommunications records; and (6) internal records of the Telecommunications Fraud Case to rectify the situation;
2. Conducting the interview with the relevant personnel of the CMA and Techdata Italy who were involved in the Telecommunications Fraud Case to gain a detailed understanding of the Telecommunications Fraud Case's specifics, including the background, chronological sequence of events, cause(s) and impact of the Telecommunications Fraud Case on all the relevant parties and the behavior of the participants;

3. Conducting the investigation of financial data shall include: 1) data shall include Techdata's financial data during the investigation timeframe; 2) data shall include bank account activity associated with the Telecom Fraud Center; 3) data shall include all activity during the identified period from 1 January 2023 to 31 December 2023, identifying and examining each illegal activity of the bank account of Techdata from all the evidence (including the identification of the amount contributed, and the time and amount of the transaction); 4) examining a month made by Techdata during the identified period from 1 January 2023 to 31 December 2023 and identify the charges and the corresponding cost, including but not limited to a local record, service and cost; and
4. Conducting background check shall include the Telecom Fraud Center, including but not limited to the access and their communication information directly or indirectly identified and the relationship between them and the management and/or employees of Techdata; additionally, public search engine conducted the same of the email domain used by the subject of the Telecom Fraud Center; and
5. Conducting electronic forensic of the Company's email account, including computer, and mobile device of the Techdata employee related to the Telecom Fraud Center, and the electronic communication record, including electronic activities include 1) creating electronic forensic data mirror and back up; and 2) extracting information. List of keywords had been prepared, and a forensic review of the identified domain has been conducted after a list of the keywords is available.

III. KEY FINDINGS OF THE INVESTIGATION

(I) COMPANY'S TRAFFIC

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 fraudster who pretended to be his secretary. The suspect emailed him to assist in a confidential activity (the A) and maintain strict confidentiality to ensure information leakage. From 13 December 2023 to 3 January 2024, he received multiple requests to assist in the fraud and a large amount of approximately 11.7 million within a week of the actual fraud. The fraud involved the Company (the P).

After the release of the general management, it was determined that he did not disclose the Payment to the affected by the fact that the Accountant should be kept strictly confidential and any information leakage could implicate the settlement of the market. On 13 December 2023, the project allocated the general management to a confidential agent and instructed him to handle the Payment and keep it confidential until the Accountant was released. During the aforementioned period, the general management took multiple actions to ensure the project's identity but did not trigger a red flag.

The Investigation Team identified the main cause of the failure of the management of Techdital and the Company to detect the abnormality of the data in time as follows:

- (i) the finance management of Techdital had limited bank account management although it was unable to check the bank account balance after the general management removed the USB- shield;
- (ii) the Company's head office could not obtain the account balance from the local staff by asking them to email the relevant information once a week and the last working day of each month.

During the investigation, the Investigation Team traced the elements of the case concerning the Telecom Fraud Case (the PRC Criminal Case). The Investigation Team conducted background checks on the Payment Company and compared their management with the Company's employment, finding the following. The Investigation Team also reached electronic information about the Payment Company. Regarding their core accounting data, but found relevant data about them, their staff, except for their name and age, the amount detail and communication related to the Telecom Fraud Case. Based on the digital forensic work of the Investigation Team, connecting a friend between the Telecom Fraud Case and the judicial associated with Techdital, the relevant of the Company.

(2) I II C III T F I

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

After receiving the Report, the Special Investigation Group found the content to be detailed and meticulous, accurately reflecting the content of the Telecom Fraud Case. The Special Investigation Group recommended the board of directors of the Company (the Board) to adopt the findings of the Report and actively implement the relevant recommendations of the Report. At the same time, the Company strengthened the active implementation of the recommendations, timely eliminate the impact of the Telecom Fraud Case and effectively safeguard the interests of the Company and its shareholders as a whole.

I. OPINIONS OF THE BOARD

After receiving the Report and the recommendations of the Special Investigation Group, the Board judges the Company to have effectively implemented the measures that the Company has initiated earlier, which are limited to:

1. Examining the business cooperation with the domestic and overseas subsidiaries of the Company (the Group) to identify major risks; date and place the relevant control matrix of the Company and its subsidiaries; based on the results of the risk assessment, further define and refine the key business, business cooperation and business relationship; based on the business relationship and risk assessment results, combined with the relevant management, enhance the control and management measures at both the Company level and the business level, and establish the relevant control matrix; date the relevant control matrix;
2. Rectifying the relevant control system to strengthen the management of the relevant control, and achieve a risk and risk compliance; examine the effectiveness of the implementation of the relevant control system; effectively implement the relevant control of the Company; manage health and sustainable development of the Company; improve the overall ability of all domestic and overseas employees to deal with a disaster and combat crime;
3. Identify the Company's audit and flight activities of the relevant control

4. Strengthening the centralized management of funds and improving the efficiency of fund utilization; strictly implement the fund management system of the Group to achieve centralized management of the financial funds of the Company and its subsidiaries; control the high cost of financing the measures of centralized management of financial funds; carry out regular legal inspection and evaluation, strengthen the credit liability of the company, and identify the problems and achieve the control of the company through measures such as legal inspection, key inspection, and evaluation;
5. After determining the responsibility of the executive director although the result of the investigation, regardless of the case related to the license, and the associated activities, the Company will initiate a legal action to ensure the accountability of the executive director. Should it be found that the executive director has violated the legal provisions, the Company will take the executive director to the appropriate judicial authorities and take the necessary measures; if the relevant legal provisions are not established, the Company will force the executive director to take measures against the executive director.

S
B
S
C
C
C
B
S
H
P
G
C., L.
L
Chairman

Shanghai, 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.