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

----------x

In the Matter of :

FIRST UNUM LIFE INSURANCE COMPANY, and
THE PAUL REVERE LIFE INSURANCE COMPANY :

----------x

## CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and First Unum Life Insurance Company ("First Unum") and The Paul Revere Life Insurance Company ("Paul Revere") agree to resolve the matters described herein without further proceedings.

## INTRODUCTION

**WHEREAS,** First Unum, and Paul Revere are collectively referred to herein as the "Companies;"

**WHEREAS**, First Unum and Paul Revere are licensed by the Department to sell life 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").

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 standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, timely reporting of cybersecurity events, and enforcement were promulgated to strengthen cybersecurity and data protection for the industry and consumers;

**WHEREAS,** the Department has been investigating certain Cybersecurity Events, as defined by 23 NYCRR § 500.01(d), experienced within First Unum, and First Unum's compliance with the Cybersecurity Regulation; and

**WHEREAS**, based on the investigation, the Department has concluded that the Companies violated the following sections of the Cybersecurity Regulation: (1) the Companies' O365 email environments did not have multi-factor authentication ("MFA") fully implemented for all users until August 29, 2019, and no reasonably equivalent or more secure access controls than MFA were approved in writing by the Companies' Chief Information Security Officer(s) ("CISO"), in violation of 23 NYCRR § 500.12(b); (2) a misconfiguration error in MFA settings exposed a broad set of First Unum IP addresses to unauthorized third-party access in further violation of 23 NYCRR § 500.12(b); and (3) First Unum and Paul Revere falsely certified compliance with the Cybersecurity Regulation for the calendar year 2018, in violation of 23 NYCRR § 500.17(b).

**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, 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 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 the Superintendent's many obligations to the public is a 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 obligation, one provision of the Cybersecurity Regulation, specifically, 23 NYCRR § 500.02(b), places on all DFS-regulated entities ("Covered Entities"[1]) an obligation to establish and maintain a cybersecurity program designed to protect the confidentiality and integrity of its Information Systems, as well as any consumer non-public information ("NPI"[2]) contained therein.

5. In addition to measures that require Covered Entities to certify compliance with the Cybersecurity Regulation on an annual basis, pursuant to 23 NYCRR § 500.17(b), the Cybersecurity Regulation also contains requirements to protect licensed entities' internal

[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 terms "Nonpublic Information" or "NPI" used herein shall have the same definition as used in 23 NYCRR § 500.01(g).

networks from threat actors seeking to access and exploit NPI, as provided in 23 NYCRR § 500.12.

6. Section 500.12(b), for example, requires that Covered Entities implement multi-factor authentication ("MFA") "for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's Chief Information Security Officer ("CISO") has approved in writing the use of reasonably equivalent or more secure access controls."[3] 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.

**Findings of Fact**

*The First Cybersecurity Event*

7. First Unum reported a Cybersecurity Event[4] to the Department on November 30, 2018 (the "First Cyber Event"). First Unum initially discovered the First Cyber Event on September 20, 2018, when a phishing email was sent to a large number of employees' electronic mailboxes. That email, which purported to be sent by an executive of First Unum's parent company, contained a link to a fake Microsoft Office 365 ("O365") login page and was designed to harvest employee credentials to the O365 system.

[3] The terms "multi-factor authentication" and "MFA" used herein shall have the same definition as used in 23 NYCRR § 500.01(f).
[4] The term "Cybersecurity Event" used herein shall have the same definition as used in 23 NYCRR § 500.01(d).

8. Pursuant to its incident response plan, First Unum immediately launched an investigation into whether the executive's email account or other email accounts had been compromised, and proceeded to take actions to stop any ongoing access.

9. First Unum's investigation determined that the First Cyber Event enabled an unauthorized third-party to obtain O365 credentials from a number of employees. The investigation also determined that consumer NPI was accessible by the unauthorized third party between June 1, 2018, and October 20, 2018.

10. The NPI of certain customers was impacted by the First Cyber Event, including both New York and non-New York residents. First Unum provided notice and credit monitoring to those individuals.

11. The First Cyber Event also affected Paul Revere. The NPI of certain Paul Revere customers was impacted, including both New York and non-New York residents. Paul Revere provided notice and credit monitoring to those individuals.

12. At the time of the First Cyber Event, neither First Unum nor Paul Revere had MFA fully implemented for their respective email environments, as required by Section 500.12(b) of the Cybersecurity Regulation.

*The Second Cybersecurity Event*

13. First Unum reported a Cybersecurity Event to the Department on November 25, 2019 (the "Second Cyber Event"). First Unum initially discovered the Second Cyber Event on October 10, 2019, when a First Unum Sales Account Executive reported that his electronic mailbox was sending suspicious emails that he had not drafted.

14. Following a prompt investigation pursuant to its incident response plan, First Unum determined that another phishing attack had compromised fifteen (15) O365 email accounts between October 1, 2019, and October 10, 2019.

15. The NPI of certain customers was impacted by the Second Cyber Event, including both New York and non-New York residents. First Unum provided notice and credit monitoring to those individuals.

16. At the time of the Second Cyber Event (approximately a year after the First Cyber Event), although MFA had been implemented for First Unum's email environment, a misconfiguration error in a range of whitelisted Internet Protocol ("IP") addresses allowed an unauthorized third-party to bypass MFA and gain access to the compromised accounts. "Whitelisting" refers to the process of listing specific, trusted IP addresses (such as service accounts that do not have interactive log on) that can gain access to a system, sometimes without the need to go through security protocols such as MFA. In this case, instead of the intended limited number of IP addresses, the misconfiguration error allowed a broader set of IP addresses to bypass the MFA setting, and that broader set made the system vulnerable for the second phishing attack.

*Multi-factor Authentication on First Unum's and Paul Revere's Email Environments*

17. Pursuant to Section 500.12(b) of the Cybersecurity Regulation, MFA "shall be utilized for any individual accessing [a] Covered Entity's internal network from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls." Section 500.12(b) became effective on March 1, 2018. *See* Section 500.22(b)(1).

18. As of March 1, 2018, First Unum's Outlook Web Access ("OWA") system, the email platform used by First Unum, did not utilize MFA. The OWA portal sat behind First Unum's firewall, but OWA was accessible without MFA.

19. First Unum began migrating a small number of email accounts from traditional Outlook email accounts accessible through OWA to O365 Outlook email accounts in May 2017. By August 1, 2018, approximately 27% of First Unum's user base had been migrated to O365. On January 16, 2019, First Unum completed the MFA roll-out for these users.

20. First Unum implemented MFA simultaneously with the provisioning of O365 to the remaining employees, which took place on a rolling basis, with the migration of all employee accounts not being completed until August 29, 2019, almost a year and a half after the Cybersecurity Regulation requiring MFA became effective.

21. Paul Revere has the same cybersecurity program in place as First Unum and was part of the same MFA migration that was completed on August 29, 2019, almost a year and a half after the Cybersecurity Regulation required MFA.

22. During the period between the effective date of Section 500.12(b) and the date MFA was fully implemented on their email environments, First Unum and Paul Revere had certain controls designed to protect the OWA environment.

23. These controls, however, fell short of the Section 500.12(b) standard, requiring Covered Entities to have "reasonably equivalent or more secure access controls" than MFA in place. Further, First Unum and Paul Revere did not present sufficient evidence that these controls were approved in writing by the entities' CISO, as required by Section 500.12(b).

*Multi-factor Authentication on First Unum's Whitelisted Accounts*

24. A misconfiguration error in MFA settings allowed a broader set of IP addresses to bypass the MFA setting and allowed the unauthorized third-party to gain access to the compromised accounts.

25. This misconfiguration error left First Unum open to the Second Cyber Event.

*Part 500 Compliance Certification*

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

27. First Unum certified compliance with the Cybersecurity Regulation for the 2018 calendar year on February 8, 2019.

28. Paul Revere certified compliance with the Cybersecurity Regulation for the 2018 calendar year on February 8, 2019.

29. While First Unum and Paul Revere timely certified compliance for the 2018 calendar year, due to the foregoing failures with respect to MFA implementation, First Unum and Paul Revere were not in compliance with the Cybersecurity Regulation at the time of certification.

30. Thus, First Unum's and Paul Revere's filings of Certifications of Compliance, attesting to compliance with the Cybersecurity Regulation for the 2018 calendar year, were false, in violation of Section 500.17(b).

## VIOLATIONS OF LAW AND REGULATIONS

31. The First Unum and Paul Revere's O365 email environments, which accessed their internal networks, did not fully implement MFA for all users until August 29, 2019, and no reasonably equivalent or more secure access controls were approved in writing by the entities'

CISO, in violation of 23 NYCRR § 500.12(b).

32. First Unum's MFA misconfiguration of a whitelist allowed a number of IP addresses to bypass the MFA setting between July 2019 and October 2019, in violation of 23 NYCRR § 500.12(b).

33. First Unum and Paul Revere falsely certified compliance with the Cybersecurity Regulation for the calendar year 2018, in violation of 23 NYCRR § 500.17(b).

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

## SETTLEMENT PROVISIONS

### Monetary Penalty

34. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, the Companies shall pay a total civil monetary penalty pursuant to Financial Services Law § 408 to the Department in the amount of One Million Eight Hundred Thousand U.S. Dollars ($1,800,000). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

35. The Companies 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.

36. The Companies 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.

37. 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 Companies have 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.

38. The Department acknowledges the Companies' commendable cooperation throughout this investigation. The Department also recognizes and credits the Companies' ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, the Companies demonstrated their commitment to remediation by devoting significant financial and other resources to enhance their cybersecurity program, including through changes to their policies, procedures, systems, and governance structures. In addition, the Company has demonstrated it had a cybersecurity program in place at the time of the Cyber Events that included, among other things, training for employees and an incident response plan.

**Remediation**

39. The Companies shall continue to strengthen their controls to protect their 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 twenty (120) days of the date of this Order, First Unum and Paul Revere shall conduct a comprehensive Cybersecurity Risk Assessment of their 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 First Unum and Paul Revere plan 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 First Unum's and Paul Revere'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;

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 First Unum and Paul Revere;

2. criteria for the assessment of the confidentiality, integrity, security, and availability of First Unum'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 First Unum and Paul Revere; and

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

b. Independent Third-Party Audit of MFA Controls. Within one hundred twenty (120) days of the date of this Order, the Companies shall have a third-party audit conducted of current MFA controls in the various environments utilized by First Unum and Paul Revere and submit the results of the same to the Department. Upon completion, a copy of the third-party audit will be provided to the Department. To the extent any material issues are discovered, the Companies are to remediate those issues within a reasonable timeframe agreed to by the

Department following the issuance of any report or findings by the third-party conducting said audit.

**Full and Complete Cooperation**

40. The Companies commit and agree that they will fully cooperate with the Department regarding all terms of this Consent Order.

**Waiver of Rights**

41. 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**

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

43. No further action will be taken by the Department against the Companies for the conduct set forth in this Consent Order that was found to have violated the Cybersecurity Regulation, provided that the Companies fully comply with the terms of the Consent Order. Furthermore, no further action will be taken by the Department against the Companies for conduct in connection with the Department's investigation.

44. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against the Companies 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**

45. In the event that the Department believes the Companies to be in material breach of the Consent Order, the Department will provide written notice to the Companies of the breach. Within ten (10) days of receiving such notice, or on a later date if so determined in the Department's sole discretion, the Companies must 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.

46. The Companies understand and agree that their failure to make the required showing within the designated time period set forth in Paragraph 45 shall be presumptive evidence of the Companies' 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, or any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

**Notices**

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

For the Department:

Laura Sarli
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

Patrick B. Kim
Assistant Counsel
Cybersecurity Division
New York State Department of Financial Services
One State Street
New York, NY 10004

For First Unum Life Insurance Company and The Paul Revere Life Insurance Company:

Lisa G. Iglesias
Executive Vice President & General Counsel
1 Fountain Square
Chattanooga, TN 37402

Timothy P. Tobin
Hogan Lovells US LLP
555 Thirteenth Street NW
Washington, DC 20004

**Miscellaneous**

48. 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.

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

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

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

52. 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.

53. 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.

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

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

56. 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 12th day of May, 2021.

**FIRST UNUM LIFE INSURANCE COMPANY**

**THE PAUL REVERE LIFE INSURANCE COMPANY**

By: /s
PUNEET BHASIN
Executive Vice President
Chief Information and Digital 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

By: /s
LINDA A. LACEWELL
Superintendent of Financial Services