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

----------x

In the Matter of :

EYEMED VISION CARE LLC :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and EyeMed Vision Care LLC ("EyeMed" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS**,** EyeMed 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 Part 500 (the "Cybersecurity Regulation");

WHEREAS, the Cybersecurity Regulation defines clear 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 was promulgated to strengthen cybersecurity and data protection for the industry and consumers;

WHEREAS, the Department has been investigating a Cybersecurity Event experienced within EyeMed, as well as EyeMed's compliance with the Cybersecurity Regulation; and

WHEREAS, based on the investigation, the Department has concluded that EyeMed violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.02(b), which requires Covered Entities to maintain a cybersecurity program based on the Covered Entity's Risk Assessment; (2) 23 NYCRR § 500.03, which requires Covered Entities to implement and maintain a cybersecurity policy based on the Covered Entity's Risk Assessment and address information security, access controls and identity management, customer data privacy, and risk assessment; (3) 23 NYCRR § 500.07, which requires Covered Entities to limit user access privileges to Information Systems that provide access to Nonpublic Information; (4) 23 NYCRR § 500.09(a), which requires Covered Entities to conduct a periodic Risk Assessment of the Covered Entity's Information Systems, sufficient to inform the design of the cybersecurity program; (5) 23 NYCRR § 500.12(b), which requires Covered Entities to implement multi-factor authentication for all users, or reasonably equivalent or more secure access controls approved in writing by the Chief Information Security Officer; (6) 23 NYCRR § 500.13, which requires Covered Entities to include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information; and (7) 23 NYCRR § 500.17(b), which requires Covered Entities to annually certify compliance with the Cybersecurity Regulation.

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. 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 DFS-regulated entities ("Covered Entities"), including EyeMed, an obligation to establish and maintain a cybersecurity program, based on Risk Assessment and designed to protect the confidentiality and integrity of its Information Systems, as well as any consumer nonpublic information ("NPI") contained therein. 23 NYCRR §§ 500.01(c), 500.01(e), 500.01(g), 500.01(k), 500.02(b).

5. To inform the design of the cybersecurity program, as well as the written cybersecurity policies, Covered Entities must periodically conduct a Risk Assessment, which should be updated as necessary to address changes to the Covered Entities' Information Systems, NPI, or business operations. 23 NYCRR §§ 500.03, 500.09(a).

6. The Cybersecurity Regulation also contains requirements to protect licensed entities' internal networks from threat actors seeking to access and exploit NPI, as provided in 23 NYCRR § 500.12. Section 500.12(b) requires that Covered Entities implement Multi-Factor Authentication ("MFA") "for any individual accessing the Covered Entity's internal networks from an external network." 23 NYCRR §§ 500.01(f), 500.12(b). MFA requires two or more distinct authentication factors for successful access, such that username and password credentials alone are insufficient for access. MFA is the first line of defense against attempts to gain unauthorized access to accounts, including through phishing emails, which are emails sent by cyber attackers to deceive users into providing personal details or other confidential information to permit unauthorized access or harm to protected information systems.

7. To secure and protect customer NPI and prevent Cybersecurity Event(s), as defined below, Covered Entities shall limit user access privileges to Information Systems that provide access to NPI and shall implement "policies and procedures for the secure disposal on a periodic basis of any NPI . . . that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity." 23NYCRR § 500.07, 500.13.

8. 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 file notice of a Cybersecurity Event with the Department pursuant to the requirements of 23 NYCRR §§ 500.17(a)(1) and (a)(2).

9. Finally, Covered Entities are required to certify compliance with the Cybersecurity Regulation on an annual basis. 23 NYCRR § 500.17(b).

Events at Issue

The Cybersecurity Event

10. EyeMed reported a Cybersecurity Event to the Department on October 9, 2020 (the "Cyber Event"). EyeMed discovered that an unauthorized individual gained access to an email account used by EyeMed to process enrollment (the "Mailbox") on July 1, 2020, when phishing emails were sent to the email addresses contained in the Mailbox's address book. The Mailbox was used internally and externally by some EyeMed group clients to communicate, for example, vision care enrollment updates.

11. Nine EyeMed employees shared access to the Mailbox using the same username and password.

12. EyeMed immediately blocked the unauthorized access upon discovery of the incident, launched an investigation, and retained outside breach counsel.

13. The intrusion, which lasted from June 24, 2020, until July 1, 2020, allowed the threat actor access to, and the ability to view, emails and attachments containing consumer NPI dating back six years prior to the attack. The investigation was not able to determine how the unauthorized individual gained access to the Mailbox, but EyeMed believes that it was likely a result of a successful phishing scheme. The investigation confirmed that the threat actor had the ability to exfiltrate the documents and information within the Mailbox during the time that the threat actor was accessing the account.

14. On September 28, 2020, EyeMed began to notify the affected individuals and file regulatory notices.

MFA Implementation

15. Pursuant to Section 500.12(b) of the Cybersecurity Regulation, MFA must be

utilized for any individuals accessing a Covered Entity's internal network from an external network.

16. At the time of the Cyber Event, EyeMed was in the process of rolling out MFA for its email environment, but did not yet have MFA implemented for the Mailbox, as required by 23 NYCRR § 500.12(b) of the Cybersecurity Regulation.

17. EyeMed transitioned to using Microsoft Office 365 ("O365") for its email platform in December 2018. However, despite Section 500.12(b) becoming effective on March 1, 2018, EyeMed did not begin rolling out MFA for O365, which accessed EyeMed's internal networks, until March 2020. MFA was not fully implemented for all O365 users until of September 18, 2020.

18. The delay in MFA implementation left EyeMed's Information Systems and its consumers' NPI vulnerable to threat actors.

Risk Assessments

19. Pursuant to Section 500.09 of the Cybersecurity Regulation, "[e]ach Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Security Systems sufficient to inform the design of the cybersecurity program as required by this Part."

20. Risk Assessments constitute a core component of a robust cybersecurity program. For example, Section 500.02(b) of the Cybersecurity Regulation requires the cybersecurity program to be based on the Covered Entity's Risk Assessment, and Section 500.03 of the Cybersecurity Regulation requires the implementation of a written cybersecurity policy to be based on the Covered Entity's Risk Assessment.

21. To date, EyeMed has not conducted a Risk Assessment that complies with the requirements of the Cybersecurity Regulation, Section 500.09(a).

22. While EyeMed engaged third-party vendors to conduct periodic audits of IT controls and Enterprise Risk Management reviews, these assessments do not meet the standard required of Risk Assessments for Covered Entities contained in Section 500.09.

23. The Cyber Event was an attack on EyeMed's Enrollment Processing Mailbox, housed within O365; however, none of the assessments performed by EyeMed's vendors addressed the risks associated with the NPI stored within this Mailbox.

24. EyeMed's lack of compliant cybersecurity Risk Assessment to evaluate and address the risks to its Information Systems and NPI stored on its networks left EyeMed vulnerable to threat actors, including the threat actor who initiated the Cyber Event.

User Access Privileges and NPI Disposal

25. Pursuant to Section 500.07, Covered Entities are required to limit user access privileges to Information Systems that provide access to NPI. Further, Section 500.13 requires all Covered Entities to maintain policies and procedures for the secure periodic disposal of NPI that is no longer necessary.

26. At the time of the Cyber Event, nine EyeMed employees shared login credentials to the compromised Mailbox containing consumer NPI. As a result, the Mailbox was protected only by a weak password, shared by nine employees, which made it more vulnerable to threat actors.

27. Moreover, because EyeMed failed to implement a sufficient data minimization strategy and disposal process for the Mailbox, the compromised shared Mailbox contained old data that was accessible to the threat actor. Proper disposal processes minimize the amount of NPI accessible to an unauthorized third party during a Cyber Event.

Part 500 Compliance Certification

28. Pursuant to 23 NYCRR § 500.17(b), Covered Entities are required to annually certify their compliance with the Cybersecurity Regulation.

29. EyeMed certified compliance with the Cybersecurity Regulation for the 2017 calendar year on February 15, 2018.

30. EyeMed certified compliance with the Cybersecurity Regulation for the 2018 calendar year on February 15, 2019.

31. EyeMed certified compliance with the Cybersecurity Regulation for the 2019 calendar year on February 14, 2020.

32. EyeMed certified compliance with the Cybersecurity Regulation for the 2020 calendar year on April 15, 2021.

33. Although EyeMed's certifications were timely and, the Company asserts, made in good faith when filed, in light of the foregoing findings, EyeMed was not in compliance with the Cybersecurity Regulation at the time of the certifications.

34. Thus, EyeMed's certifications filings for the calendar years 2017 through 2020, attesting to its compliance with the Cybersecurity Regulation, were improper.

Violations of Law and Regulations

35. EyeMed did not conduct an adequate Risk Assessment, as required by the Cybersecurity Regulation, and, thus, EyeMed's cybersecurity program is not based on a Risk Assessment, in violation of 23 NYCRR § 500.02(b).

36. EyeMed did not conduct an adequate Risk Assessment, as required by the Cybersecurity Regulation, and, thus, EyeMed's cybersecurity policy is not based on a Risk Assessment, in violation of 23 NYCRR § 500.03.

37. At the time of the Cyber Event, EyeMed did not limit user access privileges to the Mailbox, in violation of 23 NYCRR § 500.07.

38. EyeMed has not conducted a periodic Risk Assessment of its Information Systems sufficient to inform the design of its cybersecurity program, in violation of 23 NYCRR § 500.09(a).

39. At the time of the Cyber Event, EyeMed had not fully implemented MFA of its O365 environment, and no reasonably equivalent or more secure access controls were approved in writing by the Company's CISO, in violation of 23 NYCRR § 500.12(b).

40. At the time of the Cyber Event, EyeMed did not have policies and procedures in place for the secure disposal on a periodic basis of NPI contained within the Mailbox that was no longer necessary for business operations or other legitimate business purpose, in violation of 23 NYCRR § 500.13.

41. EyeMed improperly certified compliance with the Cybersecurity regulation for the calendar years 2017-2020, 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

42. No later than twenty (20) business 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 Four Million, Five Hundred

Thousand U.S. Dollars ($4,500,000). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

43. 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.

44. 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.

45. 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 entity 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.

46. The Department acknowledges EyeMed's commendable cooperation throughout this investigation. The Department also recognizes and credits EyeMed's ongoing and completed efforts to remediate the shortcomings identified in this Consent Order. Among other things, EyeMed has 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.

Remediation

47. EyeMed shall continue to strengthen its controls to protect its cybersecurity systems and consumers' NPI and shall, in accordance with the relevant provisions and definitions of 23 NYCRR 500:

a. Cybersecurity Risk Assessment. Within one hundred and eighty (180) days of the date of this Consent Order, EyeMed shall conduct a comprehensive Cybersecurity Risk Assessment of its information systems consistent with 23 NYCRR § 500.09. The Cybersecurity Risk Assessment results shall contain:

i. the reasonably necessary changes EyeMed plans to implement to address any material 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 EyeMed'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 additional written policies and procedures to include:

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

2. criteria for the assessment of the confidentiality, integrity, security, and availability of EyeMed'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 EyeMed; 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 risks.

b. Action Plan. Within sixty (60) days of the completion of Cybersecurity Risk Assessment, EyeMed shall submit the results of the Cybersecurity Risk Assessment to the Department, together with a detailed Action Plan describing what steps EyeMed's plans to take to address the risks identified in the Cybersecurity Risk Assessment. The Department's approval of the Action Plan shall not be unreasonably withheld.

Full and Complete Cooperation

48. 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

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

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

Waiver of Rights

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

52. 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

53. 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

54. 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) business 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.

55. 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, Financial Services Law, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

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

For the Department:

Tatsiana Zhuk
Law Clerk
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Justin D. Parnes
Excelsior Fellow
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For EyeMed Vision Care LLC:

Jodi Adolf
Bryan Cave Leighton Paisner LLP
Counsel for EyeMed Vision Care LLC
1200 Main Street, Suite 3800
Kansas City, MO 64105

Thora Johnson
Hannah Levin
Orrick, Herrington & Sutcliffe LLP
Counsel for EyeMed Vision Care LLC
1152 15th Street N.W.
Washington, D.C. 20005

Miscellaneous

57. 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.

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

59. 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.

60. 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.

61. 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.

62. No promise, assurance, representation, 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.

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

64. 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 (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/ Madeline W. Murphy
MADELINE W. MURPHY
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

October 17, 2022

By: /s/ Christopher B. Mulvihill
CHRISTOPHER B. MULVIHILL
Deputy Superintendent for
Consumer Protection and Financial Enforcement

October 17, 2022

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

October 17, 2022

EYEMED VISION CARE LLC

By: /s/ Sara Francescutto
SARA FRANCESCUTTO
Chief Financial Officer

October 12, 2022

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

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

October 18, 2022