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

----------x

In the Matter of :

LIFEMARK SECURITIES CORPORATION :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and LifeMark Securities Corporation ("LifeMark" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, LifeMark is licensed by the Department to sell life, accident, and health insurance in New York State;

WHEREAS**,** August 29, 2017, marked the initial effective date of New York's first-in-the-nation cybersecurity regulation, 23 NYCRR 500 (the "Cybersecurity Regulation"). The Department's 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 clearly defined 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 a Cybersecurity Event experienced within LifeMark, and LifeMark's compliance with the Cybersecurity Regulation; and

WHEREAS, based on the investigation, the Department has concluded that LifeMark violated the Cybersecurity Regulation by failing to implement written policies and procedures designed to ensure the security of its cybersecurity system and the safe-guarding of consumer, nonpublic, private data that is accessible to, or held by, its third-party service providers, in violation of 23 NYCRR § 500.11. The Department has concluded that this failure made LifeMark vulnerable to threat actors seeking to steal consumers' private and personally sensitive data.

NOW THEREFORE**,** to resolve this matter without further proceedings pursuant to the Superintendent's authority under Section 408 of the New York Financial Services Law, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the insurance regulator of the State of New York. 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 participants.

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 protection of individuals' private and personally sensitive data from careless, negligent, or willful exposure by licensees of the Department.

4. To support this critical role, the Superintendent's Cybersecurity Regulation places on all DFS-regulated entities ("Covered Entities"),[1] including LifeMark, an obligation to establish and maintain a cybersecurity program designed to protect the confidentiality and integrity of its Information Systems,[2] as well as any consumer nonpublic information ("NPI")[3] contained therein. 23 NYCRR § 500.02(b).

5. This program extends to any Third Party Service Provider(s)[4] of any Covered Entities that may have access to any NPI.

6. The Cybersecurity Regulation requires that all Covered Entities have a Third Party Service Provider(s) policy in place that is based on the Covered Entity's Risk Assessment[5] and that, among other things, addresses: (1) the identification and risk assessment of Third Party Service Providers; (2) minimum cybersecurity practices that must be met by Third Party Service Providers; (3) due diligence processes used to evaluate the adequacy of cybersecurity practices by these Third Party Service Providers; and (4) periodic assessments of Third Party Service

[1] The terms "Covered Entity" or "Covered Entities" as used herein shall have the same definition as used in 23 NYCRR § 500.01(c).
[2] The term "Information Systems" as used herein shall have the same definition as used in 23 NYCRR § 500.01(e).
[3] The terms "Nonpublic Information" or "NPI" as used herein shall have the same definition as used in 23 NYCRR § 500.01(g).
[4] The term "Third Party Service Provider(s)" as used herein shall have the same definition as used in 23 NYCRR § 500.01(n).
[5] The term "Risk Assessment" as used herein shall have the same definition as used in 23 NYCRR § 500.01(k).

Providers based on risks they present and the adequacy of their cybersecurity practices. 23 NYCRR § 500.11(a).

7. Further, a Covered Entity's cybersecurity Risk Assessment must be carried out pursuant to written policies and procedures that include: (1) criteria for evaluating and identifying cybersecurity threats; (2) criteria for the assessment of the "confidentiality, integrity, security and availability of the Covered Entity's Information Systems and [NPI]"; and (3) requirements that must be taken to address and mitigate any identified risks. 23 NYCRR § 500.09(b).

Findings of Fact

The Cybersecurity Event

8. LifeMark self-reported a Cybersecurity Event[6] to the Department on October 9, 2019. LifeMark discovered the Cybersecurity Event on September 4, 2019, when a LifeMark employee identified a suspicious request for a transfer of funds from a client's account to a fraudulent bank account.

9. LifeMark's investigation of the Cybersecurity Event revealed that a threat actor harvested employee credentials via a phishing email — *i.e.*, an email sent by a cyber attacker to deceive users into providing their credentials or personal or other confidential information to permit unauthorized access or harm to protected Information Systems — received on August 1, 2019.

10. The investigation further revealed that, on August 27, 2019, the threat actor, fraudulently posing as a LifeMark registered representative, succeeded in attacking LifeMark's Microsoft Office 365 email platform by getting LifeMark to initiate a $35,000 withdrawal of

[6] The term "Cybersecurity Event" as used herein shall have the same definition as used in 23 NYCRR § 500.01(d).

funds from a client's account and transfer the money into a bank account under the threat actor's control.

11. Upon learning of the fraudulent transfer, LifeMark immediately reimbursed the client and recovered some of the funds transferred to the fraudulent bank account.

12. Following discovery of the Cybersecurity Event, LifeMark provided notice and credit monitoring to all of its clients.

Third Party Service Provider Security Policy

13. Pursuant to Section 500.11 of the Cybersecurity Regulation, a Covered Entity must implement written policies and procedures designed to ensure the security of Information Systems and NPI that are accessible to, or held by, its Third Party Service Providers, and such policies and procedures must be based on the Covered Entity's Risk Assessment. Section 500.11 was required to be complied with no later than March 1, 2019, or two years from the effective date of the Cybersecurity Regulation. 23 NYCRR § 500.22(b)(3).

14. The Department has concluded that LifeMark did not have a Third Party Service Provider(s) security policy that met all of the requirements of Section 500.11.

15. The Department has concluded that LifeMark's lack of a compliant Third Party Service Provider(s) security policy at the time of the Cybersecurity Event left LifeMark vulnerable to threat actors.

VIOLATIONS OF LAW AND REGULATIONS

16. LifeMark failed to implement written policies and procedures designed to ensure the security of Information Systems and NPI accessible to, or held by, its Third Party Service Providers, in violation of 23 NYCRR § 500.11.

Factors Affecting the Penalty

17. In assessing an appropriate penalty for the violations it found in this case, several factors have served to substantially mitigate the penalty to be paid by LifeMark under this Consent Order. Most significantly, the Department considered LifeMark's size and revenues.

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

18. 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 Hundred Fifty Thousand U.S. Dollars ($150,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

19. 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

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

Remediation

21. LifeMark shall continue to strengthen its controls to protect its cybersecurity systems and consumers' private data and shall, in accordance with the relevant provisions and definitions of 23 NYCRR § 500, in particular as follows:

a. Third Party Provider Security Policy. Within ninety (90) days of the date of this Consent Order, LifeMark shall develop and implement written policies and procedures designed to ensure the security of Information Systems and NPI accessible to, or held by, its Third Party Service Providers, as required by 23 NYCRR § 500.11, and submit a copy of same to the Department.

b. Cybersecurity Risk Assessment. Within one hundred twenty (120) days of the date of this Consent Order, LifeMark shall conduct a comprehensive Cybersecurity Risk Assessment of its information systems consistent with 23 NYCRR § 500.09 and submit the results of the same to the Department. The Cybersecurity Risk Assessment results shall contain:

i. the reasonably necessary changes to LifeMark's plan to implement to address any issues raised in the Cybersecurity Risk Assessment;

ii. any and all plans for revisions of controls to respond to technological developments and evolving threats, which shall consider the particular risks of LifeMark's business operations related to cybersecurity, NPI collected or stored, Information Systems utilized, and the availability and effectiveness of controls to protect NPI and Information Systems; and

iii. any and all plans for updating or creating written policies and procedures to include:

1. criteria for the evaluation and categorization of identified cybersecurity risks or threats facing LifeMark;

2. criteria for the assessment of the confidentiality, integrity, security, and availability of LifeMark's Information Systems and NPI, including the adequacy of existing controls in the context of identified risks;

3. criteria for the periodic assessments of any Third Party Service Providers used by LifeMark; and

4. requirements describing how identified risks will be mitigated or accepted based on the Cybersecurity Risk Assessment and how the cybersecurity program will address the risk.

c. Training and Monitoring. Within one hundred fifty (150) days of the date of this Consent Order, LifeMark shall submit to the Department the following materials consistent with 23 NYCRR § 500.14:

i. its risk-based policies, procedures, and controls designed to: (a) monitor the activity of Authorized Users[7] and (b) detect unauthorized access or use of, or tampering with, NPI by such Authorized Users; and

ii. its most recent cybersecurity awareness training for all personnel, updated to reflect risks identified by LifeMark in its Cybersecurity Risk Assessment.

Full and Complete Cooperation

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

Waiver of Rights

23. 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.

24. The Company waives its right to further notice and hearing in this matter as to the allegations of past violations by the Department's Consumer Protection and Financial Enforcement Division up to and including the Effective Date of this Consent Order.

[7] The term "Authorized Users" as used herein shall have the same definition as used in 23 NYCRR § 500.01(b).

Parties Bound by the Consent Order

25. 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.

26. No further action will be taken by the Department against the Company for the conduct set forth in this Consent Order that was found to have violated the Cybersecurity Regulation or any other conduct that was investigated by the Department related to the Cybersecurity Regulation, 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.

Breach of Consent Order

28. 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.

29. The Company understands and agrees that its failure to make the required showing within the designated time period set forth in Paragraph 28 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

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

For the Department:

Alison L. Passer
Senior Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Madeline W. Murphy
Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One Commerce Plaza
Albany, NY 12257

Tatsiana Zhuk
Special Assistant to the Executive Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For LifeMark Securities Corporation:

Vincent Micciche
Chief Executive Officer & Chief Compliance Office
LifeMark Securities Corp.
400 West Metro Financial Center
Rochester, NY 14623

Peter W. Baldwin
Robert J. Mancuso
Faegre Drinker Biddle & Reath LLP
1177 Avenue of the Americas, 41st Floor
New York, NY 10036

Miscellaneous

31. 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.

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

33. 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.

34. 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.

35. 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.

36. 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.

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

38. Except with regard to the enforcement of this Consent Order, the Company's consent to the provisions of this Consent Order does not bar, estop, waive, or otherwise prevent the Company from raising any defenses to any action taken by any federal or state agency or department, or any private action against the Company.

39. 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 this 20th day of September, 2021.

LIFEMARK SECURITIES CORP.

By: /s
VINCENT MICCICHE
Chief Executive Officer & Chief Compliance Officer

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s
DESIREE S. MURNANE
Senior Assistant Deputy Superintendent for Consumer Protection and Financial Enforcement

By: /s
KEVIN R. PUVALOWSKI
Senior Deputy Superintendent for Consumer Protection and Financial Enforcement

By: /s
KATHERINE A. LEMIRE
Executive Deputy Superintendent for Consumer Protection and Financial Enforcement

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

By: /s
ADRIENNE A. HARRIS
Acting Superintendent of Financial Services