SHENZHEN 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)
(Stock 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 Inside Information Provisions under 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 on The Stock Exchange of Hong Kong Limited.

FORMATION OF SPECIAL INVESTIGATION GROUP

References are made to the telecom fraud incident disclosed in the inside information announcements of the Company dated 15 January 2024, 30 January 2024 and 15 March 2024 (the "**Telecom Fraud Incident**").

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 directors, engaged an internationally leading forensic investigation team (the "**Investigation Team**") to conduct an independent forensic investigation, in collaboration with a renowned international law firm, into the Telecom Fraud Incident encountered by the Company's wholly-owned subsidiary Techdow Pharma Italy S.R.L. ("**Techdow Italy**") (the "**Investigation**").

On 26 March 2024, the Investigation Team delivered an investigation report to the Special Investigation Group (the "**Report**"). The relevant status of the Investigation is as follows:

I. BACKGROUND OF THE INVESTIGATION

As disclosed in the inside information announcement of the Company dated 15 January 2024, Techdow Italy was recently defrauded by a criminal syndicate as a result of telecom fraud, involving an amount of approximately 11.7 million euros. After the Telecom Fraud Incident, the Company reported to the Italian police and the Shenzhen Municipal Public Security Bureau under the supervision of the Company's legal risk management team, hired a law firm and established the Special Investigation Group led by the Company's independent non-executive directors, which engaged the Investigation Team to conduct the Investigation in collaboration with a renowned international law firm.

II. SCOPE OF THE INVESTIGATION

The Investigation involved the following procedures:

1. Obtaining and reviewing the relevant documentation and records, including communications with regulatory bodies and documentation related to the Telecom Fraud Incident; the policies and related management processes of the Company and Techdow Italy; basic information of the companies involved (such as organizational charts and lists of employees); and transaction documents related to the Telecom Fraud Incident, including but not limited to (1) specific bank accounts involved and their transaction records; (2) records from accounting ledger; (3) approval records in electronic or paper format and logs of system operations; (4) internal and external investigation reports regarding the Telecom Fraud Incident; (5) the Company's board minutes or relevant communication records; and (6) plans developed in response to the Telecom Fraud Incident to rectify the situation;

2. Conducting interviews with the relevant personnel of the Company and Techdow Italy who were involved in the Telecom Fraud Incident in order to gain a detailed understanding of the Telecom Fraud Incident's specifics, including the background, chronological sequence of events, cause(s) and status of the Telecom Fraud Incident as well as the reason(s) and process behind the allocation of funds;

3. Conducting voucher inspections and financial data analysis, including: 1) data analysis on Techdow Italy's financial data during the relevant investigation timeframe; 2) data analysis on bank account transactions associated with the Telecom Fraud Incident; 3) any unusual transactions during the period from 1 June 2023 to 31 December 2023, identify and examine any such irregular transactions in the bank account funds of Techdow Italy from various perspectives (such as the identities of the payment counterparties, and the time and amounts of the transactions); 4) sampling payments made by Techdow Italy during the period from 1 June 2023 to 31 December 2023 and reviewing their vouchers and supporting documents, including but not limited to approval records, invoices and contracts;

4. Conducting background checks on all parties involved in the Telecom Fraud Incident, including but not limited to the payees and their company registration information or directorship appointments to identify any potential relationships between them and the management and/or employees of Techdow Italy; additionally, public searches were conducted on the names of the email domains used by the suspects of the Telecom Fraud Incident; and

5. Conducting electronic forensics on the Company's email accounts, work computers, and work mobile devices of the Techdow Italy personnel related to the Telecom Fraud Incident, and the relevant personal communication records, such forensics activities include 1) creating electronic forensic data mirroring and backup; and 2) extracting information. Lists of keywords has been prepared, and a forensic review of the identified documents has been conducted after applying these keywords in a search.

III. KEY FINDINGS OF THE INVESTIGATION

(1) Circumstances of the Telecom Fraud Incident

According to the interviews with the management and recovered IT data, the general manager of Techdow Italy received an email on 13 December 2023 from a fraud suspect who pretended to be his supervisor. The suspect requested him to assist in a confidential acquisition (the "**Acquisition**") and maintain strict confidentiality to prevent information leakage. From 13 December 2023 to 3 January 2024, he received multiple rounds of purported instructions from the suspect and arranged a payment of approximately 11.7 million euros without seeking the approval of or informing anyone else in the Company (the "**Payment**").

After interviewing the general manager, it was understood that he did not disclose the Payment as he was informed by the suspect that the Acquisition should be kept strictly confidential and any information leakage could implicate the investors and competitors in the market. On 13 December 2023, the suspect also asked the general manager to sign a confidentiality agreement and instructed him to handle the Payment alone and keep it confidential until the Acquisition was announced. During the aforementioned period, the general manager took multiple actions to verify the suspect's identity but did not find any red flags.

The Investigation Team identified two main reasons for the failure of the management of Techdow Italy and the Company to detect the abnormality in funds in a timely manner:

(i) the finance manager of Techdow Italy had limited bank account management authority and was unable to check the bank account balance after the general manager removed the USB-shield; and

(ii) the Company's headquarters could only obtain the account balance from the local staff by requiring them to email the relevant information twice a week and on the last working day of each month.

During the Investigation, the Investigation Team noticed the involvement of seven payee companies in the Telecom Fraud Incident (the "**Payee Companies**"). The Investigation Team conducted background checks on the Payee Companies and compared their management's names with the Company's employee list, finding no overlapping. The Investigation Team also searched electronically for key information about the Payee Companies using their core corporate data as keywords, but found no relevant data about them or their staff, except for their names appearing in the payment details and communications related to the Telecom Fraud Incident. Based on the digital forensics work of the Investigation Team, no connection was found between the Telecom Fraud Incident and the individuals associated with Techdow Italy or other personnel of the Company.

(2) Immediate actions of the Company after the Telecom Fraud Incident

After the Telecom Fraud Incident, the Company took various steps to improve its internal controls. The Company collaborated with banks to enforce stricter policies for reporting bank account balances and controlling the USB-shield. The Company's IT department also re-examined and analyzed the Company's potential information security risks and vulnerabilities, and implemented follow-up measures to strengthen email security.

(3) Recommendations on improving internal controls

Based on the Investigation findings, the Investigation Team found that Techdow Italy had failed to (i) set up an adequate separation of responsibilities for managing its bank account, as required by the relevant regulations and policies, and (ii) submit timely reports on its bank account balances in accordance with its balance reporting policy.

The Investigation Team recommended Techdow Italy to (i) strengthen its bank account management and (ii) raise employees' awareness of email phishing and cyber phishing.

IV. POSSIBLE LIMITATIONS OF THE FORENSIC INVESTIGATION

1. The data and personnel available for interviews were limited;

2. The data obtained include information that was not audited, verified or confirmed; and

3. The Investigation results may not represent commitments regarding past or future matters, or represent the latest situation, and the results may need to be updated accordingly.

V. WORKING CONDITION AND OPINIONS OF THE SPECIAL INVESTIGATION GROUP

After becoming aware of the Telecom Fraud Incident, the independent non-executive directors of the Company expressed serious concern about the Telecom Fraud Incident and made a number of recommendations to the Company. These include referring to similar Telecom Fraud Incidents worldwide and engaging an external independent organization to conduct the Investigation. Once the recommendations were confirmed and adopted, the 3 independent non-executive directors of the Company immediately established the Special Investigation Group and began the selection process for the Investigation Team. They considered qualifications, service cases, investigation plans, and international coordination capabilities, and made a prudent decision.

During the Investigation, the Special Investigation Group and the Investigation Team maintained close communication with the other directors and members of the Company's management. They closely monitored the progress of the Investigation, actively coordinated resources of all parties and assisted the Investigation Team in their work, effectively ensuring the successful completion of the Investigation, as well as its independence and authority.

After reviewing the Report, the Special Investigation Group found the content to be detailed and meticulous, accurately reconstructing the course of the Telecom Fraud Incident. 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 therein. At the same time, the Company is urged to actively implement such recommendations, strive to eliminate the impact of the Telecom Fraud Incident and effectively safeguard the interests of the Company and its shareholders as a whole.

VI. OPINIONS OF THE BOARD

After reviewing the Report and the recommendations of the Special Investigation Group, the Board urges the Company to continue to reinforce and effectively implement the multiple measures that the Company has initiated earlier, including but not limited to:

1. Examining the business processes within the domestic and overseas subsidiaries of the Company (the "**Group**") to identify major risks; update and enhance the internal control matrix of the Company and its subsidiaries; based on the results of the risk assessment, further define and refine the key branches, business processes and sub-processes of internal control; based on the business operations and risk assessment results, combined with information system tools, enhance the corresponding control measures at both the Company level and the business processes level, and regularly review and update the internal control matrix;

2. Recruiting internal control experts to strengthen training programs on internal control, and raise awareness of risk and risk compliance; ensuring the effective implementation of internal control systems; effectively improving the operational standards of the Company; promoting healthy and sustainable development of the Company; improving the awareness and ability of all domestic and overseas employees to prevent fraud and combat crimes;

3. Intensifying the Company's audits and flight inspections of internal control of overseas subsidiaries; implementing rectification responsibilities and promoting rectification evaluations and monitoring their progress; based on the results of the risk assessment and the effectiveness of daily supervision, enhancing the oversight over the internal audits and assessments of key business processes of overseas subsidiaries of the Company; building a "closed loop" of internal control that focuses on improving management value; in response to the risks, defects and causes identified during the audit supervision process, formulating practical and feasible rectification plans, identifying persons responsible for the rectification, and communicating and providing feedback in a timely manner;

4. Strengthening the centralized management of funds and improving the efficiency of utilization of funds; strictly implementing the fund management systems of the Group to achieve centralized management of the internal funds of the Company and its subsidiaries; continuously enhancing and improving the measures for centralized management of internal funds; carrying out regular inspections and supervision, enforcing strict liability for losses, promptly identifying any problems and achieving continuous improvement through measures such as regular inspections, key spot inspections, or audit supervision; and

5. After determining the responsibilities of the pertinent individuals through the results of the Investigation, progress of the case opened with the police, and other associated activities, the Company will initiate an internal accountability procedure to hold the relevant individual strictly accountable. Should it be found that any of the involved employees have violated any laws or regulations, the Company will transfer such individuals to the appropriate judicial authorities and provide cooperation; in instances where gross negligence is established, the Company will enforce stringent disciplinary measures against the offending individuals.

Shareholders and potential investors of the Company are reminded that the information provided in this announcement is based on the currently available information to the Board. Shareholders and potential investors of the Company are advised to exercise caution when dealing in the shares of the Company.

By order of the Board
Shenzhen Hepalink Pharmaceutical Group Co., Ltd.
Li Li
Chairman

Shenzhen, 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.