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

----------x

In the Matter of :

CARNIVAL CORPORATION d/b/a CARNIVAL CRUISE LINE;
PRINCESS CRUISE LINES, LTD; :
HOLLAND AMERICA LINE NV;
SEABOURN CRUISE LINE, LTD; and
COSTA CRUISE LINES, INC. :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and Carnival Corporation d/b/a Carnival Cruise Line ("Carnival"); Princess Cruise Lines, LTD ("Princess"); Holland America Line NV ("Holland"); Seabourn Cruise Line, LTD ("Seabourn"); and Costa Cruise Lines, Inc. ("Costa") (collectively referred to herein as the "Carnival Companies" or the "Companies") agree to resolve the matters described herein without further proceedings.

WHEREAS, the Carnival Companies are licensed by the Department to sell life insurance, accident and health insurance, and variable life/variable annuities 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");

WHEREAS**,** the Cybersecurity Regulation defines clear standards and guidelines 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 four Cybersecurity Events experienced within the Carnival Companies, as well as the Carnival Companies' compliance with the Cybersecurity Regulation; and

WHEREAS, based on the investigation, the Department has concluded that the Carnival Companies violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.12(b), which requires Covered Entities to implement multi-factor authentication for individuals accessing a Covered Entity's internal network from an external network, or reasonably equivalent or more secure access controls approved in writing by the Chief Information Security Officer; (2) 23 NYCRR § 500.02(b)(6), which requires Covered Entities to fulfill applicable regulatory reporting obligations as part of their cybersecurity program; (3) 23 NYCRR § 500.17(a), which requires Covered Entities to notify the Department of Cybersecurity Events within 72 hours of a determination that: (i) notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body, or (ii) there is a reasonable likelihood of material harm to any material part of the operation(s) of the Covered

Entity; (4) 23 NYCRR § 500.14(a), which requires Covered Entities to implement sufficient risk-based policies and procedures designed to detect unauthorized access or use of, or tampering with, nonpublic information; and (5) 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 the Carnival Companies, 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 nonpublic

information ("NPI") contained therein. 23 NYCRR §§ 500.01(c), 500.01(e), 500.01(g), 500.02(b).

5. The importance of securing consumer NPI is paramount, especially in the current digital age as criminals seek to steal consumer data and utilize the data to cause financial harm. With this key goal in mind, cybersecurity programs must, at a minimum: (1) include effective controls and secure access privileges; (2) include systems and policies in place for conducting thorough and routine cybersecurity risk assessments; and (3) provide for comprehensive training and monitoring for all employees and users, including independent contractors and vendors.

6. Further, Covered Entities must have well-grounded governance processes in place, with adequate board reporting, to ensure senior management's attention to securing and protecting consumer NPI and preventing Cybersecurity Event(s), as defined below.

7. In an effort to prevent unauthorized access, Section 500.12 of the Superintendent's Cybersecurity Regulation requires that Covered Entities implement multi-factor authentication ("MFA") when there is external access to a Covered Entity's internal network. 23 NYCRR §§ 500.01(f), 500.12. MFA requires more than one distinct authentication factor for successful access, such that a username and password alone are not sufficient to access an email account and its contents. MFA is the first line of defense against attempts to gain unauthorized access, including through phishing emails, which are emails sent by cyber criminals to deceive users into providing personal details or other confidential information to permit unauthorized access or harm to a protected information system.

8. In furtherance of the goal of protecting NPI, Section 500.14(a) of the Superintendent's Cybersecurity Regulation further requires that Covered Entities "implement risk-based policies, procedures and controls designed to . . . detect unauthorized access or use of,

or tampering with, Nonpublic Information" by Authorized Users. 23 NYCRR §§ 500.01(b), 500.14(a).

9. Each of the foregoing requirements are part of each Covered Entities' cybersecurity program, which must be "designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems" and perform core cybersecurity functions. 23 NYCRR § 500.02.

10. Absent an effective cybersecurity program that complies with 23 NYCRR § 500.02, a Covered Entity runs the risk of not only leaving its own Information Systems vulnerable to attack and intrusion by threat actors, but also allowing consumer NPI to be accessed and exploited.

11. 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). Section 500.17(a)(1) requires notice to the Superintendent, within 72 hours of determining there has been a Cybersecurity Event, when notices are "required to be provided to any government body, self-regulatory agency or any other supervisory body."

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

The Facts at Issue

Background

13. The Carnival Companies are licensed by the Department to sell life insurance, accident and health insurance, and variable life/variable annuities insurance in New York State.

As such, the Carnival Companies are "Covered Entities" under the Cybersecurity Regulation. 23 NYCRR §500.01(c).

14. The Carnival Companies share a cybersecurity program, which is overseen by a Chief Information Security Officer ("CISO").

The First Cybersecurity Event

15. On April 20, 2020, the Carnival Companies reported a Cybersecurity Event to the Department (the "First Cyber Event"). The Carnival Companies became aware of suspicious email activity on May 22, 2019, when the Carnival Companies' Threat Intel/Security Operations Team received a service desk ticket indicating that a company email account was sending spam to other internal email accounts.

16. After an extensive internal investigation, the Carnival Companies concluded that between approximately April 11, 2019, and July 29, 2019, one or more unauthorized parties had gained access to one hundred and twenty-four (124) employee email accounts hosted primarily on Microsoft's Office 365 ("O365") platform and used that access to send a series of phishing emails — *i.e.*, an email sent by threat actors to deceive users into providing their credentials, or personal or other confidential information, to permit unauthorized access or harm to protected information systems — to other employees. The First Cyber Event affected the Information Systems of Carnival, Holland, and Princess.

17. This unauthorized access to employee email accounts resulted in the exposure of emails and attachments that contained NPI belonging to the Companies' consumers and employees.

18. The Carnival Companies believed that the initial unauthorized access likely occurred due to (a) a phishing email; or (b) a password spray attack — *i.e.*, a brute force attack

where a threat actor attempts to gain unauthorized access to accounts by attempting the same password on many accounts before moving on to another one and repeating the process over and over again in a very short period of time.

19. The NPI of consumers, including hundreds New York residents, was affected by the First Cyber Event. The types of potentially exposed NPI included names, addresses, and government identification information — such as passport numbers or driver's license numbers. Potentially exposed information also included comparatively smaller numbers of Social Security numbers and credit card and financial account information. The Carnival Companies provided credit counseling to all affected individuals.

20. Though the Carnival Companies became aware of the First Cyber Event in May 2019, due to the omission of the Department's notification requirement from the Carnival Companies' incident response plan (23 NYCRR § 500.16(b)(6)), the Carnival Companies did not notify the Department of the event, as mandated by 23 NYCRR § 500.17(a), until April 2020.

21. At the time of the First Cyber Event, Princess had not completed the rollout of MFA on its O365 environment, even though the Cybersecurity Regulation's MFA requirement had become effective on March 1, 2018.

Three Additional Cybersecurity Events

22. On August 19, 2020, the Carnival Companies reported another Cybersecurity Event, a ransomware attack, to the Department (the "Second Cyber Event"). The ransomware attack accessed and encrypted certain of the Carnival Companies' Information Systems, and certain data files were exfiltrated. Some of the consumer NPI exposed included consumer names, addresses, dates of birth, passport numbers, and in some limited instances, employee social

security numbers, and private health information. The data belonged to consumers and employees of Seabourn, Holland, and Carnival.

23. On January 7, 2021, the Carnival Companies reported a third cybersecurity event, another ransomware attack, to the Department (the "Third Cyber Event"). On December 25, 2020, the Carnival Companies learned that a threat actor had deployed malware, encrypted a number of Costa's computer systems (along with those of another affiliate), and downloaded a number of data files containing customer passport numbers and dates of birth and employee credit card numbers. An internal investigation revealed that the malware virus had been sent via a phishing e-mail.

24. On March 26, 2021, the Carnival Companies reported a fourth cybersecurity event to the Department (the "Fourth Cyber Event"). The Companies reported that, on March 19, 2021, they became aware of a phishing e-mail being sent from an employee's e-mail account. Upon further investigation, it was uncovered that a threat actor had gained access to the employee's credentials through a phishing scheme, then sent the phishing e-mail from the compromised e-mail account. The Fourth Cyber Event impacted Carnival's, Holland's, and Princess' Information Systems and led to the exposure of NPI belonging to the Carnival Companies' guests, employees, and crew, including names, addresses, phone numbers, passport numbers, dates of birth, health information, and, in some limited instances, social security and national identification numbers.

25. The Carnival Companies provided credit monitoring and identity theft protection to consumers impacted by the Second, Third, and Fourth Cyber Events.

MFA Implementation

26. As discussed above, 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. All Covered Entities were required to have MFA in place by March 1, 2018, the effective date of Section 500.12(b).

27. As of April 11, 2019, the date when unauthorized access for the First Cyber Event first occurred, *i.e.*, over a year past the effective date of Section 500.12(b), the Carnival Companies had not completed implementation of MFA on Princess' O365 environment.

Training

28. Section 500.14 of the Cybersecurity Regulation calls for regular cybersecurity awareness training for all personnel. Covered Entities must "implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, nonpublic information by such authorized users." 23 NYCRR § 500.14(a).

29. Given the occurrence of four cybersecurity events, with at least some being the result of successful phishing attacks, all within a period of less than four years demonstrates that the Carnival Companies' training was inadequate.

Part 500 Compliance Certification

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

31. The Companies' CISO certified compliance with the Cybersecurity Regulation for the 2018 calendar year on February 14, 2019.

32. The Companies' CISO certified compliance with the Cybersecurity Regulation for the 2019 calendar year on April 23, 2020.

33. The Companies' CISO certified compliance with the Cybersecurity Regulation for the 2020 calendar year on April 15, 2021.

34. Although the Companies' certifications were timely, due to the foregoing failures, the Companies were not in compliance with the Cybersecurity Regulation at the time of the certifications.

35. Thus, the Companies' certification filings for the 2018, 2019, and 2020 calendar years, attesting to their compliance with the Cybersecurity Regulation, were improper.

Department's Violations of Law and Regulations

36. Based upon the foregoing, Department finds that the Carnival Companies violated the following provisions of the Cybersecurity Regulation:

a. 23 NYCRR § 500.12(b);

b. 23 NYCRR § 500.02(b)(6);

c. 23 NYCRR § 500.17(a);

d. 23 NYCRR § 500.14(a); and

e. 23 NYCRR § 500.17(b).

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

SETTLEMENT PROVISIONS

Monetary Penalty

37. No later than ten (10) business days after the Effective Date (as defined below) of this Consent Order, the Carnival Companies shall pay a total civil monetary penalty pursuant to Financial Services Law § 408 to the Department in the amount of Five Million U.S. Dollars

($5,000,000). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

38. The Carnival 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.

39. The Carnival 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.

40. 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 Carnival Companies have cooperated with the Department in the investigation, and such other matters as justice and the public interest may require.

Surrender of Licenses

41. In letters dated August 5, 2021, and August 17, 2021, the Carnival Companies submitted applications to the Department that sought the return of all of its licenses, including any licenses held by sublicensees (including James Colwell and Carol Pennington). At or around those dates, the Carnival Companies ceased the sale of insurance to residents of New York State.

42. With the execution of this Consent Order, the Carnival Companies hereby surrender any and all licenses issued to them by the Department and consent to the denial of any and all pending applications for licenses, such surrender and denial having the same force and effect as if said licenses had been revoked or denied after a hearing.

43. The Department agrees and hereby accepts the surrender of any and all licenses issued by it to the Carnival Companies and hereby denies any and all pending applications for

licenses, such surrender and denial having the same force and effect as if said licenses had been revoked or denied after a hearing.

Full and Complete Cooperation

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

Further Action by the Department

45. No further action will be taken by the Department against the Carnival Companies or its successors for any conduct involving the Department's Cybersecurity Regulation through the date of this Consent Order, provided that the Carnival Companies fully comply with the terms of the Consent Order.

Waiver of Rights

46. The Carnival Companies submit to the authority of the Superintendent to effectuate this Consent Order.

47. 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

48. This Consent Order is binding on the Department and the Carnival 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.

Breach of Consent Order

49. In the event that the Department believes the Carnival 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) business days of receiving such notice, or on a later

date if so determined in the Department's sole discretion, the Carnival 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.

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

Notices

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

For the Department:

Madeline W. Murphy
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement
New York State Department of Financial Service
One Commerce Plaza, 20th Floor
Albany, New York 12257

Terri-Anne S. Caplan
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For the Carnival Companies:

Enrique Miguez
General Counsel
3655 N.W. 87th Avenue
Miami, FL 33178-2428

Miscellaneous

52. 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.

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

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

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

56. 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.

57. 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.

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

59. 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 for Consumer Protection and Financial Enforcement

June 23, 2022

By: /s/ Terri-Anne S. Caplan
TERRI-ANNE S. CAPLAN
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement

June 23, 2022

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

June 23, 2022

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

June 23, 2022

CARNIVAL CORPORATION d/b/a CARNIVAL CRUISE LINES

By: /s/ Enrique Miguez
ENRIQUE MIGUEZ
General Counsel

June 22, 2022

PRINCESS CRUISE LINES, LTD

By: /s/ Enriquez Miguez
ENRIQUE MIGUEZ
General Counsel

June 22, 2022

HOLLAND AMERICA LINE NV

By: /s/ Enrique Miguez
ENRIQUE MIGUEZ
General Counsel

June 22, 2022

SEABOURN CRUISE LINE, LTD

By: /s/ Enrique Miguez
ENRIQUE MIGUEZ
General Counsel

June 22, 2022

COSTA CRUISE LINES, INC.

By: /s/ Enrique Miguez
ENRIQUE MIGUEZ
General Counsel

June 22, 2022

ORRICK

By: /s/ Aravind Swaminathan
ARAVIND SWAMINATHAN
Counsel to the Carnival Companies

June 22, 2022

ORRICK

By: /s/ Jonathan A. Direnfeld
JONATHAN A. DIRENFELD
Counsel to the Carnival Companies

June 22, 2022

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

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

June 23, 2022