RECEIVED
ATTORNEY GENERAL OF OHIO

DEC 2 8 2020

CONSUMER PROTECTION SECTION
PUBLIC INSPECTION FILE

IN THE MATTER OF:)

SABRE CORPORATION.)

DOCKET NO: 538687)

ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance ("Assurance") is entered into by the Attorneys General of Alaska, Arizona, Arkansas, Connecticut,[1] Florida, Hawaii,[2] Illinois, Indiana, Iowa, Louisiana, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Tennessee, Vermont, Virginia, and Washington (referred to collectively as the "Attorneys General") and SABRE, as defined below (collectively, with the Attorneys General, the "Parties"), to resolve the Attorneys General's investigation into the security incident announced by SABRE on or about June 6, 2017.

In consideration of their mutual agreements to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

I. INTRODUCTION

This Assurance constitutes a good faith settlement and release between SABRE and the Attorneys General of claims related to a data breach, publicly announced by SABRE on June 6, 2017, in which a person or persons gained unauthorized access to portions of SHS (defined

[1] Connecticut shall include both the Office of the Attorney General and the Office of the Attorney General acting on behalf of the Commissioner of Consumer Protection.

[2] Hawaii is represented by its Office of Consumer Protection, an agency which is not part of the state Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. For simplicity purposes, the entire group will be referred to as the "Attorneys General," or individually as "Attorney General" and the designations, as they pertain to Hawaii, refer to the Executive Director of the State of Hawaii Office of Consumer Protection.

below) SynXis (defined below) that maintains payment card and reservation information (hereinafter referred to as the "Breach").

II. DEFINITIONS

1. For the purposes of this Assurance, the following definitions shall apply:

   A. "Cardholder Data Environment" shall mean SHS's technologies that store, process, or transmit payment card authentication data, consistent with the Payment Card Industry Data Security Standard ("PCI DSS").

   B. "Consumer" shall mean any individual who makes a reservation with a Hotel Customer.

   C. "Consumer Protection Acts" shall mean the State citations listed in Appendix A.

   D. "Channel Partner" means an entity that directly provides Personal Information to a third-party business entity that contracts for and/or uses SynXis for the purpose of facilitating hotel bookings on behalf of Consumers. This term shall not include Hotel Customers.

   E. "Days" shall mean calendar days unless otherwise specified.

   F. "Effective Date" shall be the date on which SABRE receives a copy of this Assurance duly executed in full by SABRE and by each of the Attorneys General.

   G. "Hotel Customer" shall mean a hotel or hotel brand which contracts for and/or uses SynXis.

H. "Personal Information" shall mean the data elements in the definitions of personal information set forth in the Security Breach Notification Acts and/or Personal Information Protection Acts.

I. "Personal Information Protection Acts" shall mean the State citations listed in Appendix B.

J. "Security Breach Notification Acts" shall mean the State citations listed in Appendix B.

K. "SABRE" shall mean Sabre Corporation, its affiliates, subsidiaries and divisions, successors, and assigns doing business in the United States.

L. "Security Event" shall mean any compromise to the confidentiality, integrity, or availability of a SHS information asset that presents a reasonable likelihood of unauthorized access to Personal Information.

M. "SHS" shall mean Sabre Hospitality Solutions, a business segment of SABRE.

N. "SynXis" shall mean the SynXis Central Reservation system operated by SHS, as well as any future versions or releases of SynXis owned and controlled by SABRE. In the event that the SynXis system is retired, discontinued, or disabled and another system is enabled to permit substantially similar functions, "SynXis" shall include the new system owned and controlled by SABRE.

III. APPLICATION

2. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to SABRE and its officers, employees, and directors.

IV. BACKGROUND

3. SHS operates SynXis. SynXis is an interface that facilitates the booking of hotel reservations for Hotel Customers. SynXis allows Hotel Customers to configure what data they receive, according to their own preferences. Hotel Customers retrieve booking information from SynXis in two ways: (1) automated integrations with their own property management system (PMS); or (2) manual access and export. When a Hotel Customer's PMS is integrated with SynXis, SynXis automatically "pushes" reservation data from SynXis to the PMS (and, in some cases, from the PMS back to SynXis). When a Hotel Customer accesses SynXis manually, the Hotel Customer's personnel can view and export a variety of information about reservations. If a Hotel Customer has configured their SynXis account to require payment information in order to complete a booking and the Hotel Customer's personnel has appropriate privileges to view such information, the payment information—including a Consumer's credit card number, expiration date, and, in some cases, CVV code—may be made visible to such personnel on a credit card summary page.

4. From August 10, 2016 through March 9, 2017, an attacker was able to regularly access SynXis and view credit card information, including credit card number, expiration date, and authorization code, displayed on a summary page intended for Hotel Customers. The amount of activity varied, but during certain months, the attacker accessed the summary pages daily.

5. Throughout this period, to access the credit card summary pages, the attacker was able to compromise and exploit an administrator-level account, ESite, within SynXis. The password for this account was stored in plain text within SynXis.

6. Further, the attacker was able to create an unauthorized account, ESynxis, to view additional credit card summary pages. While SABRE detected and disabled this unauthorized account in August 2016, it did not further investigate.

7. On March 9, 2017, while investigating a report about an unrelated incident, SABRE noticed unusual activity associated with the ESite account. SABRE disabled the account's access to the credit card summary page and queued it for further investigation, but did not fully disable the account. As a result, the attacker continued to use ESite to access other administrator pages—which did not display Personal Information—after this date.

8. Beginning on March 29, 2017, and continuing over the next two weeks, SABRE received reports from online travel agencies of suspicious activity associated with approximately forty reservations booked through SynXis.

9. SABRE began investigating a potential Security Event on or about April 10, 2017 and did not fully disable the ESite account until April 13, 2017.

10. On May 2, 2017, SABRE disclosed the Breach in its quarterly 10-Q SEC filing and on May 3, 2017 it notified the payment card brands about the Breach.

11. SABRE estimates the number of Consumer payment cards potentially affected by the Breach to be approximately 1.3 million, though the actual number may be lower because a significant amount of reservations in SynXis were made through virtual cards, corporate cards, or using the same payment card for multiple reservations.

12. SABRE began informing potentially affected Hotel Customers of the Breach on June 6, 2017, almost two months after it started investigating and one month after it informed the payment card brands.

13. SABRE did not have sufficient information to determine whether notification to individual Consumers would be appropriate.

14. As a result, SABRE provided template notices to its Hotel Customers and left it to each Hotel Customer's discretion to determine whether there was a legal obligation to notify consumers and to provide such notice.

15. The potentially affected Consumers did not receive notice until months after SABRE discovered the Breach, with some notices not going out until the late 2017 or early 2018.

V. ASSURANCES

Compliance with State Laws and Industry Standards

16. SABRE shall comply with the Consumer Protection Acts and the Personal Information Protection Acts in connection with its collection, maintenance, and safeguarding and disposal of Personal Information and shall maintain reasonable security policies and procedures designed to protect or safeguard Consumers' Personal Information from unauthorized access, use, or disclosure.

17. SABRE shall comply with the Security Breach Notification Acts.

a. In particular, when SABRE has determined it experienced a security breach, as defined under the Security Breach Notification Acts, involving Personal Information owned or licensed by its Channel Partners or Hotel Customers, SABRE will promptly provide notice to its Channel Partners or Hotel Customers and to the Attorneys General, as appropriate.

b. Where SABRE determines that a Security Event did not result in unauthorized access to Personal Information and, as such, does not require reporting under the Security Breach Notification Acts, SABRE shall create a report that

includes a description of the Security Event and SABRE's response to that Security Event ("Security Event Report"). SABRE shall make the Security Event Report available to the Attorneys General upon request.

18. SABRE shall comply with the PCI DSS, or an alternative standard acceptable to the payment card industry should one be developed, with respect to its Cardholder Data Environment and any SABRE system component the compromise of which SABRE reasonably believes would impact the security of the Cardholder Data Environment.

Breach Notification

19. SHS shall include in any future contract for travel services the roles and responsibilities to be undertaken by SABRE and the counterparty in the event of a breach as defined under the Security Breach Notification Acts, including which party will be responsible for providing notice to consumers and the requisite timeframes for notice. SHS shall ensure that any such provision complies with all applicable laws and that information requested via legal process may be furnished to regulators unless SHS or a customer takes legal action to resolve any dispute about the validity of such legal process.

20. In particular, when SABRE has determined it experienced a security breach, as defined under the Security Breach Notification Acts, involving Personal Information owned or licensed by its Channel Partners or Hotel Customers, it will promptly provide information to its Channel Partners or Hotel Customers concerning the breach details, scope, and the categories of information compromised. If SABRE does not provide notice directly to Consumers, SABRE shall take reasonable steps to inquire as to Channel Partners' or Hotel Customers' individual determinations regarding whether they are required to provide notice to Consumers, and if such notice is made, when Channel Partners or Hotel Customers issued notice to Consumers ("Notice

Log"). Upon providing notice to its Hotel Customers as described under Paragraph 17(a) herein, SHS will also provide a list of notified Hotel Customers to the Vermont Attorney General. Sixty (60) days after providing this list, SHS will provide the Notice Log to the Vermont Attorney General. The Vermont Attorney General shall make the reports available to other Attorneys General upon request.

Hotel Customer Interaction

21. SHS shall recommend to its Hotel Customers that they implement a token-based electronic payment system or virtual credit card system for all end users.

Information Security Program

22. SABRE shall develop, implement, and maintain a written information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information that SABRE collects, stores, transmits, and/or maintains. The Information Security Program shall, at a minimum, include the specific information security requirements set forth in Paragraphs 22 through 36 of this Assurance.

a. The Information Security Program shall be at least compliant with any applicable requirements under state or federal law, and at a minimum, shall be written and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of SABRE's operations; (ii) the nature and scope of SABRE's activities; and (iii) the sensitivity of the Personal Information that SABRE collects, stores, transmits, and/ or maintains.

b. The Information Security Program shall be written and modified using a zero-trust approach both for internal systems and for remote access, allowing access to users only to the extent necessary and requiring verification prior to allowing any such access.

c. SABRE shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program (hereinafter referred to as the Chief Information Security Officer ("CISO")). The CISO shall have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of the position's role in implementing, maintaining, and monitoring the Information Security Program.

d. SABRE shall ensure that the role of the CISO includes regular reporting to the Chief Executive Officer and Board of Directors concerning SABRE's security posture, the security risks faced by SABRE, and the security implications of SABRE's business decisions.

e. SABRE shall ensure that employees who are responsible for implementing, maintaining, or monitoring the Information Security Program, including but not limited to the CISO, have sufficient knowledge of the requirements of this Assurance and receive training appropriate for their role in safeguarding and protecting Consumers' Personal Information, to enable and ensure their ability to comply with the terms of this Assurance and to enable the terms of this Assurance. SABRE shall provide the training required under this paragraph to such employees within ninety (90) days of the Effective Date of this Assurance or prior to their starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

23. SABRE may satisfy the implementation of the Information Security Program through review, maintenance, and if necessary, updating of an existing Information Security Program or existing safeguards, provided that such existing program and safeguards meet the requirements set forth in this Assurance.

24. SABRE shall review not less than annually the Information Security Program, which shall include a review of the configuration of SABRE's Security Incident and Event Management ("SIEM") solution.

25. SABRE shall ensure that its Information Security Program receives the resources and support reasonably necessary to ensure that it functions as intended.

Incident Response and Data Breach Notification Plan

26. As part of its Information Security Program, SABRE shall develop, implement, and maintain a written Incident Response and Data Breach Notification Plan ("Plan") to prepare for and respond to Security Events.

27. The Plan shall, at a minimum:

a. Address the following phases: (i) Preparation; (ii) Detection and Analysis; (iii) Containment; (iv) Notification and Coordination with Law Enforcement; (v) Eradication; (vi) Recovery; (vii) Consumer and Regulator Notification and Remediation; and (viii) Post-Incident Analysis.

b. Identify the types of incidents that fall within the scope of the Plan, which must include any incident that SABRE reasonably believes might be a Security Event;

c. Clearly describe key individuals' roles in fulfilling responsibilities under the Plan, including back-up contacts and escalation pathways; and

d. Require bi-annual testing and review of the Plan, and the evaluation and revision of the Plan in light of such testing and review.

Specific Information Security Requirements

28. SABRE shall implement and maintain a system to secure use of privileged credentials to SynXis, such as through a privileged access management tool that vaults credentials and requires multi-factor authentication for access.

29. SHS shall require the use of multi-factor authentication for user remote access to SynXis. If multi-factor authentication for remote access to SynXis is disabled on a temporary basis for technical or other reasons, SHS will document: (i) the technical reason; (ii) the compensating security controls, and (iii) the duration for which authentication was disabled.

30. SABRE shall implement and maintain reasonable password policies and procedures in accordance with industry-accepted standards or frameworks.[3] For PCI DSS covered systems, SABRE shall follow the requirements as specified in the latest version of PCI DSS.

31. SHS shall adopt reasonable account management policies and ensure that widely deployed local administrative accounts are unique to each application within SynXis, not generic, and shall implement regular password rotation. SHS shall restrict the ability for service accounts to logon locally and be used interactively within SynXis.

32. SHS shall implement and maintain appropriate policies and procedures to manage and audit SHS-owned accounts. For SHS-owned accounts, SHS shall define access needs and restrict access to cardholder data by business need-to-know. SHS shall perform regular audits of all active and disabled SHS-owned accounts and permissions to identify which are active and how they are used. SHS shall remove system access promptly for terminated employees and lower access level quarterly where an employee's job function no longer requires a higher level.

---

[3] For example, the National Institute of Standards and Technology Cybersecurity Framework.

33. SHS shall employ enhanced behavior analytics tools, such as a SIEM solution, to log and monitor all potential Security Events in SynXis.

a. SHS shall ensure such tools are configured, updated, and maintained to ensure that system activity is adequately logged, and that Security Events are reviewed.

b. SHS shall ensure that logs are regularly and actively reviewed in near real-time—through either automated or manual means that detect anomalous behavior—and that appropriate follow-up is taken with respect to Security Events.

c. SHS shall create a formalized process to review Security Events and anomalous privileged user activity on a regular and systemic basis.

d. SHS shall maintain logs and retain audit trails as required by the PCI DSS.

34. SABRE shall maintain tools to scan SHS's code and applications for vulnerabilities in the code or production environment.

35. SHS shall implement and maintain current, up-to-date antivirus protection programs on computer systems.

36. SHS shall maintain a penetration testing program in accordance with industry standard practices, which shall include reasonable remediation of vulnerabilities revealed by such testing. The program shall include at least one annual penetration test of SynXis components containing Personal Information where the loss of such information would constitute a security breach pursuant to Security Breach Notification Acts and at least one weekly vulnerability scan of SynXis.

VI. SETTLEMENT COMPLIANCE ASSESSMENT

37. SHS shall obtain an information security assessment and report from a third-party professional ("Third-Party Assessor"), using procedures and standards generally accepted in the profession ("Third-Party Assessment"), within one (1) year after the Effective Date of this Assurance. The Third-Party Assessor's report on the Third-Party Assessment shall use reasonable methods to:

A. Identify security vulnerabilities in SynXis and provide recommendations as to how to improve the security of SynXis;

B. Set forth the specific administrative, technical, and physical safeguards implemented by SHS;

C. Explain the extent to which such safeguards are appropriate in light of SHS's size and complexity, the nature and scope of SHS's activities, and the sensitivity of the Personal Information maintained by SHS;

D. Explain the extent to which the safeguards that have been implemented meet the requirements of the Information Security Program; and

E. Identify SHS's Qualified Security Assessor for purposes of PCI DSS compliance.

38. SHS's Third-Party Assessor shall be: (a) a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization; and (b) have at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

39. SHS shall take reasonable steps to implement recommendations and remedy vulnerabilities identified by the Third-Party Assessor. In the event SHS does not address a

recommendation or vulnerability, it will document its decision and the justification for the decided course of action.

VII. SUBMISSION TO ATTORNEYS GENERAL

40. SABRE shall provide a copy of the Third-Party Assessor's report on the Third-Party Assessment to the Vermont Attorney General within one hundred and eighty (180) days of the completion of the report.

41. Any Third-Party Assessor report provided pursuant to this Assurance and all information contained therein, to the extent permitted by the laws of the State of Vermont shall be treated by the Vermont Attorney General's Office as confidential; shall not be shared or disclosed except to other multistate Attorneys General as described in Paragraph 42 (below); and shall be treated by the Vermont Attorney General's Office as a trade secret subject to 1 V.S.A. § 317(c)(9). In the event that the Vermont Attorney General's Office receives any request from the public to inspect any Third-Party Assessor's report provided pursuant to this Assurance or other documents under this Assurance and believes such information is subject to disclosure under the relevant public records laws, the Vermont Attorney General's Office agrees to provide SABRE with at least five (5) business days advance notice before producing the information, to the extent permitted by state law (and with any required lesser advance notice), so that SABRE may take appropriate action to defend against the disclosure of such information. The notice under this paragraph shall be provided consistent with Paragraph 63.

42. The Vermont Attorney General shall make the Third-Party Assessor report available to other multistate Attorneys General upon request provided the Attorney General receiving the information confirms in writing, to the extent permitted by the relevant state law, to the prohibitions against non-disclosure in Paragraph 41, including that the receiving State has

laws preventing the disclosure of trade secrets, proprietary commercial information, competitively sensitive information, information revealing sensitive security information, and related material.

VIII. PAYMENT TO THE STATES

43. SABRE shall pay $2,400,000 to the Attorneys General. Said payment shall be divided and paid by SABRE directly to each of the Attorneys General in an amount designated by the Attorneys General and communicated to SABRE by the Vermont Attorney General, as the lead state of the multistate investigation. Each of the Attorneys General agrees that the Vermont Attorney General has the authority to designate such amount to be paid by SABRE to each Attorney General and to provide SABRE with instructions for the payments to be distributed under this paragraph. Payment shall be made no later than thirty (30) days after the Effective Date of this Assurance and receipt of such payment instructions by SABRE from the Vermont Attorney General, except that where state law requires judicial or other approval of the Assurance, payment shall be made no later than thirty (30) days after notice from the relevant Attorney General that such final approval for the Assurance has been secured.

44. Said payment shall be used by the Attorneys General for such purposes that may include, but are not limited to, being placed in, or applied to, the consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving fund, defraying costs of the inquiry leading hereto, or for attorneys' fees and other costs of investigation, or for other uses permitted by state law, at the sole discretion of the Attorneys General.

IX. RELEASE

45. Following full payment of the amounts due under this Assurance, the Attorneys General shall release and discharge SABRE and its officers, employees, and directors from all civil or administrative claims that the Attorneys General could have brought under the Consumer Protection Acts, the Personal Information Protection Acts, and the Security Breach Notification Acts based on SABRE's conduct related to the Breach. Nothing contained in this paragraph shall be construed to limit the ability of the Attorneys General to enforce the obligations that SABRE has under this Assurance. Further, nothing in this Assurance shall be construed to create, waive, or limit any private right of action.

46. This Assurance is not intended, and shall not be deemed, to constitute evidence or precedent of any kind except in: (a) any action or proceeding by one of the Parties to enforce, rescind, or otherwise implement or affirm any or all terms of this Assurance; or (b) any action or proceeding involving a claim covered by the release to support a defense of res judicata, collateral estoppel, release or other theory of claim preclusion, issue preclusion, or similar defense.

X. PRESERVATION OF AUTHORITY

47. Nothing in this Assurance shall be construed to limit the authority or ability of an Attorney General to protect the interests of his/her State or the people of his/her State. This Assurance shall not bar the Attorney General or any other governmental entity from enforcing laws, regulations, or rules against SABRE for conduct subsequent to or otherwise not covered by this Assurance. Further, nothing in this Assurance shall be construed to limit the ability of the Attorney General to enforce the obligations that SABRE has under this Assurance.

XI. GENERAL PROVISIONS

48. The Parties understand and agree that this Assurance shall not be construed as an approval or a sanction by the Attorneys General of SABRE's business practices, nor shall SABRE represent that this Assurance constitutes an approval or sanction of its business practices. The Parties further understand and agree that any failure by the Attorneys General to take any action in response to any information submitted pursuant to this Assurance shall not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date.

49. SABRE neither admits nor denies any violation of law in connection with the Breach.

50. Nothing in this Assurance shall be construed as relieving SABRE of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Assurance be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

51. SABRE shall deliver a copy of this Assurance to, or otherwise fully apprise, each of its current officers of the rank of executive vice president or above, the executive management officer having decision-making authority with respect to the subject matter of this Assurance, and each member of its Board of Directors. SABRE shall deliver a copy of this Assurance to, or otherwise fully apprise, any new officers of the rank of executive vice president or above, new executive management officer having decision-making authority with respect to the subject matter of this Assurance, and each new member of its Board of Directors, within ninety (90) days from which such person assumes his/her position with SABRE.

52. To the extent that there are any, SABRE agrees to pay all court costs associated with the filing (if legally required) of this Assurance. No court costs, if any, shall be paid by any Attorney General.

53. SABRE shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Assurance or for any other purpose that would otherwise circumvent any term of this Assurance. SABRE shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Assurance.

54. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart thereof and all of which together shall constitute one and the same document. One or more counterparts of this Assurance may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

55. SABRE agrees that this Assurance does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and SABRE further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

56. This Assurance shall not be construed to waive any claims of sovereign immunity the States may have in any action or proceeding.

57. This Assurance shall not be construed or used as a waiver or any limitation of any defenses, including jurisdictional defenses, otherwise available to SABRE in any pending or future actions of any nature, including but not limited to actions of a private, administrative, criminal, individual, class, or any other nature and including claims or suits relating to the existence, subject matter, or terms of this Assurance.

58. This Assurance may be enforced only by the Parties hereto. Nothing in this Assurance shall provide any rights to or permit any person or entity not a party hereto, including any state or attorney general not a party hereto, to enforce any provision of this Assurance. No person or entity not a signatory hereto is a third-party beneficiary of this Assurance. Nothing in this Assurance shall be construed to create, affect, limit, alter, or assist any private right of action, including without limitation any private right of action that a consumer or other third-party may hold against SABRE.

XII. SEVERABILITY

59. If any clause, provision, or section of this Assurance shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Assurance, and this Assurance shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

XIII. TIMELINE FOR IMPLEMENTATION

60. The Parties agree that, except as otherwise provided, SABRE shall implement the requirements set forth in Sections V-VII within ninety (90) days of the Effective Date. Specific exceptions include,

a. SABRE shall implement a system to secure use of privileged credentials to SynXis, as described in Paragraph 28, within one hundred and eighty (180) days of the Effective Date.

b. The payment deadline in Paragraph 43; and

c. The deadline for submission of the report described in Paragraph 37 shall be one hundred and eighty (180) days after the completion of the report.

61. The Parties agree that the requirements set forth in Paragraphs 17(b), 21 and 28-36 shall sunset five (5) years after the Effective Date.

XIV. REQUIREMENT TO MEET AND CONFER

62. The Parties agree that the steps required to implement the requirements of this Assurance involve a high degree of technical complexity and the coordination of multiple systems and business teams within SABRE. If the Attorney General reasonably believes SABRE has failed to comply with any of this Assurance, and if the failure to comply does not threaten the health or safety of the citizens of the State of Ohio and/or does not create an emergency requiring immediate action, the Attorney General will notify SABRE in writing of such failure to comply, and SABRE shall have thirty (30) days from receipt of such written notice to provide a good faith written response, including either a statement that SABRE believes it is in full compliance, or otherwise a statement explaining how the violation occurred, how it has been addressed or when it will be addressed, and what SABRE will do to make sure the violation does not happen again. The Attorney General may agree to provide SABRE more than thirty (30) days to respond.

XV. NOTICE / DELIVERY OF DOCUMENTS

63. Whenever SABRE shall provide notice to the Attorneys General under this Assurance, that requirement shall be satisfied by sending notice to the Designated Contacts on behalf of the Attorneys General listed in Appendix C. Any notices or other documents sent to SABRE pursuant to this Assurance shall be sent to the following physical and email addresses:

Sabre Corporation
ATTN: General Counsel
3150 Sabre Dr.
Southlake, TX 76092.

With a copy to:

Benjamin A. Powell
Sonal Mehta
Wilmer Cutler Pickering Hale and Dorr
1875 Pennsylvania Ave.
Washington, DC 20006
Benjamin.Powell@wilmerhale.com
Sonal.Mehta@wilmerhale.com

All notices or other documents to be provided under this Assurance shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall have been deemed to be sent upon mailing. Any party may update its address by sending written notice to the other party.

ASSURANCE OF VOLUNTARY COMPLIANCE
IN RE SABRE SECURITY BREACH

On behalf of State of Ohio

Signature: Melissa S Smith Date: 12.22.2020

Melissa S. Smith (0083551)
Assistant Section Chief
Ohio Attorney General's Office
30 E. Broad Street, Floor 14
Columbus, OH 43215
Melissa.s.smith@ohioattorneygeneral.gov
614.466.6112

Signature: Michael Ziegler per MSS MSS Date: 12.22.2020

Michael Ziegler (0042206)
Principal Assistant Attorney General
Ohio Attorney General's Office
30 E. Broad Street, Floor 14
Columbus, OH 43215
Michael.Ziegler@ohioattorneygeneral.gov
614.466.3980

SABRE Corporation

By: _____

Aimee Williams-Ramey
General Counsel, SABRE Corporation

Date: December 8, 2020

Counsel for SABRE Corporation

By: _____

Benjamin A. Powell
Wilmer Cutler Pickering Hale and Dorr
1875 Pennsylvania Ave.
Washington, DC 20006

Date: Dec. 7, 2020

Appendix A

STATE	CONSUMER PROTECTION ACTS
Alaska	Unfair Trade Practices Act, AS 45.50.471 *et seq.*
Arizona	Arizona Consumer Fraud Act, A.R.S. §§ 44-1521 *et seq.*
Arkansas	Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-101 *et seq.*
Connecticut	Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110b *et seq.*
Florida	Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes
Hawaii	Uniform Deceptive Trade Practice Act, Haw. Rev. Stat. Chpt. 481A and Haw. Rev. Stat. Sect. 480-2
Illinois	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*
Indiana	Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-1 *et seq.*
Iowa	Iowa Consumer Fraud Act, Iowa Code § 714.16
Louisiana	Unfair Trade Practices and Consumer Protection Law, La. R.S. §§ 51:1401 *et seq.*
Michigan	Michigan Consumer Protection Act, MCL §§ 445.901 *et seq.*
Minnesota	The Uniform Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43–.48; Consumer Fraud Act, Minn. Stat. §§ 325F.68-.694
Missouri	Missouri Merchandising Practices Act, Mo. Rev. Stat. §§ 407.010 *et seq.*
Montana	Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. §§ 30-14-101 *et seq.*
Nebraska	Nebraska Consumer Protection Act, Neb. Rev. Stat. §§ 59-1601 *et seq.*; Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 *et seq.*
Nevada	Nevada Deceptive Trade Practices Act; Nev. Rev. Stat. §§ 598.0903 *et seq.*
New Jersey	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 *et seq.*
New York	Executive Law 63(12), General Business Law 349/350
North Carolina	North Carolina Unfair and Deceptive Trade Practices Act, N.C.G.S. §§ 75-1.1 *et seq.*
North Dakota	Unlawful Sales or Advertising Practices, N.D.C.C. §§ 51-15-01 *et seq.*
Ohio	Ohio Consumer Sales Practices Act, R.C. §§ 1345.01 *et seq.*
Oregon	Oregon Unlawful Trade Practices Act, ORS 646.605 *et seq.*
Pennsylvania	Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1 *et seq.*
Tennessee	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 to -132
Vermont	Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 *et seq.*
Virginia	Virginia Consumer Protection Act, Virginia Code §§ 59.1-196 through 59.1-207
Washington	Washington Consumer Protection Act, RCW 19.86.020

Appendix B

STATE	PERSONAL INFORMATION PROTECTION ACTS & SECURITY BREACH NOTIFICATION ACTS
Alaska	Personal Information Protection Act, AS §§ 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 18-552
Arkansas	Personal Information Protection Act, Ark. Code Ann. §§ 4-110-101 *et seq.*
Connecticut	Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471; Breach of Security, Conn. Gen. Stat. § 36a-701b
Florida	Florida Information Protection Act, Section 501.171, Florida Statutes
Hawaii	Security Breach of Personal Information, Haw. Rev. Stat. Chpt. 487N
Illinois	Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.*
Indiana	Disclosure of Security Breach Act, Indiana Code §§ 24-4.9-1-1 *et seq.*
Iowa	Personal Information Security Breach Protection Act, Iowa Code § 715C
Louisiana	Database Security Breach Notification Law, La. R.S. §§ 51:3071 *et seq.*
Michigan	Identity Theft Protection Act, MCL §§ 445.61 *et seq.* (Breach notification only; no applicable State personal information protection Act)
Minnesota	Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Montana Impediment of Identity Theft Act, Mont. Code Ann. §§ 30-14-1701 *et seq.*
Nebraska	Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 *et seq.*
Nevada	Nevada Security and Privacy of Personal Information Act; Nev. Rev. Stat. §§ 603A.010 – 603A.290
New Jersey	New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166
New York	General Business Law 899-aa and 899-bb
North Carolina	North Carolina Identity Theft Protection Act, N.C.G.S. §§ 75-60 *et seq.*
North Dakota	Notice of Security Breach for Personal Information N.D.C.C. §§ 51-30-01 *et seq.*
Ohio	Security Breach Notification Act, R.C. §§ 1349.19 *et seq.*
Oregon	Oregon Consumer Information Protection Act, ORS 646A.600 *et seq.*
Pennsylvania	Breach of Personal Information Notification Act, 73 P.S. §§ 2301 *et seq.*
Tennessee	Tennessee Identity Theft Deterrence Act of 1999, Tenn. Code. Ann. §§ 47-18-2101 to -2111
Vermont	Vermont Security Breach Notice Act, 9 V.S.A. § 2435
Virginia	Virginia Breach of Personal Information Notification Law, § 18.2-186.6
Washington	Washington Data Breach Notification Law, RCW 19.255.010

Appendix C

STATE	DESIGNATED CONTACT
Alaska	John Haley Assistant Attorney General 1031 West 4th Ave, Suite 200 Anchorage, AK 99501 John.haley@alaska.gov 907-269-5200
Arizona	Mark James Ciafullo Assistant Attorney General 2005 N. Central Ave. Phoenix, Arizona 85004 Mark.Ciafullo2@azag.gov 602-542-7716
Arkansas	Peggy Johnson Assistant Attorney General 323 Center Street, Suite 200 Little Rock, Arkansas 72201 peggy.johnson@arkansasasag.gov 501-682-8062
Connecticut	Michele Lucan Assistant Attorney General Privacy & Data Security Department, Office of the Attorney General 165 Capitol Avenue, Suite 900 Hartford, Connecticut 06106 Michele.lucan@ct.gov 860-808-5440
Florida	Gregory Sadowski Senior Assistant Attorney General 110 SE 6th Street Ft. Lauderdale, FL 33301 Gregory.sadowski@myfloridalegal.com 954-712-4690
Hawaii	Lisa P. Tong Enforcement Attorney 235 S. Beretania Street #801 Honolulu, HI 96813 ltong@dcca.hawaii.gov (808) 586-2636
Illinois	Matthew W. Van Hise Chief, Privacy Unit 500 South Second Street Springfield, IL 62701 mvanhise@atg.state.il.us 217-782-4436

Appendix C

Indiana	Douglas S. Swetnam Section Chief Data Privacy & Identity Theft Unit 302 W. Washington Street, IGCS-5th Floor Indianapolis, IN 46204 Douglas.Swetnam@atg.in.gov 317-232-6294
Iowa	William R. Pearson Assistant Attorney General 1305 E. Walnut, 2nd Fl. Des Moines, IA 50319 William.pearson@ag.iowa.gov (515) 242-6773
Louisiana	Alberto A. De Puy Assistant Attorney General 1885 N. 3rd Street 4th floor Baton Rouge, LA 70802 depuya@ag.louisiana.gov 225-326-6471
Michigan	Joseph E. Potchen Assistant Attorney General Corporate Oversight Division P.O. Box 30736 Lansing, MI 48909 potchenj@michigan.gov 517-335-7632
Minnesota	Caitlin Micko Assistant Attorney General 445 Minnesota Street, Suite 1200 St. Paul, MN 55101 Caitlin.micko@ag.state.mn.us 651-724-9180
Missouri	Kimberley Biagioli Assistant Attorney General 615 E. 13th Street, Suite 401 Kansas City, MO 64106 Kimberley.Biagioli@ago.mo.gov 816-889-3090
Montana	Caitlin Buzzas Assistant Attorney General Montana Office of Consumer Protection P.O. Box 200151 Helena, MT 59620-0151 caitlinbuzzas@mt.gov 406-444-2026

Appendix C

Nebraska	Michaela Lutz Assistant Attorney General 2115 State Capitol Building Lincoln, NE 68509 michaela.lutz@nebraska.gov 402-471-1928
Nevada	Lucas J. Tucker Senior Deputy Attorney General 8945 West Russell Rd., Suite #204 Las Vegas, Nevada 89148 ltucker@ag.nv.gov 702-486-3256
New Jersey	Kashif Chand Chief, Deputy Attorney General Data Privacy & Cybersecurity Section 124 Halsey Street, P.O. Box 54029 Newark NJ 07101 Kashif.Chand@law.njoag.gov (973) 648-2748
New York	Clark P. Russell Deputy Bureau Chief Bureau of Internet and Technology New York State Office of the Attorney General 28 Liberty Street, New York, NY 10005 clark.russell@ag.ny.gov 212-416-6494
North Carolina	Kim D'Arruda Special Deputy Attorney General NC Dept of Justice, Consumer Protection Div, 114 W Edenton Steet, Raleigh, NC 27603 kdarruda@ncdoj.gov 919-716-6013
North Dakota	Brian M. Card Assistant Attorney General 1050 E. Interstate Ave., Ste. 200 Bismarck, ND 58503 bmcard@nd.gov (701) 328-5570
Ohio	Melissa Smith Assistant Section Chief 30 E. Broad St., Floor 14 Columbus, OH 43215 Melissa.s.smith@ohioattorneygeneral.gov 614.466.6112

Appendix C

Oregon	Kristen G. Hilton Senior Assistant Attorney General Oregon Department of Justice, Consumer Protection Section 1162 Court Street NE Salem, OR 97301 Kristen.hilton@doj.state.or.us 503-934-4400
Pennsylvania	John M. Abel Assistant Director for Multistate and Special Litigation 15th Floor, Strawberry Square Harrisburg, PA 17120 jabel@attorneygeneral.gov 717-783-1439
Tennessee	Ann Mikkelsen Asst. Attorney General Office of the Tennessee Attorney General, Consumer Protection Division, P.O. Box 20207 Nashville, TN 37202-0207 Ann.mikkelsen@ag.tn.gov (615) 253-3819
Vermont	Ryan Kriger Public Protection Division, Vermont Office of the Attorney General 109 State Street Montpelier, VT 05609 802-828-3170 ryan.kriger@vermont.gov
Virginia	Gene Fishel Senior Assistant Attorney General 202 North 9th Street Richmond, VA 23219 sfishel@oag.state.va.us 804-786-3870
Washington	Andrea Alegrett Assistant Attorney General 800 Fifth Avenue, Suite 2000 Seattle, WA 98104 Andrea.alegrett@atg.wa.gov 206-389-3813