UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 101794 / December 2, 2024

ADMINISTRATIVE PROCEEDING
File No. 3-22335

In the Matter of **INDUSTRIAL AND COMMERCIAL BANK OF CHINA FINANCIAL SERVICES LLC,** **Respondent.**	**ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS, PURSUANT TO SECTIONS 15(b) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASE-AND-DESIST ORDER**

I.

The Securities and Exchange Commission ("Commission") deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 ("Exchange Act"), against Industrial and Commercial Bank of China Financial Services LLC ("Respondent" or "ICBC Financial Services").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Adminitrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds that:

Summary

In November 2023, ICBC Financial Services was the victim of a ransomware cyberattack (the "Cybersecurity Incident"). This attack led to a disruption with the firm's access to and ability to update its books and records information in its various systems, and caused ICBC Financial Services to terminate connectivity to its clearing firms and clearing agents in response to the Cybersecurity Incident. Between November 8, 2023 and March 1, 2024 (the "Relevant Period"), ICBC Financial Services failed to keep current its books and records, and to give or send written confirmations for securities related transactions to its customers. The violations indicate, in part, that the Respondent needed to be better prepared for a potentially severe cybersecurity incident.

Respondent

1. ICBC Financial Services is a Delaware limited liability company with its principal place of business in New York, New York. ICBC Financial Services has been a wholly-owned subsidiary of Industrial and Commercial Bank of China Limited since 2010. ICBC Financial Services is registered with the Commission as a broker-dealer.

Facts

The Cybersecurity Incident

2. On November 8, 2023, ICBC Financial Services discovered that malicious software had blocked access to its computer systems and data by encrypting data and programs within its network. This Cybersecurity Incident had a significant impact on the firm's operations. Specifically, the attack disrupted ICBC Financial Services' access to, and ability to update its books and records information in its various systems, as well as caused ICBC Financial Services to terminate connectivity to its clearing firms and clearing agents, impeding trading.

3. ICBC Financial Services subsequently investigated the Cybersecurity Incident and determined that it needed to enhance its related governance, cybersecurity resources, and its risk assessment and mitigation processes.

Books and Records Issues Resulting from the Cybersecurity Incident

4. Following the Cybersecurity Incident, during the Relevant Period, ICBC Financial Services' books and records were not kept current and reflected inaccurate and/or incomplete information. Among other things, ICBC Financial Services' books and records related to its fixed income and repurchase system ("TSS") were not updated on a current basis. While ICBC Financial Services manually updated the system and created an offline spreadsheet to capture certain fixed income transactions, for a period of time various books and records information was incomplete and/or inaccurate, including fixed income blotters, ledgers, ledger accounts, securities record,

memoranda of brokerage orders, memoranda of purchase or sale of securities, and confirmations of purchases and sales of securities.

5. In addition, ICBC Financial Services' books and records related to its equity system (which also maintained its consolidated stock record), were not updated on a current basis to reflect various equities transactions. Following the Cybersecurity Incident, ICBC Financial Services had to regain access to its equity system and recreate various missing trades. As a result, for a period of time, various books and records information in its equity system was incomplete and/or inaccurate, including blotters, ledgers, ledger accounts, securities record, memoranda of brokerage orders, memoranda of purchase or sale of securities, and confirmations of purchases and sales of securities.

6. ICBC Financial Services' inaccurate books and records in its TSS and equity systems further impacted its Customer and its Proprietary Accounts of Broker-Dealers ("PAB") reserve computations. As ICBC Financial Services was unable to produce accurate and complete ledgers and ledger account information of its customer and PAB accounts, and was unable to access its equity system, for a period of time it produced customer and PAB reserve computations using estimates and incomplete records.

7. As a result of the Cybersecurity Incident, ICBC Financial Services also lost access to its general ledger and trial balance system. In addition, as a result of the Cybersecurity Incident's impact on its TSS and equity systems, ICBC Financial Services' books and records, and its sub-ledgers supporting its net capital computation were incomplete, inaccurate, and/or inaccessible. As a result, for a period of time, its computations of aggregated indebtedness and net capital, which were based on available books and record information, were inaccurate.

8. Finally, following the Cybersecurity Incident, ICBC Financial Services executed various customer transactions. However, because of the impact of the Cybersecurity Incident, for a period of time it did not send trade confirmations to these customers at or before the completion of each of these transactions.

Violations of the Federal Securities Laws

9. Exchange Act Rule 17a-3(a) requires that every member of a national securities exchange who transacts a business in securities directly with others than members of a national securities exchange, and every broker or dealer who transacts a business in securities through the medium of any such member, and every broker or dealer registered pursuant to Section 15 of the Exchange Act, as amended, shall make and keep current various books and records relating to its business, including: blotters, ledgers, ledger accounts, securities record, memorandums of each brokerage order and each purchase or sale of securities, confirmations of all purchases and sales of securities, trial balances, computation of aggregate indebtedness and net capital and reserve computation. As a result of the conduct described above, ICBC Financial Services willfully[1]

[1] "Willfully," for purposes of imposing relief under Section 15(b) of the Exchange Act, "'means no more than that the person charged with the duty knows what he is doing.'" *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)).

violated Section 17(a) of the Exchange Act and Rule 17a-3(a) thereunder, which require broker-dealers to make and keep current certain books and records.

10. Exchange Act Rule 10b-10(a) indicates that it shall be unlawful for any broker or dealer to effect for or with an account of a customer any transaction in, or to induce the purchase or sale by such customer of, any security (other than U.S. Savings Bonds or municipal securities) unless such broker or dealer, at or before completion of such transaction, gives or sends to such customer written notification disclosing various information such as: the date and time of the transaction (or the fact that the time of the transaction will be furnished upon written request to such customer) and the identity, price, and number of shares or units (or principal amount) of such security purchased or sold by the customer; whether the Firm is acting as an agent or principal. ICBC Financial Services, therefore, willfully violated Rule 10b-10(a) of the Exchange Act, which requires broker-dealers to send trade confirmations to customers at or before the completion of transactions.

ICBC Financial Services' Cooperation and Remedial Efforts

11. In determining to accept the Offer, the Commission considered remedial acts promptly undertaken by Respondent and cooperation afforded the Commission staff.

12. Following the Cybersecurity Incident, ICBC Financial Services cooperated with staff from the Division of Examinations ("Exams") to address the issues stemming from the incident. It promptly terminated connections, downscaled operations, secured funding, collaborated with clearing partners, and aided clients in finding alternative clearing firms. ICBC Financial Services also promptly hired third-party cybersecurity specialists to assistant in the containment and remediation of the incident.

13. In connection with its collaboration with Exams staff, it further made individuals available promptly, documents available promptly upon recovery, and provided both regular and ad hoc briefings on the incident and its response.

14. ICBC Financial Services then instituted cybersecurity enhancements, the implementation of which remains ongoing, which included:

- enhancement to ICBC Financial Services' cybersecurity posture and the securing of information assets, including the augmentation of dedicated resources, such as the hiring of third-party consultants to aid in identifying weaknesses and implementing remediation;

- securing assets to prevent, detect, and respond to cyber threats, including hiring a Chief Information Security Officer to evaluate and escalate IT and cybersecurity-related risk within its systems;

- establishing a working group responsible for technology infrastructure, end-of-life risk assessment, and other related matters;

- enhancing technical and administrative controls, including revising incident response plans, conducting regular security testing, and enhancing its training program; and

- assessing and redefining of the components of ICBC Financial Services' business continuity, cybersecurity, and IT practices to enhance their effectiveness against cyber threats, including annually recurring internal audits and periodic assessments of its policies, procedures, and controls to make sure that they are effective and in line with current industry standards and regulatory expectations.

15. In consideration of the foregoing, the Commission has determined not to impose a civil penalty on Respondent.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent's Offer.

Accordingly, pursuant to Sections 15(b) and 21C of the Exchange Act, it is hereby ORDERED that:

A. Respondent cease and desist from committing or causing any violations and any future violations of Section 17(a) of the Exchange Act and Rule 17a-3(a) thereunder, and Rule 10b-10(a) under the Exchange Act.

B. Respondent is censured.

C. Respondent acknowledges that the Commission is not imposing a civil penalty based upon its cooperation in a Commission investigation and/or related enforcement action. If at any time following the entry of the Order, the Division of Enforcement ("Division") obtains information indicating that Respondent knowingly provided materially false or misleading information or materials to the Commission, or in a related proceeding, the Division may, at its sole discretion and with prior notice to the Respondent, petition the Commission to reopen this matter and seek an order directing that the Respondent pay a civil money penalty. Respondent may contest by way of defense in any resulting administrative proceeding whether it knowingly provided materially false or misleading information, but may not: (1) contest the findings in the Order; or (2) assert any defense to liability or remedy, including, but not limited to, any statute of limitations defense.

By the Commission.

Vanessa A. Countryman
Secretary