NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of :

SA STONE WEALTH MANAGEMENT INC. :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and SA Stone Wealth Management Inc. (the "Company" or "SA Stone") agree to resolve the matters described herein without further proceedings.

WHEREAS**,** SA Stone is licensed by the Department to sell life, accident, health, property, and casualty insurance in New York State;

WHEREAS, SA Stone is wholly owned by StoneX Group Inc. ("StoneX");

WHEREAS**,** August 29, 2017, marked the initial effective date of New York's first-in-the-nation cybersecurity regulation, 23 NYCRR Part 500 (the "Cybersecurity Regulation");

WHEREAS**,** the Cybersecurity Regulation is designed to address significant issues of cybersecurity and protect the financial services industry and consumers from the ever-increasing threat of data breaches and cyberattacks;

WHEREAS**,** the Cybersecurity Regulation's standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, timely reporting of Cybersecurity Events (as defined by 23 NYCRR § 500.01(d)), and enforcement were promulgated to strengthen cybersecurity and data protection for the industry and consumers;

WHEREAS**,** the Department has been investigating certain Cybersecurity Events experienced within SA Stone and SA Stone's compliance with the Cybersecurity Regulation; and

WHEREAS, based on the investigation, the Department has concluded that SA Stone violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.12(b), which requires all DFS-regulated entities ("Covered Entities") to implement multi-factor authentication ("MFA") for all users, or reasonably equivalent or more secure access controls approved in writing by the Chief Information Security Officer ("CISO"); (2) 23 NYCRR § 500.17(a), which requires Covered Entities to timely file notice of a Cybersecurity Event with the Department; and (3) 23 NYCRR § 500.17(b), which requires Covered Entities to certify compliance with the Cybersecurity Regulation on an annual basis.

NOW THEREFORE**,** in connection with an agreement to resolve this matter without further proceedings, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the insurance regulator of the State of New York, and the Superintendent of Financial Services is responsible for ensuring the safety and soundness of New York's insurance industry and promoting the reduction and elimination of fraud, abuse, and unethical conduct with respect to insurance licensees.

2. The Superintendent has the authority to conduct investigations, bring enforcement proceedings, levy monetary penalties, and order injunctive relief against parties who have violated the relevant laws and regulations.

3. Among her many roles is the Superintendent's consumer protection function, which includes the critical protection of individuals' private and personally sensitive data from careless, negligent, or willful exposure by licensees of the Department.

4. To support this important role, the Superintendent's Cybersecurity Regulation places on all Covered Entities, including SA Stone, an obligation to establish and maintain a cybersecurity program designed to protect the confidentiality and integrity of their electronic information systems ("Information Systems"), as well as any consumer non-public information ("NPI") contained therein. 23 NYCRR §§ 500.01(e), 500.01(g).

5. Section 500.12(b), for example, requires that Covered Entities implement MFA "for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls." MFA requires two or more distinct authentication factors for successful access, such that username and password credentials alone are insufficient for access. MFA is an important line of defense against attempts to gain unauthorized access to accounts,

including through phishing emails — *i.e.*, emails sent by cyber attackers to deceive users into providing their credentials or personal or other confidential information to permit unauthorized access or harm to protected Information Systems.

6. A "Cybersecurity Event" is an act or attempt, whether or not successful, to gain unauthorized access to information stored on an Information System or disrupt or misuse such Information System. 23 NYCRR § 500.01(d). Covered Entities must report to the Department the types of Cybersecurity Events described in Sections 500.17(a)(1) and (a)(2) no more than 72 hours from a determination that a Cybersecurity Event has occurred. 23 NYCRR § 500.17(a).

7. Moreover, Section 500.17(b) of the Cybersecurity Regulation requires Covered Entities to certify compliance with the Cybersecurity Regulation on an annual basis by filing a Certificate of Compliance with the Department.

Events at Issue

MFA Implementation

8. As noted above, pursuant to 23 NYCRR § 500.12(b), MFA must be utilized for any individuals accessing a Covered Entity's internal network from an external network. The structure of SA Stone's Information Systems requires the Company's independent contractors to access SA Stone's internal network, including email systems, from an external network. As such, MFA, or a reasonable equivalent approved in writing by SA Stone's CISO, should have been implemented.

9. SA Stone, however, did not implement MFA for its independent contractors until October 11, 2021. The absence of MFA until that date left SA Stone's Information Systems and its consumers' NPI vulnerable to threat actors, including those threat actors who attacked SA Stone's Information Systems in connection with the Cybersecurity Events described below.

Cybersecurity Events

10. On October 5, 2021, SA Stone reported to the Department that, on January 22, 2021, five of its independent contractors' email clients had been compromised in a phishing campaign, as evidenced by these email addresses sending phishing emails of their own. SA Stone first learned of this event four months earlier, on June 15, 2021. This Cybersecurity Event, which was reportable under Section 500.17(a), affected a total of 3,947 individuals, of whom 17 were New Yorkers.

11. Following the Department's queries, on February 10, 2022, SA Stone disclosed a previously unreported Cybersecurity Event, and, on March 4, 2022, the Company disclosed multiple previously unreported Cybersecurity Events. Of these additional Cybersecurity Events — all of which involved independent contractors — the Department determined that nearly all of them should have been reported to the Department under Section 500.17(a). The longest span of time between the date that SA Stone was required to notify DFS of a reportable Cybersecurity Event and the date that SA Stone gave such notice was 1,463 days, or about four years.

12. Most of these additional reportable Cybersecurity Events, like the one reported to the Department on October 5, 2021, were successful phishing events wherein an independent contractor's login credentials were stolen. The remaining reportable Cybersecurity Event involved a ransomware attack on an independent contractor's personal device that locked the contractor out of her device.

13. The additional reportable Cybersecurity Events affected a total of 2,151 individuals, 11 of whom were New Yorkers. SA Stone had previously reported the majority of these additional reportable Cybersecurity Events to other governmental agencies, but not to DFS.

14. Following the Department's investigation, SA Stone and StoneX took multiple remedial measures. On October 11, 2021, StoneX implemented MFA for all independent contractors, including SA Stone's. StoneX also significantly increased its Information Systems budget and engaged multiple outside consultants to conduct penetration testing and provide continuous monitoring and incident response. StoneX now also includes cybersecurity as a quarterly board topic.

15. Since SA Stone implemented MFA, it has not experienced another Cybersecurity Event.

Part 500 Compliance Certification

16. Prior to the Department's investigation, SA Stone had not certified its compliance with the Cybersecurity Regulation, as required by 23 NYCRR § 500.17(b).

Violations of Law and Regulations

17. SA Stone did not implement MFA for all users until October 11, 2021, nor had the Company's CISO approved in writing reasonably equivalent or more secure access controls, in violation of 23 NYCRR § 500.12(b).

18. SA Stone did not timely report numerous Cybersecurity Events, in violation of 23 NYCRR § 500.17(a).

19. SA Stone failed to certify compliance with the Cybersecurity Regulation, in violation of 23 NYCRR § 500.17(b).

NOW THEREFORE**,** to resolve this matter without further proceedings, the Department and the Company stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Penalty

20. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, the Company shall pay a total civil monetary penalty pursuant to Financial Services Law § 408 to the Department in the amount of One Million, Three Hundred Fifty Thousand U.S. Dollars and 00/100 Cents ($1,350,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

21. The Company shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

22. The Company shall neither seek nor accept, directly or indirectly, reimbursement or indemnification from any unaffiliated third party with respect to payment of the penalty amount, including, but not limited to, payment made pursuant to any insurance policy.

23. In assessing a penalty for failures in cybersecurity compliance and required reporting, the Department has taken into account factors that include, without limitation: the extent to which the Company has cooperated with the Department in the investigation of such conduct, the gravity of the violations, and such other matters as justice and the public interest may require.

24. The Department acknowledges the Company's cooperation throughout this investigation. The Department also recognizes and credits the Company's ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, the Company demonstrated its commitment to remediation by devoting significant financial and other

resources to enhance its cybersecurity program, including through changes to its policies, procedures, systems, and governance structures.

Full and Complete Cooperation

25. The Company commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Further Action by the Department

26. No further action will be taken by the Department against the Company for the conduct set forth in this Consent Order, provided that the Company fully complies with the terms of the Consent Order.

27. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against the Company for transactions or conduct that was not disclosed in the written materials submitted to the Department in connection with this matter.

Waiver of Rights

28. The Company submits to the authority of the Superintendent to effectuate this Consent Order.

29. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal, or agency outside of the Department.

Parties Bound by the Consent Order

30. This Consent Order is binding on the Department and the Company, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

Breach of Consent Order

31. In the event that the Department believes the Company to be in material breach of the Consent Order, the Department will provide written notice to the Company, and the Company must, within ten (10) days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

32. The Company understands and agrees that its failure to make the required showing within the designated time period shall be presumptive evidence of the Company's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under the New York State Insurance Law, the Financial Services Law, or any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

33. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

David A. Casler
Senior Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For SA Stone Wealth Management Inc.:

Andrew Chambless
General Counsel
SA Stone Wealth Management
2 Perimeter Park, Suite 100 W
Birmingham, Alabama 35243

Alan Raul, Partner
Colleen Brown, Partner
Sidley Austin LLP
1501 K Street, NW
Washington, DC 20005

Miscellaneous

34. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

35. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

36. This Consent Order constitutes the entire agreement between the Department and the Company and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

37. Each provision of this Consent Order shall remain effective and enforceable against the Company, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

38. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

39. No promise, assurance, representation, warranty, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of this Consent Order.

40. Nothing in this Consent Order shall be construed to prevent any consumer from pursuing any right or remedy at law.

41. This Consent Order may be executed in one or more counterparts and shall become effective when such counterparts have been signed by each of the parties hereto and the Consent Order is So Ordered by the Superintendent of Financial Services or her designee (the "Effective Date").

[*remainder of this page intentionally left blank*]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s/ David A. Casler
DAVID A. CASLER
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

June 20, 2023

By: /s/ Alison L. Passer
ALISON L. PASSER
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement

June 21, 2023

By: /s/ Kevin R. Puvalowski
KEVIN R. PUVALOWSKI
Acting Executive Deputy Superintendent
Consumer Protection and Financial Enforcement

June 23, 2023

SA STONE WEALTH MANAGEMENT INC.

By: /s/ Andrew R. Chambless
ANDREW CHAMBLESS
General Counsel
SA Stone Wealth Management Inc.

June 20th, 2023

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services

July 7, 2023