UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 100780 / August 20, 2024

ADMINISTRATIVE PROCEEDING
File No. 3-22024

In the Matter of **Equiniti Trust Company, LLC f/k/a American Stock Transfer & Trust Company, LLC** **Respondent.**	**ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS, PURSUANT TO SECTIONS 17A 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 17A and 21C of the Securities Exchange Act of 1934 ("Exchange Act") against Equiniti Trust Company, LLC f/k/a American Stock Transfer & Trust Company, LLC ("American Stock Transfer" or "Respondent").

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 Respondent and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 17A 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

1. This matter concerns violations of Section 17A(d) of the Exchange Act and Rule 17Ad-12 thereunder by registered transfer agent American Stock Transfer by failing to assure that: (i) all securities in its custody or possession related to its transfer agent activities were held in safekeeping and were handled, in light of all facts and circumstances, in a manner reasonably free from risk of theft, loss or destruction, and (ii) all funds in its custody or possession related to its transfer agent activities were protected, in light of all facts and circumstances, against misuse.

2. Respondent suffered two separate cyber incidents in 2022 and 2023, respectively, that led to the net loss of approximately $4.08 million total in client funds. First, in September 2022, an unknown threat actor impersonating an issuer-client contact of Respondent successfully directed American Stock Transfer to issue millions of the issuer's shares, liquidate them, and then send the proceeds to bank accounts located in Hong Kong. Second, in April 2023, an unknown and apparently different threat actor used Social Security numbers fraudulently obtained outside of Respondent's systems to gain access to certain online accounts maintained by American Stock Transfer that contained securities of shareholders of American Stock Transfer's public-issuer clients. The threat actor liquidated shares in those accounts and sent the proceeds to external bank accounts. In both instances, American Stock Transfer did not assure that it held securities in its custody and possession in safekeeping and handled them in a manner reasonably free from risk of theft, and did not assure that it protected funds in its custody and possession against misuse.

3. Based on the foregoing, and as described in further detail below, Respondent willfully violated Section 17A(d) of the Exchange Act and Rule 17Ad-12 thereunder.

Respondent

4. **Equiniti Trust Company, LLC f/k/a American Stock Transfer & Trust Company, LLC** is a New York limited liability trust company based in New York, New York. Respondent initially registered as a transfer agent with the Commission in 2002 under the name "American Stock Transfer & Trust Company, LLC." Effective as of June 30, 2023, Respondent merged with Equiniti Trust Company ("EQ Trust"), a registered transfer agent, with Respondent as the surviving entity. Immediately upon closing of the merger, Respondent amended its Certificate of Organization to change its name to "Equiniti Trust Company, LLC." In September 2023, EQ Trust withdrew its registration as a transfer agent with the Commission.

Facts

September 2022 Incident

5. In January 2022, Respondent sent a company communication by email to employees involved in processing client payments, including relationship managers who interacted directly with Respondent's public-issuer clients, alerting them to increasing industry-wide incidents of fraud, providing guidance, and warning them to be on alert for fraudulent wire transfer requests

sent by email. Along with the warnings in the email, Respondent instructed employees to never rely on a client's emailed request alone and to always perform a call-back to the requestor using a client telephone number from Respondent's system of record to verify the emailed request. Respondent also cautioned employees to pay attention to requestors' email addresses because threat actors often masquerade as clients by using email domains that appear identical to the clients' real domains at first glance but actually have slight differences. However, beyond identifying necessary mitigation strategies and distributing these initial instructions, Respondent did not take additional steps to implement the safeguards and procedures outlined in the warning email. For example, Respondent did not confirm that the January 2022 warning email was read by its recipients, provide training to its employees on this topic, or otherwise ensure that call-backs were performed or that the other risk mitigation steps outlined in the warning email were acknowledged and followed.

6. In September 2022, an unknown threat actor outside of Respondent joined an existing email chain that included the client contact at a U.S.-based public-issuer client of Respondent (the "Issuer"), the Issuer's relationship manager at Respondent, and an external financial management adviser to the Issuer. Pretending to be the Issuer's employee, the threat actor instructed Respondent to issue millions of new shares of the Issuer, liquidate those shares, and send the proceeds to bank accounts located in Hong Kong. The threat actor concealed its identity by using an email domain that was almost identical to the real Issuer's domain except for one letter, by imitating closely the verbal patterns and practices of the existing contact at the Issuer, and by sending its instructions as a continuation of the existing email chain rather than as a new stand-alone request. The relationship manager at Respondent, who did not notice the altered email address used by the threat actor, did not take steps beyond replying to the email chain to verify that the Issuer did in fact want to issue and liquidate new shares and then transfer the proceeds to a foreign bank.

7. Over the course of a month, at the direction of what appeared to be the Issuer but was actually the threat actor, Respondent issued approximately 5.3 million shares of the Issuer and then instructed a third-party broker-dealer to sell approximately 3.3 million of those new shares for about $4.78 million. Respondent transferred all the proceeds to Hong Kong-based bank accounts.

8. The Issuer eventually noticed in November 2022 that the number of its shares outstanding in the market was greater than reflected in its internal records. The Issuer alerted Respondent, which investigated and then discovered the fraud and took action to claw back the funds that had been sent to Hong Kong. Ultimately, Respondent was able to recover approximately $1 million and fully reimbursed the Issuer for the money lost as a result of the issuance and sale of the shares.

April 2023 Incident

9. Respondent's online platform allowed individuals to create accounts to purchase shares of Respondent's public-issuer clients. These orders were executed by third-party broker-dealers. Individuals could also use their accounts to receive share issuances. To create these accounts, individuals had to use, among other information, their Social Security numbers to create separate accounts for each issuer. Respondent's online platform had a default setting that automatically linked together accounts that shared the same Social Security number, which enabled an accountholder to view all of their issuer-specific accounts and conduct transactions from one central online portal. This left Respondent's online platform vulnerable to attack because accounts with identical Social Security numbers would be linked automatically even if other important

personal information, such as the accountholders' names, addresses, or email addresses, did not match.

10. In or before April 2023, an unknown threat actor opened online accounts with Respondent using stolen Social Security numbers of certain accountholders of Respondent that were obtained from outside of Respondent's systems. Those fraudulent accounts, which had fake names and addresses associated with them, were then linked to the accountholders' legitimate accounts and used by the threat actor to transfer cash from those accounts to a third-party bank. Although the Social Security numbers belonged to certain of Respondent's accountholders, there is no evidence that the threat actor breached Respondent's systems or otherwise obtained the numbers from Respondent. The source of the stolen numbers remains unknown. The default settings put in place by Respondent allowed the threat actor to gain access to real customer accounts based solely on the matching Social Security numbers, notwithstanding that the names and other personal information associated with the fraudulent accounts did not match those of the legitimate accounts. The threat actor then liquidated a certain number of securities and transferred a total of approximately $1.9 million in proceeds out of the legitimate accounts to external bank accounts.

11. Respondent did not notice or discover the fraudulent transfers on its own. Instead, it learned of the transfers from the bank that handled the transfers, which flagged the transactions in April 2023. After Respondent confirmed these were fraudulent transfers, the bank was able to pull back approximately $1.6 million, which represented all but around $300,000 of the fraudulently transferred cash. In response to this cyber incident, Respondent shut down its online portal, began an investigation, and limited transactions to telephonic customer service assistance until August 2023, when, among other enhancements to its systems, Respondent eliminated the ability to link accounts using only Social Security numbers. Respondent also fully reimbursed the affected accountholders for the approximately $300,000 in lost funds.

Violations

12. As a result of the conduct described above, Respondent willfully[1] violated Section 17A(d) of the Exchange Act, which prohibits registered transfer agents from acting in contravention of the Commission's rules and regulations, and Rule 17Ad-12 thereunder, which requires transfer agents to assure that all securities in their custody or possession related to their transfer agent activities are "held in safekeeping and are handled, in light of all facts and circumstances, in a manner reasonably free from risk of theft, loss or destruction," and that all funds in their custody or possession related to their transfer agent activities are "protected, in light of all facts and circumstances, against misuse."

Respondent's Cooperation and Remedial Efforts

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

[1] "Willfully," for purposes of imposing relief under Section 17A 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)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Tager v. SEC*, 344 F.2d 5, 8 (2d Cir. 1965).

including, but not limited to, hiring a Chief Control Officer responsible for overseeing cyber security, engaging a third-party cyber security firm to conduct a forensic review of Respondent's systems, and fully reimbursing Respondent's clients and accountholders for losses resulting from the cyber incidents.

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 17A 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 17A(d) of the Exchange Act and Rule 17Ad-12 thereunder.

B. Respondent is censured.

C. Respondent shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of $850,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying Equiniti Trust Company, LLC f/k/a American Stock Transfer & Trust Company, LLC as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Jason H. Lee, Associate Regional Director,

Division of Enforcement, San Francisco Regional Office, Securities and Exchange Commission, 44 Montgomery Street, Suite 2800, San Francisco, CA 94104.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman
Secretary