FILED: 11/7/2022 2:27 PM
Vermont Superior Court
Washington Unit
22-CV-03908

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

IN RE:	**EXPERIAN INFORMATION SOLUTIONS, INC.**	)	**CIVIL DIVISION** **DOCKET NO. _____**

ASSURANCE OF DISCONTINUANCE

This Assurance of Discontinuance ("Assurance")[1] is entered into by the Attorneys General[2] of Arizona, Arkansas, Connecticut, Delaware, the District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Vermont, Virginia, Washington, and Wisconsin (collectively, the "ATTORNEYS GENERAL") and Defendant Experian Information Solutions, Inc. ("EXPERIAN") (collectively, the "Parties") to resolve the investigation of the ATTORNEYS GENERAL into the data breach discovered by Experian on September 15, 2015. The investigation examined the alleged facts and circumstances surrounding this incident and whether EXPERIAN complied with the STATE CONSUMER PROTECTION ACTS, STATE PERSONAL INFORMATION PROTECTION ACTS, and STATE DATA BREACH NOTIFICATION ACTS.

[1] This Assurance of Discontinuance shall, for all necessary purposes, also be considered an Assurance Voluntary Compliance.

[2] For ease of reference, this entire group will be referred to collectively herein as the "ATTORNEYS GENERAL" or individually as "Attorney General." Such designations, however, as they pertain to Connecticut, shall refer to the Attorney General, both acting on his own behalf and as authorized by the Commissioner of the Department of Consumer Protection. Such designations, as they pertain to Hawaii, shall refer to the Executive Director of the State of Hawaii Office of Consumer Protection. Such designations, as they pertain to Maryland, shall refer to the Consumer Protection Division of the Office of the Attorney General of Maryland, which has authority to enter into this Assurance pursuant to Md. Code Ann., Com. Law § 13-402.

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 EXPERIAN and the ATTORNEYS GENERAL of claims related to the data breach discovered by EXPERIAN on September 15, 2015, in which a cyber attacker gained unauthorized access to portions of the EXPERIAN NETWORK that stored PERSONAL INFORMATION of consumers who had applied for services offered by T-Mobile USA, Inc. The data breach affected approximately 15 million individuals nationwide ("2015 DATA BREACH"). The compromised information included names, addresses, dates of birth, Social Security numbers, government identification numbers, and related information used in T-Mobile's assessment of consumers' credit histories.

II. DEFINITIONS

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

a. "2015 DATA BREACH" shall mean the security incident discovered by EXPERIAN on or about September 15, 2015 in which a cyber attacker gained unauthorized access to portions of the EXPERIAN NETWORK that stored PERSONAL INFORMATION of consumers who had applied for services offered by T-Mobile USA, Inc.

b. "AFFECTED CONSUMERS" shall mean all consumers whose PERSONAL INFORMATION was accessible to unauthorized individuals in connection with the 2015 DATA BREACH.

c. "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(s) to be impractical to implement at the present time due to legitimate technical or business constraints. Such alternative mechanisms must: (1) meet the intent 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(s) agree(s) with both the risk analysis and the determination that the risk is acceptable.

d. "CREDIT REPORT" shall mean a consumer report as defined in 15 U.S.C. § 1681a(d) generated by EXPERIAN.

e. "CRITICAL ASSETS" shall be any hardware, software, and network security device that either EXPERIAN or any third party on EXPERIAN's behalf uses to collect, store, transmit, or use PERSONAL INFORMATION.

f. "EFFECTIVE DATE" shall be December 7, 2022.

g. "ENCRYPT", "ENCRYPTED", or "ENCRYPTION" shall mean rendering data—at rest or in transit—unusable, unreadable or indecipherable through an algorithm generally accepted in the field of information security commensurate with the sensitivity of the data at issue.

h. "EXPERIAN" shall mean Experian Information Solutions, Inc., its affiliates, subsidiaries and divisions, successors and assigns, and officers and employees doing business in the United States.

i. "EXPERIAN NETWORK" shall mean all networking equipment, databases or data stores, applications, servers, and endpoints that: (1) are capable of using and sharing software, data, and hardware resources; (2) are owned, operated, and/or controlled by EXPERIAN; and (3) collect, process, store, or have access to PERSONAL INFORMATION of consumers who reside in the United States.

j. "MULTISTATE LEADERSHIP COMMITTEE" shall mean the Attorneys General of the States of Connecticut, Illinois, Maryland, Massachusetts, and Texas and the Attorney General for the District of Columbia, as represented by designated individuals.

k. "PERSONAL INFORMATION" shall mean the following:

i. The individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number; (c) state or federal issued identification number, including passport number and military identification number; or (d) financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's financial account;

ii. Any biometric information, meaning data generated by electronic measurements of the individual's unique physical characteristics, such as a fingerprint, voiceprint, retina or iris image, or other unique physical characteristics or digital representation thereof;

iii. A username or e-mail address in combination with a password or security question and answer that would permit access to an online account of the individual; and

iv. Any additional personal information found in the definition as set forth in the STATE DATA BREACH NOTIFICATION ACTS and/or STATE PERSONAL INFORMATION PROTECTION ACTS.

l. "SECURITY EVENT" shall mean any compromise, or threat that gives rise to a reasonable likelihood of compromise, to the confidentiality, integrity, or availability of PERSONAL INFORMATION of consumers who reside in the United States where such PERSONAL INFORMATION is collected, processed, transmitted, stored, or disposed of by EXPERIAN.

m. "SECURITY INCIDENT" for purposes of this Assurance shall mean any compromise by unauthorized access or inadvertent disclosure to the confidentiality, integrity, or availability of PERSONAL INFORMATION of at least 500 consumers who reside in the United States where such PERSONAL INFORMATION is collected, processed, transmitted, stored, or disposed of by EXPERIAN.

n. "STATE CONSUMER PROTECTION ACTS" shall mean the statutes listed in Appendix A.

o. "STATE DATA BREACH NOTIFICATION ACTS" shall mean the statutes listed in Appendix B.

p. "STATE PERSONAL INFORMATION PROTECTION ACTS" shall mean the statutes listed in Appendix B.

III. ASSURANCES

COMPLIANCE WITH STATE LAW

2. EXPERIAN shall comply with the STATE CONSUMER PROTECTION ACTS, STATE PERSONAL INFORMATION PROTECTION ACTS, and STATE DATA BREACH NOTIFICATION ACTS, in connection with its collection, maintenance, safeguarding, and disposal of PERSONAL INFORMATION of consumers.

3. EXPERIAN shall not make any representations or material omissions of fact that are capable of misleading client companies that store, maintain, or transmit PERSONAL INFORMATION through the EXPERIAN NETWORK regarding the extent to which EXPERIAN maintains and/or protects the privacy, security, confidentiality, or integrity of any PERSONAL INFORMATION collected from or about consumers.

4. EXPERIAN shall comply with the STATE DATA BREACH NOTIFICATION ACTS. If a SECURITY INCIDENT does not trigger the STATE DATA BREACH NOTIFICATION ACTS, EXPERIAN shall create a report that includes a description of the SECURITY INCIDENT and EXPERIAN's response to that SECURITY INCIDENT ("SECURITY INCIDENT REPORT"). EXPERIAN shall retain and make available the SECURITY INCIDENT REPORT, as set forth in Paragraph 39.

INFORMATION SECURITY PROGRAM

5. EXPERIAN shall, within ninety (90) days after the EFFECTIVE DATE of this Assurance, implement, maintain, and comply with a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the confidentiality, integrity, and availability of PERSONAL INFORMATION on the EXPERIAN NETWORK. EXPERIAN's Information Security Program shall be written in one or more parts and shall contain administrative, technical, and physical safeguards appropriate to:

a. The size and complexity of EXPERIAN's operations;

b. The nature and scope of EXPERIAN's activities; and

c. The sensitivity of the PERSONAL INFORMATION on the EXPERIAN NETWORK.

The Information Security Program shall be regularly reviewed and revised. At a minimum, the Information Security Program shall include the requirements of Paragraphs 6 through 33 in this Assurance.

6. EXPERIAN shall consider and, where feasible, utilize the principles of zero-trust, as defined by the National Institute of Standards and Technology[3] in the design of EXPERIAN's Information Security Program. The time requirements of Paragraph 5 shall not apply to this Paragraph provided, however, that EXPERIAN shall develop a written plan and timetable with respect to implementation of zero-trust principles and document its progress against the plan and timetable, including any significant delays or revisions of the same as well as the business justifications for those delays or revisions.

7. EXPERIAN may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Assurance through review, maintenance, and, if necessary, updating, of an existing information security program or existing safeguards, provided that, at a minimum, such existing or updated information security program and safeguards meet the requirements set forth in this Assurance.

8. EXPERIAN shall ensure that its security office employees responsible for implementing, maintaining, monitoring, or updating the Information Security Program receive notice and have sufficient knowledge of the requirements of this Assurance and receive specialized training on safeguarding and protecting consumer PERSONAL INFORMATION to help effectuate EXPERIAN's compliance with the terms of this Assurance. EXPERIAN shall provide any training required under this paragraph which exceeds its current training to all subject security

[3] National Institute of Standards and Technology Special Publication 800-207, Natl. Inst. Stand. Technol. Spec. Publ. 800-207, 59 pages (August 2020), or any succeeding publication.

office employees within sixty (60) days of the EFFECTIVE DATE of this Assurance or prior to their starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program, whichever occurs first. On an annual basis, EXPERIAN shall provide training on safeguarding and protecting PERSONAL INFORMATION to its employees who handle PERSONAL INFORMATION, and its employees responsible for implementing, maintaining, or monitoring the Information Security Program.

INFORMATION SECURITY PROGRAM — GOVERNANCE

9. EXPERIAN shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program (for ease, hereinafter referred to as the "Chief Information Security Officer"). The Chief Information Security Officer shall have the education, qualifications, and experience appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program. This Chief Information Security Officer shall:

a. Report at least quarterly to the EXPERIAN Board of Directors or an appropriate committee on the adequacy of EXPERIAN's Information Security Program, and at least monthly to EXPERIAN'S Chief Executive Officer, regarding the security posture of the EXPERIAN NETWORK, the security risks faced by EXPERIAN, and the implications of any decisions that may impact the security of the EXPERIAN NETWORK.

b. Report to EXPERIAN'S Chief Executive Officer any SECURITY INCIDENT within forty-eight (48) hours of discovery. Any reports made under this sub-paragraph shall also be included in the reports at the next meeting of the Board of Directors or appropriate committee.

10. EXPERIAN shall ensure that the Chief Information Security Officer and the Information Security Program receive the resources and support reasonably necessary to ensure that the Information Security Program functions as required by this Assurance.

INFORMATION SECURITY PROGRAM — INCIDENT PREPAREDNESS

11. EXPERIAN's Information Security Program shall be designed and implemented to ensure the appropriate identification of, investigation of, and response to SECURITY EVENTS.

12. EXPERIAN shall implement and maintain a written incident response plan to prepare for and respond to SECURITY EVENTS. EXPERIAN shall revise and update this response plan, as necessary, to adapt to any changes to the EXPERIAN NETWORK. Such a plan shall, at a minimum, identify and describe the following phases:

a. Preparation;

b. Detection and Analysis;

c. Containment;

d. Notification and Coordination with Law Enforcement;

e. Eradication;

f. Recovery;

g. Consumer Notification and Remediation;

h. Regulator Notification and Response; and

i. Post-Incident Analysis.

13. EXPERIAN shall conduct, at a minimum, bi-annual incident response plan exercises ("table-top" exercises) to test the sufficiency of the incident response plan and assess its preparedness to respond to a SECURITY EVENT.

DUE DILIGENCE AND ACQUISITIONS

14. **Due Diligence – Prior to Acquisition and Integration:** Prior to acquiring any entity that maintains, processes, or transmits PERSONAL INFORMATION, EXPERIAN must use reasonable efforts to obtain, review, and assess:

a. Details about when, from where, to what extent, and how the entity collects, stores, processes, and transfers PERSONAL INFORMATION;

b. The entity's network and system architecture and data flows;

c. The security controls that the entity has in place to protect PERSONAL INFORMATION;

d. An inventory of all prospective Critical Assets including hardware, software, tools, and utilities used in support of the entity's business operations;

e. All written information security programs and policies maintained by the entity;

f. All documented information governance guidelines and standards maintained by the entity, including information governance categories and retention and destruction requirements for each category;

g. Details of risk assessment and risk management programs implemented by the entity, including copies of any reports issued in connection therewith, for the previous five (5) years;

h. All policies concerning the collection, maintenance, safeguarding, and disposal of PERSONAL INFORMATION;

i. The results of any audits or assessments conducted concerning the entity's network and application vulnerabilities, including the results of the most recent penetration test performed with respect to the network, and documentation of resulting remediation efforts;

j. All material contracts with, and any associated risk assessments conducted with respect to any vendors that have access to PERSONAL INFORMATION;

k. Copies of all insurance policies in place in the past five (5) years providing coverage for SECURITY EVENTS; and

l. Details of any known event(s) that could give rise to an insurance claim as a result of a SECURITY EVENT regardless of deductible, as well as any claims history involving SECURITY EVENTS, for the past five (5) years.

15. **Pre-Acquisition Risk Assessment**: Based on the due diligence performed under Paragraph 14 of this Assurance, EXPERIAN shall conduct its own risk assessment with respect to the security of PERSONAL INFORMATION to be acquired, including an analysis of any identified vulnerabilities and weaknesses that threaten the security of the PERSONAL INFORMATION to be acquired, and remediation efforts required before integration of any application or information system of the acquired entity with the EXPERIAN NETWORK.

16. **Integration Plan**: EXPERIAN shall evaluate the data security requirements that must be met before an application or information system of the acquired entity is integrated into the EXPERIAN NETWORK, including: (i) an assessment of whether the application or information system meets the requirements of this Assurance; and (ii) an assessment of all deficiencies and weaknesses requiring remediation. EXPERIAN shall develop an integration plan and timeline reflecting this analysis. EXPERIAN shall not fully integrate any application or information system into the EXPERIAN NETWORK until such application or information system meets the standards of this Assurance.

17. **Documentation Requirements**: EXPERIAN shall document its efforts to comply with the requirements set forth in Paragraphs 14 through 16 of this Assurance. All such

documentation shall be maintained by the Chief Information Security Officer or his or her designee, and shall be provided to the ATTORNEYS GENERAL upon request.

PERSONAL INFORMATION SAFEGUARDS AND CONTROLS

18. **Data Collection & Retention**: EXPERIAN shall collect, store, maintain, and/or process PERSONAL INFORMATION within the EXPERIAN NETWORK only to the minimum extent necessary to accomplish the intended legitimate business purpose(s) in using such information. EXPERIAN shall maintain, regularly review and revise as necessary, and comply with policies that provide for the secure periodic disposal of PERSONAL INFORMATION that is no longer necessary for the legitimate business purpose for which the PERSONAL INFORMATION was collected, processed, or stored, except where such information is otherwise required to be maintained by law.

19. **Encryption**: EXPERIAN shall maintain, regularly review, revise, and comply with policies requiring EXPERIAN to either (a) ENCRYPT PERSONAL INFORMATION stored in the EXPERIAN NETWORK or transmitted electronically within or outside of the EXPERIAN NETWORK, or (b) utilize COMPENSATING CONTROLS where, and only to the extent that, STATE PERSONAL INFORMATION PROTECTION ACTS do not require ENCRYPTION of PERSONAL INFORMATION.

20. **Social Security Numbers**: EXPERIAN shall make reasonable efforts to reduce its use and storage of consumer Social Security numbers by:

a. Participating in an external organization or working group focused on the development and implementation of alternative means of consumer identity authentication with a goal of identifying options for minimizing its use of Social Security numbers for identity authentication purposes, to the extent that any such group exists; and

b. Conducting its own study of the primary instances in which Social Security numbers are collected, maintained, or used on the EXPERIAN NETWORK, including for consumer authentication purposes, and evaluating potential alternatives to such collection, maintenance, or use. In evaluating such alternatives, EXPERIAN may consider, among other things, the impact on privacy, security, reducing identity theft and fraud, and ease of incorporation into EXPERIAN's business processes. Upon the conclusion of this study, or within one year of the December 7, 2022, whichever is sooner, the study shall be provided to the Chief Executive Officer, who shall establish a working group to implement identified alternatives, where feasible.

SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS

21. **Segmentation:**

a. EXPERIAN shall maintain, regularly review and revise as necessary, and comply with segmentation protocols and policies reasonably designed to segment the EXPERIAN NETWORK, which shall, at a minimum, ensure that systems communicate with each other only to the extent necessary to perform their business and/or operational functions.

b. EXPERIAN shall ensure that servers hosting client applications that use, collect, transmit, process, or store PERSONAL INFORMATION in the EXPERIAN NETWORK are properly segmented from all other EXPERIAN servers that process or store other EXPERIAN clients' data in the EXPERIAN NETWORK.

c. EXPERIAN shall logically separate its production and non-production environments in the EXPERIAN NETWORK, including the use of appropriate technological safeguards to protect PERSONAL INFORMATION within non-production environments.

22. **Network Access Controls**: EXPERIAN shall regularly scan and evaluate the ports on the EXPERIAN NETWORK, and restrict and/or disable such ports as appropriate to ensure that they are only left open to the extent necessary for legitimate business purposes.

23. **Asset Inventory and Managing Critical Assets:**

a. EXPERIAN shall use reasonable efforts to develop and maintain an inventory of all assets that comprise the EXPERIAN NETWORK, including but not limited to all software, applications, network components, databases, data stores, tools, technology, and systems. The asset inventory shall, at a minimum, identify: (i) the name of the asset; (ii) the version of the asset; (iii) the owner of the asset; (iv) the asset's location within the EXPERIAN NETWORK; (v) the business need for such asset and its purpose; (vi) the risk criticality level of each asset (i.e., whether the asset is a CRITICAL ASSET; all other assets should be rated as high, medium, or low); and (vii) each security update and security patch applied or installed during the preceding period.

b. EXPERIAN shall ensure that only authorized software and hardware assets are installed or implemented based on their asset inventory.

c. EXPERIAN shall disable and/or remove any assets identified in its asset inventory that are not necessary for any legitimate business purpose performed on the EXPERIAN NETWORK.

d. EXPERIAN shall implement measures to prevent unauthorized assets from connecting to the EXPERIAN NETWORK.

e. EXPERIAN shall update the asset inventory at least annually or whenever there is a change to the EXPERIAN NETWORK that impacts the security of PERSONAL INFORMATION.

24. **Patch and Security Update Management**: EXPERIAN shall maintain reasonable administrative and technical controls to address the potential impact security patches and security updates may have on the EXPERIAN NETWORK and shall, at a minimum:

a. Maintain a patch management and security update solution to manage software patches and security updates that includes the use of automated, standardized tool(s) to: (i) maintain a database of patches and updates applied to the EXPERIAN NETWORK; (ii) install patches and updates on the EXPERIAN NETWORK; (iii) verify installation of patches and updates on the EXPERIAN NETWORK; and (iv) retain historical data of patches and updates installed on the EXPERIAN NETWORK including, but not limited to patch version, patch release date, associated software being patched, and the patch criticality level. The patch management program must also have a dashboard or otherwise report on the success, failure, or other status of any security update or patch. For purposes of clarity, local patching may be utilized where automated, standardized patching is impracticable.

b. Maintain a tool that includes an automated Common Vulnerabilities and Exposures ("CVE") feed. The CVE tool required by this subparagraph shall provide EXPERIAN with near real-time updates regarding known CVEs for vendor-purchased software applications in use within the EXPERIAN NETWORK. The CVE tool required by this subparagraph shall also:

i. Identify, confirm, and enhance discovery of the parts of the EXPERIAN NETWORK that may be subject to CVE events and/or incidents;

ii. Scan the EXPERIAN NETWORK for CVEs; and

iii. Scan the EXPERIAN NETWORK to determine whether scheduled security patches and security updates have been successfully installed, including whether any such

patch or update rated as critical consistent with subparagraph (d) has been installed consistent with the requirements of this Assurance.

c. Prioritize the application of security patches and updates by first applying them to CRITICAL ASSETS, including those identified as such in the inventory created pursuant to Paragraph 23. In prioritizing the application of security patches and updates to CRITICAL ASSETS, EXPERIAN shall consider the risk ratings articulated by the relevant software and application vendors and disseminated by the United States Computer Emergency Readiness Team (US-CERT), and shall either accept the risk ratings or increase the severity of the ratings, as appropriate; provided, however, that EXPERIAN may lower the risk rating in instances where there is no material risk of a SECURITY INCIDENT or EXPERIAN has implemented appropriate COMPENSATING CONTROLS. Experian shall document any decision to lower the risk rating contemporaneously with that decision, and shall include detailed rationale underlying its decision.

d. Within twenty-four (24) hours, if feasible, but not later than forty-eight (48) hours of becoming aware of the availability of any security patch or security update for a vulnerability rated as critical by either US-CERT or another security advisory organization, and/or a relevant software or application vendor (and not lowered pursuant to Paragraph 24.c above), or providing its own critical rating to any patch or update, either (a) apply the patch or update to the EXPERIAN NETWORK or (b) take the identified application offline until the patch or update has been successfully applied. If EXPERIAN is not able to, within forty-eight (48) hours of rating any security update or patch as critical, either apply the update or patch to the EXPERIAN NETWORK or take the identified application offline, then EXPERIAN shall apply COMPENSATING CONTROLS as appropriate.

e. Following the scheduling and installation of any critical security patch or security update, test and verify that the patch or update was applied and installed successfully throughout the EXPERIAN NETWORK. For each security patch or security update rated as critical, EXPERIAN shall prepare a report identifying: (1) the critical patch or update that has been applied; (2) the date(s) the patch or update was applied; (3) the assets to which the patch or update was applied; and (4) whether the patch or update was applied and installed successfully (the "Critical Patch Report"). The Critical Patch Report shall be reviewed on a weekly basis by the Chief Information Security Officer or his or her designee.

f. On at least a biannual basis, EXPERIAN shall perform an internal assessment of its management and implementation of security patches and security updates for the EXPERIAN NETWORK. This assessment shall identify (i) all known vulnerabilities to the EXPERIAN NETWORK and (ii) the patches or updates applied to address each vulnerability.

25. **Intrusion Detection and Prevention Solutions**: EXPERIAN shall implement and maintain intrusion detection and prevention solutions, and ensure that such solutions are properly configured to detect and prevent unauthorized access to the EXPERIAN NETWORK. At a minimum, such solutions shall include a means of detecting malicious files or activities between the internal and external network. Experian shall ensure the intrusion detection and prevention solution is configured to detect and prevent: (1) malicious scripts (e.g., web shells) from being uploaded onto a web or application server; (2) scripts from being uploaded from external sources; and (3) PERSONAL INFORMATION from being copied, transferred, or retrieved from a system without authorization.

26. **Web Application Firewall**: EXPERIAN shall implement and maintain a web application firewall for any application that contains, maintains, or accesses PERSONAL INFORMATION, and ensure that it is properly configured to only allow authorized traffic.

27. **Access Control and Account Management:**

a. EXPERIAN shall implement and maintain appropriate controls to manage access to, and use of, all accounts with access to PERSONAL INFORMATION, including, without limitation, individual accounts, administrator accounts, service accounts, and vendor accounts.

b. The controls required under subparagraph (a) shall include strong passwords, password confidentiality policies, password-rotation policies, and two-factor authentication or any other equal or greater authentication protocol. For purposes of this subparagraph, any administrative-level passwords shall be ENCRYPTED or secured using a password vault, privilege access monitoring, or an equal or greater security tool that is generally accepted by the security industry.

c. EXPERIAN shall implement and maintain appropriate policies for the secure storage of account passwords based on industry best practices; for example, at the time that this Assurance is being entered by the Parties, hashing passwords stored online using an appropriate hashing algorithm that is not vulnerable to attack, together with an appropriate salting policy, or other equivalent or stronger protections.

d. EXPERIAN shall ensure that passwords and private encryption keys are not stored in plain text within any logs or other files.

e. EXPERIAN shall change or disable all default system credentials once the system is implemented, regardless of the level of permissions associated with such credentials.

f. EXPERIAN shall implement and maintain adequate access controls, processes, and procedures, the purpose of which shall be to grant access to the EXPERIAN NETWORK only after the user has been properly identified, authenticated, reviewed, and approved.

g. EXPERIAN shall immediately terminate access privileges for all persons whose access to the EXPERIAN NETWORK is no longer required or appropriate.

h. EXPERIAN shall limit access to PERSONAL INFORMATION by persons accessing the EXPERIAN NETWORK on a need-to-know and least-privileged basis.

i. EXPERIAN shall maintain an inventory of users who have access to the EXPERIAN NETWORK in order to review and determine whether or not such access remains necessary or appropriate. EXPERIAN shall regularly compare termination lists to user accounts to ensure access privileges have been appropriately terminated. At a minimum, such review shall be performed on a quarterly basis for administrator accounts, service accounts, and vendor accounts.

j. EXPERIAN shall implement and maintain adequate administration processes and procedures to store and monitor the account credentials and access of employees who have privileges to design, maintain, operate, and update the EXPERIAN NETWORK.

28. **Logging and Monitoring:**

a. EXPERIAN shall implement controls to monitor and log all security and operational activities on the EXPERIAN NETWORK.

b. EXPERIAN shall monitor in real time all security and operational activities on the EXPERIAN NETWORK and identify any activity that gives rise to a reasonable likelihood of compromise to the confidentiality, integrity, or availability of PERSONAL INFORMATION.

c. EXPERIAN shall test on at least a monthly basis, any tool used pursuant to this paragraph, to ensure such tool is properly configured, regularly updated, and maintained, and that the EXPERIAN NETWORK is adequately monitored.

d. SECURITY EVENTS identified through the logging and monitoring required under this Assurance shall be appropriately escalated to the Chief Information Security Officer's attention consistent with a written incident escalation protocol. The protocol shall require that all SECURITY INCIDENTS immediately be reported to the Chief Information Security Officer and in no event more than eight (8) hours from the identification of the SECURITY INCIDENT. EXPERIAN shall promptly investigate the SECURITY INCIDENT. If a vulnerability is determined to be the cause of the SECURITY INCIDENT, such vulnerability shall be remediated within twenty-four (24) hours of identification of the vulnerability. If that vulnerability cannot be remediated within twenty-four (24) hours of its identification, then EXPERIAN shall either (a) take the system offline or segregate the system from the EXPERIAN NETWORK until the vulnerability has been remediated, or (b) apply COMPENSATING CONTROLS until the vulnerability has been remediated.

29. **Penetration Testing:**

a. EXPERIAN shall implement and maintain a penetration-testing program reasonably designed to identify, assess, and remediate security vulnerabilities within the EXPERIAN NETWORK. This program shall include at least one annual penetration test and penetration testing after any change to the EXPERIAN NETWORK that creates a material risk to the security of PERSONAL INFORMATION.

b. EXPERIAN shall rate and rank the criticality of all vulnerabilities revealed as a result of penetration testing, and shall rate as "critical" any vulnerability that creates the

likelihood of a SECURITY INCIDENT. For each vulnerability rated as critical, EXPERIAN shall commence remediation planning within twenty-four (24) hours and shall apply the remediation within one (1) week. If the remediation cannot be applied within one (1) week after the vulnerability has received a critical rating, EXPERIAN shall apply COMPENSATING CONTROLS designed to protect PERSONAL INFORMATION as soon as practicable but no later than one (1) week after the vulnerability received a critical rating.

30. **Risk Assessments**

a. EXPERIAN shall maintain and regularly review and revise as necessary a risk-assessment program designed to identify, assess, and remediate risks to the EXPERIAN NETWORK. A risk assessment shall be performed at least annually and with respect to any change to the EXPERIAN NETWORK that creates a material risk to the security of PERSONAL INFORMATION. In cases where EXPERIAN deems a risk to be acceptable, EXPERIAN shall generate and retain a report demonstrating how such risk is to be managed.

b. EXPERIAN shall rate and rank the criticality of all vulnerabilities revealed as a result of any risk assessment, and shall rate as "critical" any vulnerability that creates the likelihood of a SECURITY INCIDENT. For each vulnerability rated as critical, EXPERIAN shall commence remediation planning within twenty-four (24) hours and shall apply the remediation within one (1) week. If the remediation cannot be applied within one (1) week after the vulnerability has received a critical rating, EXPERIAN shall apply COMPENSATING CONTROLS designed to protect PERSONAL INFORMATION as soon as practicable but no later than one (1) week after the vulnerability received a critical rating.

31. **Software Updates:** EXPERIAN shall maintain, keep updated, and support the software on the EXPERIAN NETWORK, taking into consideration the impact a software update

will have on data security in the context of the EXPERIAN NETWORK and its ongoing business and network operations, and the scope of the resources required to maintain, update, and support the software. For any software that will no longer be supported by its manufacturer, EXPERIAN shall commence the evaluation and planning to replace the software or to maintain the software at least one (1) year prior to the date on which the manufacturer's support will cease, or from the date the manufacturer announces it is no longer supporting the software if such period is less than one (1) year.

32. **Unauthorized Applications:** EXPERIAN shall maintain controls designed to identify and prevent the execution of unauthorized applications on the endpoints of the EXPERIAN NETWORK.

33. **Data Loss Protection**: EXPERIAN shall implement and maintain a data loss prevention technology to detect and prevent unauthorized data exfiltration from its environment.

CONSUMER-RELATED RELIEF

34. **Credit Monitoring**: EXPERIAN shall, for five (5) years from the EFFECTIVE DATE, offer and provide AFFECTED CONSUMERS with credit protection services (the "Consumer-Related Relief") at no cost which, at a minimum, shall include:

a. CREDIT REPORT monitoring and automated alerts of any changes;

b. Social Security number monitoring that includes dark web surveillance; and

c. A $1,000,000 identity theft insurance policy, which shall have no deductible and shall cover costs for obtaining services (e.g., credit monitoring, CREDIT REPORTS, dark web surveillance).

AFFECTED CONSUMERS shall have six (6) months to enroll in the Consumer-Related Relief following the initial public announcement of this Assurance. AFFECTED CONSUMERS who so

enroll shall have sixty (60) days following transmission of their redemption code to activate the Consumer-Related Relief.

35. **Credit Reports**: EXPERIAN shall, for at least five (5) years from the EFFECTIVE DATE, offer AFFECTED CONSUMERS at least two (2) free copies of their CREDIT REPORT annually.

36. **Contact for Attorneys General**: EXPERIAN shall designate a department or group to act as the point of contact for the ATTORNEYS GENERAL which will provide assistance to consumers who have submitted complaints to the ATTORNEYS GENERAL.

IV. ASSESSMENT AND REPORTING REQUIREMENTS

37. **Third-Party Assessment:** EXPERIAN shall conduct biennial assessments of its general data security practices, as well as its compliance with the terms of this Assurance as it applies to Experian's Consumer Information Services and Decision Analytics businesses (the "Third-Party Assessment"). The Third-Party Assessments required by this paragraph shall be conducted by an outside, independent third-party with no prior relationship with EXPERIAN other than as an independent third-party security assessor (the "Third-Party Assessor").

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

b. The reporting period for the Third-Party Assessments must cover: (1) the first one hundred and eighty (180) days after the EFFECTIVE DATE for the initial Third-Party Assessment; and (2) each two-year period thereafter for six (6) years after the EFFECTIVE DATE for the biennial Third-Party Assessments.

c. The findings of the Third-Party Assessment shall be documented in an individual report (the "Third-Party Assessor's Report"). The Third-Party Assessor's Reports shall:

i. Identify the specific administrative, technical, and physical safeguards maintained by EXPERIAN;

ii. Document the extent to which the identified administrative, technical, and physical safeguards are appropriate considering EXPERIAN's size and complexity, the nature and scope of EXPERIAN's activities, and the sensitivity of the PERSONAL INFORMATION maintained by EXPERIAN;

iii. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by EXPERIAN meet the requirements of the Information Security Program; and

iv. Specifically review and evaluate EXPERIAN's compliance with penetration testing and risk assessments set forth in Paragraphs 29 and 30; the logging and monitoring requirements set forth in Paragraph 28; and the patch management and security update requirements set forth in Paragraph 24.

d. Each Third-Party Assessment must be completed within sixty (60) days after the end of the reporting period to which the Third-Party Assessment applies. EXPERIAN shall provide a copy of the Third-Party Assessor's Report to the Connecticut Attorney General's Office within ten (10) days of the completion of the Third-Party Assessment.

38. The Vermont Attorney General's Office may provide a copy of the Third-Party Assessor's Report received from EXPERIAN to the Vermont Attorney General upon request, and the Vermont Attorney General shall, to the extent permitted by the laws of the state of Vermont, treat the Third-Party Assessor's report and all information contained therein as confidential and

exempt from disclosure. In the event that the Vermont Attorney General's Office receives a public records request for the Third-Party Assessor's report or other confidential documents under this Assurance and believes that such information is subject to disclosure under the relevant public records laws, the Vermont Attorney General's Office agrees to provide EXPERIAN with at least ten (10) days advance notice before producing the information, to the extent permitted by state law (or with any required lesser advance notice), so that EXPERIAN may take appropriate action to defend against the disclosure of such information. The notice under this paragraph shall be provided consistent with the notice requirements contained in Paragraph 57. Nothing contained in this subparagraph shall alter or limit the obligations of the Vermont Attorney General that may be imposed by the relevant public records laws of the State of Vermont, or by order of any court, regarding the maintenance or disclosure of documents and information supplied to the Vermont Attorney General.

DOCUMENT RETENTION

39. EXPERIAN shall retain and maintain the reports, records, documentation, exceptions, and information required by this Assurance for a period of no less than five (5) years from the date of their creation and make them available to the Third-Party Assessor required under this Assurance.

V. MONETARY PAYMENT

40. No later than thirty (30) days after the EFFECTIVE DATE, EXPERIAN shall pay a total of TWELVE MILLION SIX-HUNDRED SEVENTY-ONE THOUSAND SIX HUNDRED NINE DOLLARS AND ELEVEN CENTS ($12,671,609.11) to the ATTORNEYS GENERAL. Said payment shall be divided and paid to each of the ATTORNEYS GENERAL in an amount to

be designated by the MULTISTATE LEADERSHIP COMMITTEE and communicated to EXPERIAN.

41. Of the total amount, EXPERIAN will pay One Hundred Thousand Dollars ($100,000.00) to the State of Vermont. The State may use the payment in any of the following ways: (1) to pay for attorney's fees and other costs of investigation and litigation; (2) to place in, or apply to, consumer protection enforcement, including future consumer protection enforcement, consumer education, litigation, or local consumer aid or revolving funds; (3) to defray the costs of the inquiry leading to this final Judgement; (4) for any lawful purpose, at the sole discretion of the Attorney General; and (5) pursuant to 32 V.S.A. § 462.

VI. RELEASE

42. Following full payment of the amount due under this Assurance to the State of Vermont, the Vermont Attorney General shall release and discharge EXPERIAN from all civil claims that it could have brought under the STATE CONSUMER PROTECTION ACTS, the STATE PERSONAL INFORMATION PROTECTION ACTS, and/or the STATE DATA BREACH NOTIFICATION ACTS based on EXPERIAN's conduct related to the 2015 DATA BREACH. Nothing contained in this paragraph shall be construed to limit the ability of the Vermont Attorney General to enforce the obligations that EXPERIAN has under this Assurance. Further, nothing in this Assurance shall be construed to create, waive, or limit any private right of action.

43. Notwithstanding any term of this Assurance, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 42 as to any entity or person, including EXPERIAN:

a. Any criminal liability that any person or entity, including EXPERIAN, has or may have to the States.

b. Any civil or administrative liability that any person or entity, including EXPERIAN, has or may have to the States under any statute, regulation, or rule giving rise to, any and all of the following claims:

i. State or federal antitrust violations;

ii. State or federal securities violations; or

iii. State or federal tax claims.

44. Nothing in this Assurance shall be construed as excusing or exempting EXPERIAN from complying with any state or federal law, rule, or regulation, nor shall any of the provisions of this Assurance be deemed to authorize or require EXPERIAN to engage in any acts or practices prohibited by any law, rule, or regulation.

VII. GENERAL PROVISIONS

45. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Assurance after the EFFECTIVE DATE, or to compromise the authority of the ATTORNEYS GENERAL to initiate a proceeding for any failure to comply with this Assurance. Any failure by the ATTORNEYS GENERAL to insist upon EXPERIAN's compliance with any of the provisions of this Assurance shall not be deemed a waiver of any provisions hereof, and the ATTORNEYS GENERAL, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by EXPERIAN.

46. Other than as specifically set forth herein, nothing in this Assurance shall be construed to limit the authority or ability of the ATTORNEYS GENERAL to protect the interests

of the States. This Assurance shall not bar the ATTORNEYS GENERAL or any other governmental entity from enforcing laws, regulations, or rules against EXPERIAN 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 ATTORNEYS GENERAL to enforce the obligations that EXPERIAN has under this Assurance.

47. Nothing in this Assurance shall be construed as relieving EXPERIAN 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.

48. EXPERIAN shall deliver a copy of this Assurance to, and otherwise fully apprise, its Chief Executive Officer, its Chief Information Security Officer, General Counsel, and its Board of Directors within ninety (90) days of the EFFECTIVE DATE. To the extent EXPERIAN replaces any of the above listed officers, counsel, or Directors, EXPERIAN shall deliver a copy of this Assurance to their successors within ninety (90) days from the date on which such person assumes his/her position with EXPERIAN.

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

50. EXPERIAN 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 EXPERIAN further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

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

52. If any portion of this Assurance is held invalid or unenforceable, the remaining terms of this Assurance shall not be affected and shall remain in full force and effect.

53. In states where this Assurance must be filed with and/or approved by a court, EXPERIAN consents to the filing of this Assurance and its approval by the court, and authorizes the ATTORNEYS GENERAL in such states to represent that EXPERIAN does not object to court approval of the Assurance. EXPERIAN further consents to the jurisdiction of each such court for the purpose of approving or enforcing this Assurance. To the extent there are any court costs associated with the filing of this Assurance, EXPERIAN agrees to pay such costs.

54. EXPERIAN hereby acknowledges that its undersigned representative or representatives are authorized to enter into and execute this Assurance. EXPERIAN has been represented by legal counsel and has been advised by their legal counsel of the meaning and legal effect of this Assurance.

55. This Assurance does not constitute an approval by the ATTORNEYS GENERAL of any of EXPERIAN's past or future practices, and EXPERIAN shall not make any representation to the contrary.

56. The ATTORNEYS GENERAL's investigation was conducted pursuant to the STATE CONSUMER PROTECTION ACTS, STATE PERSONAL INFORMATION PROTECTION ACTS, and STATE DATA BREACH NOTIFICATION ACTS in connection with Experian's conduct relating to the 2015 DATA BREACH. Experian's agreement to enter into this settlement and its related payment is made exclusively to resolve the ATTORNEYS GENERAL's investigation, and is not based on any court or administrative finding of: (a) gross negligence, (b)

recklessness, (c) deliberate, willful, dishonest, fraudulent, or malicious acts, errors, or omissions, or (d) any intentional or knowing violation of the law on the part of EXPERIAN.

VIII. NOTICES UNDER THE ASSURANCE

57. Any notices or other documents required to be sent under this Assurance shall be sent to the following address via first class and electronic mail. Any party may update its designee or address by sending written notice to the other party informing them of the change.

For the Vermont ATTORNEY GENERAL:

Merideth C. Chaudoir, AAG
State of Vermont
Office of the Attorney General
109 State Street
Montpelier, VT 05609-1001
merideth.chaudoir@vermont.gov

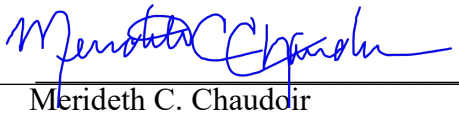
For EXPERIAN:

Office of the General Counsel
475 Anton Blvd
Costa Mesa, CA 92626
(714) 830-7000

APPROVED:

STATE OF VERMONT

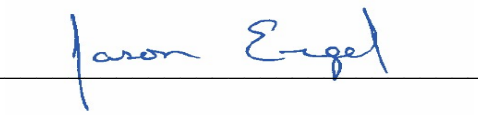
SUSANNE R. YOUNG
ATTORNEY GENERAL

By:  Date: November 7, 2022

Merideth C. Chaudoir
Assistant Attorney General
Office of the Attorney General
109 State of Vermont
Montpelier, VT 05609-1001
Merideth.chaudoir@vermont.gov
802-828-5479

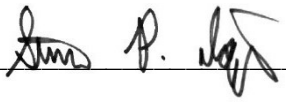
APPROVED:

DEFENDANT
EXPERIAN INFORMATION SOLUTIONS, INC.

By:  Date: 10/27/2022

Jason Engel
Global Chief Privacy, Ethics and Compliance Officer
Experian Information Solutions, Inc.
475 Anton Blvd.
Costa Mesa, CA 92626
(714) 830-5502
Jason.Engel@experian.com

COUNSEL FOR DEFENDANT, EXPERIAN INFORMATION SOLUTIONS, INC.

By:  Date: 10/25/2022

Stuart P. Ingis
Venable LLP
600 Massachusetts Ave. NW
Washington, DC 20001
(202) 344-4613
SIngis@venable.com

LOCAL COUNSEL FOR DEFENDANT, EXPERIAN INFORMATION SOLUTIONS, INC.

By: /s/ Geoffrey J. Vitt Date: 11/1/2022

Geoffrey J. Vitt
Vitt & Associates
8 Beaver Meadow Road
Norwich, VT 05055
802-649-5700
gvitt@vittandassociates.com

Attorney for Experian Information Solutions, Inc.