

**IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY
FIRST JUDICIAL DISTRICT OF PENNSYLVANIA
CIVIL TRIAL DIVISION**

COMMONWEALTH OF PENNSYLVANIA	:
By Attorney General Josh Shapiro	:
	:
Petitioner	:
	:
v.	:
	:
ORBITZ WORLDWIDE LLC	:
	:
and	:
	:
EXPEDIA, INC.	:
	:
Respondents	:

ASSURANCE OF VOLUNTARY COMPLIANCE

The Commonwealth of Pennsylvania by Attorney General Josh Shapiro, through the Bureau of Consumer Protection (“Commonwealth” or “Petitioner”) and Orbitz Worldwide LLC and Expedia, Inc. enter into the following Assurance of Voluntary Compliance (“Assurance”) pursuant to the Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, et seq.; 201-5 (“Consumer Protection Law”):

1. PREAMBLE

1.1. The Commonwealth conducted an investigation under the Consumer Protection Law regarding the data breach announced by Orbitz on March 21, 2018, which affected 20,755 Pennsylvania consumers.

1.2. On September 17, 2015, Expedia, Inc. acquired Orbitz Worldwide LLC including its brands and assets. Following the acquisition, Expedia, Inc. operated the website www.orbitz.com and began migrating Orbitz services to Expedia’s platforms and completed the migration by October

1, 2018 and now is fully governed by Expedia's information security and privacy policies. At the time of the data breach, Orbitz only utilized the Orbitz Legacy Platform for accessing certain historical consumer transactions and hosting specific travel rewards websites for a limited number of business customers. Previously, the Orbitz Legacy Platform hosted travel booking services for consumers until June 22, 2016.

1.3. On November 23, 2017, an Orbitz business partner whose travel rewards redemption portal was hosted by the Orbitz Legacy Platform notified Orbitz that the portal may have been a common point of purchase in connection with certain fraudulent payment card transactions. As part of its investigation, Orbitz determined in January 2018 that a threat actor circumvented security detection technology and created custom malware to target payment card information submitted on the business partner's travel rewards redemption portal. Orbitz notified its business partner and continued its investigation, subsequently determining that the threat actor likely accessed additional payment card information through the Orbitz Legacy Platform.

1.4. The Commonwealth's investigation found that Orbitz engaged in deceptive or unfair business practices by making material misrepresentations in its customer-facing privacy policy concerning the safeguarding of its customers' personal information within the Orbitz Legacy Platform.

1.5. By way of further background, Orbitz has disseminated, or caused to be disseminated, privacy policies or statements on its websites hosted on the Orbitz Legacy Platform to users and potential users of these websites. These policies or statements include, but are not limited to, the following statement on its www.orbitz.com website:

We want you to feel confident about using this website to make travel arrangements, and we are committed to protecting the information we collect. While no website can guarantee security, we have implemented appropriate administrative, technical, and physical security procedures to help protect the personal information you provide to us. For example, only authorized employees are permitted

to access personal information, and they may only do so for permitted business functions. In addition, we use encryption when transmitting your sensitive personal information between your system and ours, and we employ firewalls and intrusion detection systems to help prevent unauthorized persons from gaining access to your information.

According to the Payment Card Industry Forensic Investigator who performed a forensic analysis on Orbitz's web application and database server environments comprising various Travel Rewards Program platforms following the breach, certain Payment Card Industry Data Security Standard requirements or sub-requirements were not in place at the time of the breach.

1.6. Moreover, Orbitz was not in full compliance with Expedia's company policies related to penetration testing and patch management with respect to the Orbitz Legacy Platform, which may have caused or contributed to the breach. It was not until after an investigation into the breach that Expedia identified and took immediate action to address these issues.

1.7. The Commonwealth alleges the aforesaid conduct constitutes unfair methods of competition and/or unfair or deceptive acts or practices in the conduct of trade or commerce in violation of the Consumer Protection Law, including without limitation, the following:

- (i) Causing likelihood of confusion or of misunderstanding as to the source, sponsorship, approval, or certification of goods or services, as prohibited by Section 201-2(4)(ii) of the Consumer Protection Law 73 P.S. § 201-2(4)(ii);
- (ii) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has sponsorship, approval status, affiliation or connection that he does not have as prohibited by Section 201-2(4)(v) of the Consumer Protection Law, 73 P.S. § 201-2(4)(v);
- (iii) Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another as prohibited by Section 201-2(4)(vii) of the Consumer Protection Law, 73 P.S. § 201-2(4)(vii); and
- (iv) Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding in violation of 73 P.S. § 201-2(4)(xxi).

1.8. Under Section 201-5 of the Consumer Protection Law, this Assurance shall not be considered an admission of a violation for any purpose. This Assurance is for settlement purposes only, and neither the fact of, nor any provision contained in, this Assurance nor any action taken hereunder shall constitute, be construed as, or be admissible in evidence as any admission or finding of wrongdoing by Orbitz or Expedia, or any admission of the validity of any claim or any fact alleged in any other pending or subsequently filed action or of any wrongdoing, fault, violation of law, or liability of any kind on the part of Orbitz or Expedia or admission by Orbitz, or Expedia of the validity or lack thereof of any claim, allegation, or defense asserted in any other action. Orbitz and Expedia believe that its conduct has been lawful and has not violated any consumer protection statutes or other laws of the States. Furthermore, Orbitz and Expedia believe that if any violation occurred, such a violation was unintentional and unwitting.

2. PARTIES

2.1. Petitioner is the Commonwealth of Pennsylvania, acting by Attorney General Josh Shapiro, through the Bureau of Consumer Protection. The Attorney General is charged with among other things, enforcement of the Consumer Protection Law.

2.2. Respondent Orbitz Worldwide LLC ("Orbitz" and/or collectively one of the "Respondents" and, together with Expedia, Inc. and the Commonwealth, the "Parties") is a Delaware corporation with its principal place of business in Chicago, Illinois. Orbitz, a wholly owned subsidiary of Expedia, Inc., is a global online travel company that enables travelers to research, plan, and book travel products and services.

2.3. Respondent Expedia, Inc. ("Expedia" and/or collectively one of the "Respondents" and, together with Orbitz and the Commonwealth, the "Parties") is a Washington corporation with its principal place of business in Bellevue, Washington. Expedia owns and operates websites offering

multiple travel services. In September 2015, Expedia acquired Orbitz, including the Orbitz Legacy Platform that was impacted by the breach.

3. DEFINITIONS

3.1. "Cardholder Data Environment" ("CDE") shall mean Orbitz's personnel, processes, and technologies that store, process, or transmit Payment Card Information of Consumers within Expedia platforms or the Orbitz Legacy Platform. The CDE definition also includes system components or devices that are located within or connected to CDE; or provide security services, facilitate segmentation, or may impact the security of the CDE. This definition is intended to be consistent with the PCI DSS.

3.2. "Compensating Controls" shall mean alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the Chief Information Security Officer or his or her designee to be impractical to implement at the present time due to legitimate technical or business constraints. Such alternative mechanisms must: (1) meet the intent and rigor of the original stated requirement; (2) provide a similar level of security as the original stated requirement; (3) be up-to-date with current industry accepted security protocols; and (4) be commensurate with the additional risk imposed by not adhering to the original stated requirement. The determination to implement such alternative mechanisms must be accompanied by written documentation demonstrating that a risk analysis was performed indicating the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable, and that the Chief Information Security Officer or his or her designee agrees with both the risk analysis and the determination that the risk is acceptable. This definition is intended to be consistent with the PCI DSS.

3.3. "Consumer" shall mean any individual resident in the Commonwealth of Pennsylvania who initiates a purchase of or purchases goods or services directly from Orbitz.com.

- 3.4. "Effective Date" shall be the date this Assurance is filed.
- 3.5. "Orbitz Legacy Platform" shall mean the computing infrastructure operated by Orbitz that experienced the data breach announced by Orbitz on March 21, 2018.
- 3.6. "Payment Card Information" ("PCI") shall mean Cardholder Data ("CHD") and Sensitive Authentication Data ("SAD") as defined by the PCI DSS.
- 3.7. "PCI DSS" shall mean the latest version of the Payment Card Industry Data Security Standard published by Payment Card Industry Security Standards Council.
- 3.8. "Personal Information" shall mean information contained within the CDE of Consumers that is (1) "personal information" as defined under the Breach of Personal Information Notification Act, 73 P.S. § 2302 (enacted December 22, 2005), and (2) Payment Card Information ("PCI").

4. APPLICATION

- 4.1. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to Orbitz, its affiliates, subsidiaries, successors and assigns, and its officers and employees.
- 4.2. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to Expedia, its successors and assigns, and its officers and employees, but only to the extent that a specific section in this Assurance expressly applies a requirement to Expedia.
- 4.3. Respondents agree to cease and desist from engaging in the acts and practices alleged above and shall not violate the Consumer Protection Law.

5. REQUIREMENTS

- 5.1. Unless otherwise specified herein, the requirements set forth in this Assurance shall apply to Orbitz for a period of five (5) years from the Effective Date.

6. INFORMATION SECURITY PROGRAM

6.1. Orbitz shall further develop, implement, and maintain a comprehensive information security program to govern the CDE ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information Orbitz collects or obtains, and that shall, at a minimum include the requirements set forth in this Assurance to the extent appropriate based on Orbitz's assessment of relevant risks. A determination regarding the extent to which any such requirements defined in Sections 6 and 7 of this Assurance are not appropriate must be based on a reasonable assessment of relevant risks and documented by Orbitz.

6.2. Such Information Security Program shall be developed and implemented within one hundred eighty (180) days after the Effective Date of this Assurance. For any requirements not fully developed and implemented within one hundred eighty (180) days after the Effective Date of this Assurance, Orbitz shall implement interim Compensating Controls to address the identified risks.

6.3. The Orbitz Information Security Program shall be written and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Orbitz's operations; (ii) the nature and scope of Orbitz's activities; and (iii) the sensitivity of the Personal Information that Orbitz maintains.

6.4. Expedia shall employ an executive or officer to serve as Orbitz's Chief Information Security Officer ("CISO") with appropriate credentials, background and expertise in information security who shall be responsible for overseeing Orbitz's implementation and maintenance of the Information Security Program. The duties and responsibilities of the CISO shall be documented and include advising the Chief Executive Officer and the Board of Directors of Orbitz's security posture, security risks faced by Orbitz and the security implications of Orbitz's decisions.

6.5. Expedia shall ensure that Orbitz's CISO and Information Security Program receive the resources and support reasonably necessary to ensure that the Information Security Program is fully implemented and functions as required by this Assurance.

6.6. Orbitz's Information Security Program must include security awareness training designed to communicate Orbitz's commitment to full compliance with the Information Security Program and to ensure that all personnel with key responsibilities for implementation and oversight of the Information Security Program, including the CISO, have sufficient knowledge of the requirements of this Assurance and the specific knowledge, skills, and abilities to perform their functions in compliance with the Information Security Program. Orbitz's training shall ensure that system, database, network administrators, and persons with privileged access to the CDE are fully informed of the requirements of the Information Security Program relevant to their functions, which may include password policies, secure data handling, secure storage, transmission and disposal of Personal Information, and best practices to prevent attackers from obtaining credentials and other sensitive data through malicious downloads and other threats identified by Orbitz. Orbitz shall also develop accountability metrics to measure each participant's compliance with training requirements. Within 180 days of the Effective Date, Orbitz shall provide training required by this Assurance, and thereafter shall provide it to relevant personnel on at least an annual basis.

7. INFORMATION SECURITY SAFEGUARDS

7.1. As part of the Information Security Program, Orbitz shall include risk management, which at a minimum includes:

- a. Documented criteria for reasonable safeguards that appropriately protect Consumers while not being more burdensome to Orbitz than the risks they address. These criteria shall include:

-
- i. Obligations owed to Consumers for protecting their Personal Information,
 - ii. The social utility of Orbitz's handling of Consumers' Personal Information,
 - iii. The foreseeability and magnitude of harm caused by security threats,
 - iv. The burden to Orbitz's utility and objectives posed by safeguards,
 - v. The overall public interest in the proposed solution.
- b. A plan and program for designing, implementing, and operating safeguards that:
- i. Reduce identified risks to a reasonable and appropriate level.
 - ii. Enhance the security requirements required by PCI DSS if necessary to reduce risks to a reasonable and appropriate level.
 - iii. Select controls from other industry-appropriate control standards (e.g. NIST Special Publication 800-53, ISO 27001, or CIS Controls if identified risks would not be reasonably protected by controls required by PCI DSS.
- c. An annual, comprehensive assessment of risks to Personal Information conducted by an outside third party for the next three years following the Effective Date. Comprehensive assessments of the CDE shall consider foreseeable threats to all assets or classes of assets that pose a risk to Personal Information. Foreseeable threats shall be identified using a comprehensive and current listings of known effective threats compiled by the security community or a professional body. Examples of such resources include MITRE ATT&CK model, the Veris Community Database, and the Symantec Internet Security Threat Report.

7.2. Orbitz shall comply with Payment Card Industry Data Security Standards with respect to its CDE and any Orbitz Legacy Platform system component the compromise of which Orbitz should reasonably believe would impact the security of its PCI.

7.3. Segmentation — Orbitz shall implement and maintain policies, procedures, and reasonable safeguards designed to segment its CDE and ensure that systems communicate within its CDE only to the extent necessary to perform their business and/or operational functions. At a minimum:

a. Orbitz shall take reasonable, risk-based steps to scan and map the connections between its CDE and the rest of the Orbitz Legacy Platform in order to determine avenues of traffic to Personal Information and to identify and assess potential penetration vulnerabilities to Personal Information.

b. Orbitz shall segment Personal Information from the rest of the Orbitz computer network using reasonable safeguards informed by their risk assessment that would prevent reasonably foreseeable unauthorized access to systems that store, process, or transmit Personal Information, such that compromise of an out-of-scope system could not be expected to impact the security of Personal Information.

c. Orbitz shall document the risk-appropriateness of the architecture and separation of networks using a risk assessment, and detailed policies and standards that document how such segmentation of its CDE is to be implemented, tested, and maintained; and

d. Orbitz shall use reasonable safeguards to maintain the separation of the development and production environments for its CDE.

7.4. Orbitz shall design, implement, and operate policies, procedures, and safeguards for its CDE that reduce risks to a reasonable and appropriate level and comply with PCI DSS. Orbitz

shall validate PCI DSS compliance as a Level 1 merchant/service provider for its CDE by engaging a PCI QSA to conduct an onsite assessment resulting in the delivery of a PCI Report on Compliance (ROC) and Attestation of Compliance (AOC). Orbitz will implement the following information security controls, or corresponding Compensating Controls, for its CDE and shall enhance the minimal security requirements required by PCI DSS for its CDE if necessary to reduce risks to a reasonable and appropriate level including, but not limited to, the following:

- a. Encryption — Orbitz shall employ encryption or some other risk-appropriate obfuscation of PCI at rest (stored) and PCI in transit (transmitted), and as Orbitz determines is reasonably necessary, any other Personal Information that is collected and stored by Orbitz.
- b. Logging and Monitoring — Orbitz shall implement and maintain logging and log monitoring policies and procedures designed to collect, manage, and analyze security logs and monitor its CDE to detect, understand, or recover from an attack.
- c. Access Control and Account Audits — Orbitz shall implement and maintain appropriate policies and procedures to manage and audit the use of corporate user accounts (*i.e.*, not consumer user accounts) that access the CDE, including individual accounts, privileged accounts, system and service accounts, and vendor accounts.
- d. Management of Administrative Privileges and Accounts — Orbitz shall implement and maintain policies and procedures to manage the use of administrative privileges and corporate user accounts that accesses the CDE to minimize opportunities for attackers to utilize such accounts.
- e. Password Management — Orbitz shall implement and maintain secure password policies and procedures for corporate user accounts.

f. Multi-Factor Authentication — Orbitz shall require multi-factor authentication for all corporate user accounts which can access unencrypted or unobfuscated PCI. In addition, all privileged access to the CDE that could impact the security of systems that store, process, or transmit PCI shall require multi-factor authentication, including remote access to the CDE.

g. File Integrity Monitoring — Orbitz shall implement and maintain controls, including but not limited to file integrity checking tools and monitoring solutions, designed to prevent and detect unauthorized modifications to critical applications or operating system files for systems within its CDE.

h. Antivirus and Malware Maintenance — Orbitz shall implement and maintain current, up-to-date antivirus and malware protection programs for its computer systems in its CDE.

i. Firewalls — Orbitz shall implement and maintain firewall policies and procedures to restrict connections between internal networks to systems that could impact the security of its CDE through appropriately configured hardware and software tools.

j. Inventory of Authorized and Unauthorized Software — Orbitz shall manage (*i.e.*, inventory and track) all software on systems within its CDE that could impact the security of PCI. Further, Orbitz shall implement and maintain controls, such as an application whitelisting solution, designed to detect and prevent the execution of unauthorized applications on systems within its CDE that store, process, or transmit PCI.

k. Software End of Life & Vulnerability Management — Orbitz shall make reasonable efforts to maintain and keep all software used within its CDE current, to the extent technically feasible and necessary, taking into consideration the impact an update will have on data security in the context of the CDE and its ongoing business and network

operations, and the scope of the resources required to address an end-of-life software issue. If software is no longer supported, Orbitz shall, to the extent technically feasible, update to the most current version and install all relevant patches and vendor security requirements. Orbitz shall also monitor and test in-house developed software for the CDE on a regular recurring basis to detect security weaknesses and take appropriate steps to ensure the security of applications which impact Orbitz's ability to safeguard PCI.

l. Penetration Testing — Orbitz shall implement and maintain a penetration testing program designed to identify, assess, and remediate potential security vulnerabilities within Orbitz's CDE. This program shall require periodic testing from outside Orbitz's CDE as well as from within its boundaries and include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including emails or documents containing passwords or other information critical to system operation. At a minimum, such testing shall occur on an annual basis and shall include appropriate remediation of vulnerabilities revealed by such testing, as well as documentation and retesting of such remediation.

m. Intrusion Detection and/or Intrusion Prevention Solution — Orbitz shall implement and maintain controls, such as intrusion detection and/or intrusion prevention systems, to detect and prevent unauthorized access to its CDE.

7.5. Integration with External Third-Party Business Partners — For each third-party business partner with which Orbitz shares, transmits, stores, or otherwise discloses PCI from its CDE that can impact the CDE, Orbitz shall conduct a risk assessment sufficient to determine whether the partner utilizes substantially similar and equally robust data security measures to protect PCI, as applicable. Based on the results of this risk assessment, Orbitz shall either take reasonable steps to

require such third parties to implement risk-appropriate data security measures or establish adequate Compensating Controls.

7.6. Data Loss Prevention — Orbitz shall implement and maintain reasonable safeguards within the CDE designed to detect and prevent risks posed by exfiltration of PCI, such as the use of data loss prevention technology.

8. SETTLEMENT COMPLIANCE ASSESSMENT

8.1. Orbitz shall obtain an information security compliance assessment and report for the CDE 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 shall:

- A. Set forth the specific administrative, technical, and physical safeguards maintained by Orbitz;
- B. Explain the extent to which such safeguards are appropriate in light of Orbitz’s size and complexity, the nature and scope of Orbitz’s activities, and the PCI maintained by Orbitz;
- C. Explain the extent to which the safeguards that have been implemented meet the requirements of the Information Security Program; and
- D. Identify Orbitz’s Qualified Security Assessor for purposes of PCI DSS validation.

8.2. Orbitz’s Third-Party Assessor shall (a) be 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.

8.3. Within ninety (90) days of completion of the Third-Party Assessor's report, Orbitz shall notify the Commonwealth of the completion of the report. If the Commonwealth seeks a copy of the Third Party Assessor's report, the Commonwealth shall issue an administrative subpoena, under Section 919 of the Administrative Code of 1929, 71 P.S. § 1, *et seq.*, § 307-3, to direct Orbitz to produce and deliver or cause to be delivered a copy of the report.

8.4. The identification of any deficiencies or recommendations for correction in the Third Party Assessor's report shall not constitute a violation of this Assurance unless Orbitz fails to take corrective action within a reasonable time.

9. MONETARY PAYMENT

9.1. Upon execution of this Assurance, Respondents shall pay \$110,000.00 (One Hundred Ten Thousand dollars and 00/100) to the Commonwealth which shall be allocated as follows:

9.2. A civil penalty in the amount of \$80,000.00 (Eighty Thousand dollars and 00/100).

9.3. The sum of \$30,000.00 (Thirty Thousand dollars and 00/100) to the Commonwealth in costs to be deposited in an interest bearing account to be used for future public protection and education purposes.

10. GENERAL PROVISIONS

10.1. The Parties understand and agree that this Assurance shall not be construed as an approval or a sanction by the Commonwealth of Respondents' business practices, nor shall Respondents represent that this Assurance constitutes an approval or sanction of its business practices. The Parties further understand and agree that any failure by the Commonwealth 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.

10.2. Nothing in this Assurance shall be construed as relieving Respondents 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 authorize or require Respondents to engage in any acts or practices prohibited by such laws, regulations, and rules.

10.3. Respondents 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 within ninety (90) days of the Effective Date. Respondents 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 Expedia.

10.4. Respondents 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. Respondents shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf to engage in practices prohibited by this Assurance.

10.5. 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.

10.6. This Assurance shall not be construed to limit any private course of action. This Assurance may be enforced only by the Parties hereto. 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 Respondents.

10.7. The Court of Common Pleas of Philadelphia County, Pennsylvania shall maintain jurisdiction over the subject matter of this Assurance and over Respondents for the purpose of enforcing this Assurance.

10.8. Whenever Orbitz or Expedia shall provide notice to the Attorney General under this Assurance, that requirement shall be satisfied by sending notice to John Abel, Assistant Director for Multistate and Special Litigation. Any notices sent to Respondents pursuant to this Assurance shall be sent to the following address: (1) Orbitz Worldwide LLC, ATTN: Chief Legal Officer, 1111 Expedia Way W, Seattle, WA 98119; and (2) Expedia, Inc., ATTN: Chief Legal Officer, 1111 Expedia Way W, Seattle, WA 98119. Any Party may update its address by sending written notice to the other Party. All notices under this Assurance shall be provided via electronic and overnight mail.

10.9. This Court shall maintain jurisdiction over the subject matter of this Assurance and over the Respondents for the purpose of enforcement of this Assurance in accordance with §201-8 of the Consumer Protection Law.

10.10. The Respondents certify that Robert Dzielak, Chief Legal Officer, Expedia and Orbitz, and David Montague, Senior Vice President, Enterprise Risk & Security, Expedia, are authorized by the Respondents to enter into this Assurance on behalf of the Respondents and that his/her signature on this document binds the Respondents to all terms herein.

NOW THEREFORE, Respondents agree by the signing of this Assurance that Respondents shall abide by each and every one of the aforementioned terms of this Assurance, and that the Commonwealth may enforce this Assurance pursuant to §§201-8, 201-9 and 201-9.1 of the Consumer Protection Law by petitioning this Court or any other Court of competent jurisdiction, to order any

equitable or other relief which may be deemed necessary and appropriate as provided herein and by law.

FOR THE PETITIONER:

COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ATTORNEY GENERAL

JOSH SHAPIRO
ATTORNEY GENERAL

Date: 9-12-19

By: _____



TIMOTHY R. MURPHY
Deputy Attorney General
PA Attorney I.D. No. 321294
Bureau of Consumer Protection
1600 Arch Street, Suite 300
Philadelphia, Pennsylvania 19103
Telephone: (215) 560-2414
Facsimile: (215) 560-2494

FOR THE RESPONDENTS:

Expedia, Inc. and Orbitz Worldwide LLC

Date: 12/10/19

By: 

Robert Dzielak, Chief Legal Officer
1111 Expedia Way W
Seattle, WA 98119

Expedia, Inc.

Date: 12/10/19

By: 

David Montague, Senior Vice President
1111 Expedia Way W.
Seattle, WA 98119

Covington & Burling LLP

Counsel to Respondents

Date: _____

By: _____

Michael Imbroscio, PA Attorney I.D. No. 72129
Ashden Fein
Caleb Skeath
One CityCenter
850 Tenth Street NW
Washington, DC 20001

FOR THE RESPONDENTS:


Expedia, Inc. and Orbitz Worldwide LLC

Date: _____ By: _____
Robert Dzielak, Chief Legal Officer
1111 Expedia Way W
Seattle, WA 98119

Expedia, Inc.

Date: _____ By: _____
David Montague, Senior Vice President
1111 Expedia Way W.
Seattle, WA 98119

Covington & Burling LLP
Counsel to Respondents

Date: December 11, 2015 By: 
Michael Imbroscio, PA Attorney I.D. No. 72129
Ashden Fein
Caleb Skeath
One CityCenter
850 Tenth Street NW
Washington, DC 20001

**IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY
FIRST JUDICIAL DISTRICT OF PENNSYLVANIA
CIVIL TRIAL DIVISION**

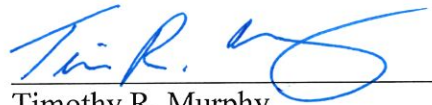
COMMONWEALTH OF PENNSYLVANIA	:
By Attorney General Josh Shapiro	:
	:
Petitioner	:
	:
v.	:
	:
ORBITZ WORLDWIDE LLC	:
	:
and	:
	:
EXPEDIA, INC.	:
	:
Respondents	:

CERTIFICATE OF SERVICE

I, Timothy R. Murphy, Deputy Attorney General, do hereby certify that on the date stated below, a true and correct copy of the executed and filed Assurance of Voluntary Compliance was served upon Respondents, Orbitz Worldwide LLC and Expedia, Inc., by serving Michael Imbroscio, Esquire, Ashden Fein, Esquire, and Caleb Skeath, Esquire, attorneys for Respondents, via USPS first class mail, postage prepaid, at the following address:

One CityCenter
850 Tenth Street NW
Washington, DC 20001

Date: 12-13-19



Timothy R. Murphy
Deputy Attorney General