RECEIVED
ATTORNEY GENERAL OF OHIO

NOV 07 2022

CONSUMER PROTECTION SECTION
PUBLIC INSPECTION FILE

IN THE MATTER OF:	§	
	§	**DOCKET NO.: 515393**
T-MOBILE USA, INC.	§	

ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance[1] ("Assurance") is entered into by the Attorneys General of Arizona[2], Arkansas, Connecticut[3], District of Columbia, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New York, Nevada, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Vermont[4], Virginia, Washington and Wisconsin (referred to collectively as the "Attorneys General") and T-Mobile USA, Inc. ("T-Mobile"; collectively, with the Attorneys General, the "Parties") to resolve the investigation by the Attorneys General into the unauthorized access to portions of the Experian network that stored the sensitive personal information of individuals who had applied for postpaid services offered by T-

[1] The term "Assurance" as used herein may refer to the Assurance of Voluntary Compliance or an Assurance of Discontinuance, as applicable.

[2] The State of Arizona, *ex rel.* Mark Brnovich, Attorney General, and T-Mobile have agreed to entry into the settlement, of which the Assurance is a part, pursuant to Arizona Revised Statutes ("A.R.S.") § 44-1530 of the Arizona Consumer Fraud Act, A.R.S. §§ 44-1521 to 44-1534. T-Mobile has consented and stipulated to the terms of this Assurance and has agreed to enter it, to compromise and settle claims in connection with the multi-state investigation by the State Attorneys General listed in this paragraph.

[3] 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. "Connecticut Attorney General" shall mean only the Attorney General. 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.

[4] For Vermont, in lieu of instituting an action or proceeding against T-Mobile, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Assurance of Discontinuance. By signing below, T-Mobile voluntarily agrees with and submits to the terms of this Assurance of Discontinuance.

Mobile and that was announced by T-Mobile on or about September 30, 2015 (the "2015 Experian Data Breach").

In consideration of their mutual agreement 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 T-Mobile and the Attorneys General of claims related to the 2015 Data Breach in which a person or persons gained unauthorized access to portions of Experian's computer systems that included Personal Information of individuals who had applied for postpaid services offered by T-Mobile. By entering into this Assurance, neither Party is taking any position on any substantive issue, including any wrongdoing, fault, violation of law, deviation from industry norms and practices, liability, or any causal relationship between any action or inaction by T-Mobile and the 2015 Experian Data Breach.

II. DEFINITIONS

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

   A. "2015 Experian Data Breach" shall mean the security incident in which a person or persons gained unauthorized access to portions of the Experian network that stored the Personal Information of individuals who applied for postpaid services offered by T-Mobile and that was announced by T-Mobile on or about September 30, 2015. "2015 Experian Data Breach" shall not,

under any circumstances and regardless of the consumers impacted, data involved, or the date of discovery or compromise, include any security incidents announced on or after October 1, 2015 ("Future Incidents").

B. "Consumer" shall mean any individual who provides Personal Information to T-Mobile in connection with any offer or transaction for goods or services.

C. "Consumer Protection Acts" shall mean the State unfair and deceptive acts and practices statutes listed in Appendix A.

D. "Effective Date" shall be December 7, 2022.

E. "Leadership States" shall mean the Maryland, Connecticut, Illinois and the District of Columbia Attorneys General.

F. "Personal Information" shall mean the data elements in the definitions of Personal Information set forth in the applicable Security Breach Notification Acts and/or Personal Information Protection Acts listed in Appendix B. Nothing in this Assurance would broaden the jurisdiction or scope of any such law, or nullify any exceptions.

G. "Personal Information Protection Acts" shall mean the statutes listed in Appendix B.

H. "Security Breach Notification Acts" shall mean the statutes listed in Appendix B.

I. "T-Mobile" shall mean T-Mobile USA, Inc., its affiliates, subsidiaries and divisions, successors and assigns doing business in the United States.

J. "Security Event" shall mean any compromise that results in the unauthorized access, acquisition, or exfiltration of Personal Information owned, licensed, or maintained by T-Mobile or any Consumer Personal Information maintained by any Vendor.

K. "Vendor" shall mean any third party that accesses, collects, or stores Consumer Personal Information on behalf of T-Mobile, pursuant to a contract with T-Mobile. For purposes of this Assurance, "Vendor" shall not include: 1) any third party that only accesses, collects, or stores de minimis amounts of Consumer Personal Information on behalf of T-Mobile; 2) law firms and third party dealers[5]; and 3) any third party that is of a type that is not monitored by T-Mobile's Third Party Risk Management processes and procedures as of the Effective Date.[6] It shall be T-Mobile's burden to show that a third party falls within one of the above exceptions.

III. APPLICATION

2. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall, subsequent to the Effective Date, apply to T-Mobile, its affiliates, subsidiaries, agents, directors, successors and assigns, and its executive management officers having decision-making authority with respect to the subject matter of this Assurance.

---

[5] For purposes of this Assurance, the term "third party dealers" shall refer only to third party retailers that sell T-Mobile products and services.

[6] The parties agree that any third party, or type of third party, monitored by T-Mobile's Third Party Risk Management processes and procedures within the two (2) years preceding the Effective date shall not fall under exception (3) to the definition of "Vendor" and shall continue to be subject to T-Mobile's Third Party Risk management processes and procedures, as required by this Assurance, after the Effective Date.

IV. ASSURANCES

GENERAL COMPLIANCE

3. Subsequent to the Effective Date:

   A. T-Mobile shall comply with the Consumer Protection Acts, Personal Information Protection Acts and Security Breach Notification Acts, as applicable, in connection with its collection, use, and maintenance of Personal Information, and shall maintain reasonable security policies and procedures, consistent with applicable state and federal laws and industry norms and practices, designed to safeguard Personal Information from unauthorized use or disclosure.

   B. T-Mobile shall not misrepresent the extent to which T-Mobile maintains and protects the privacy, security, or confidentiality of Personal Information collected from or about Consumers.

   C. T-Mobile shall comply with the reporting and notification requirements set forth in any applicable Security Breach Notification Act.

INFORMATION SECURITY PROGRAM

4. T-Mobile shall maintain and continue to implement a written information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information that T-Mobile collects, stores, and/or transmits. T-Mobile shall also have a vendor management program that incorporates the specific vendor management requirements set forth in Paragraphs 12 through 20 of this Assurance ("Vendor Management Program"). For purposes of this Assurance, the term "Information Security

Program" will be understood to include the Vendor Management Program, but nothing in this Assurance is intended to require any particular relationship between T-Mobile's implementation of its Information Security Program and Vendor Management Program.

5. The Information Security Program shall comply with any applicable requirements under state or federal law, and shall contain reasonable administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of T-Mobile's operations; (ii) the nature and scope of T-Mobile's activities; and (iii) the sensitivity of the Personal Information that T-Mobile collects, stores, and/or transmits.

6. The Information Security Program shall be written and modified to require reasonable efforts to collect and share Personal Information only to the minimum extent necessary to satisfy legitimate business purposes.

7. T-Mobile shall review the Information Security Program not less than annually and make any updates that are necessary to reasonably protect the privacy, security, and confidentiality of Personal Information that T-Mobile collects, stores, and/or transmits.

8. T-Mobile shall employ one or more executives or officers responsible for implementing, maintaining, and monitoring the Information Security Program (hereinafter referred to as the Chief Information Security Officer but may be differently titled in an equivalently ranked position) ("CISO"). The CISO shall have credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program.

9. The role of the CISO will include regular and direct reporting to the Chief Executive Officer, Executive Staff, and Board of Directors concerning T-Mobile's security

posture, the security risks faced by T-Mobile, and the security implications of T-Mobile's lines of business.

10. T-Mobile shall provide training on the requirements of its Information Security Program, to employees directly responsible for implementing, maintaining, or monitoring it, including those who report directly or indirectly to the CISO. T-Mobile shall provide the training required under this paragraph to such 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 is later. T-Mobile shall provide notice of the Assurance to employees directly responsible for implementing, maintaining, or monitoring T-Mobile's Information Security Program, within sixty (60) days of the Effective Date of this Assurance.

11. T-Mobile shall maintain and continue to implement its written cyber incident and response plan to prepare for and respond to suspected and confirmed Security Events ("Incident Response Plan"), which shall comply with industry norms and practices and all applicable state and federal laws. The Incident Response Plan shall include a review of the role and security of any Vendor involved in the Security Event.

THIRD-PARTY RISK MANAGEMENT PROGRAM

12. T-Mobile shall maintain and continue to implement written policies and procedures to oversee its Vendors' performance of any security and privacy obligations (arising by contract or law) relating to any Consumer Personal Information provided to Vendors by T-Mobile. T-Mobile shall take reasonable steps to confirm that such Vendors are taking reasonable security measures to safeguard Consumer Personal Information.

13. **Third-Party Risk Management Team**: T-Mobile shall maintain a dedicated third-party risk management team ("TPRM Team") responsible for implementing and maintaining a comprehensive third-party risk management program ("TPRM Program"). Members of the TPRM Team shall have the appropriate credentials, background, and expertise in information security necessary to effectuate the TPRM Program, including assessing and managing data security risks for Vendors. The TPRM Team shall:

A. Meet frequently and regularly report to the CISO, or his/her designee, on the effectiveness of the TPRM Program, including how the TPRM Team mitigates and monitors vendor security risks.

B. Consider the inherent risk rating assigned to the Vendor engagement pursuant to Paragraph 15 in determining whether to escalate internal reporting regarding a Vendor, including, but not limited to, to the CISO; and

C. Engage in regular meetings with the CISO to identify risk strategies and priorities and to incorporate those into the TPRM Program.

14. **Third-Party Risk Management Program Review**: T-Mobile shall review the TPRM Program not less than bi-annually and make any updates necessary to ensure the reasonable security and confidentiality of Consumer Personal Information that Vendors access, process, or store on behalf of T-Mobile. Any such T-Mobile obligation of oversight is not intended to, nor does it, supplant the Vendor's own responsibility to protect Personal Information under any applicable laws or contracts.

15. **Vendor Inventory**: T-Mobile shall maintain and regularly update an inventory of all active T-Mobile Vendors ("Vendor Inventory") and a repository of active Vendor contracts. T-Mobile shall assign an inherent risk rating to each Vendor engagement or class of vendor engagements based on the nature and type of the Consumer Personal Information accessed, collected, processed, transmitted, used, maintained, or stored by each such Vendor. In assessing a Vendor's ability to protect and secure Consumer Personal Information, T-Mobile shall:

A. Identify the nature and type of Consumer Personal Information that each Vendor may process, transmit, use, or store on T-Mobile's behalf during a specific engagement;

B. Assign a risk rating for each Vendor engagement and design and deploy risk assessments and ongoing monitoring programs appropriate to each level of risk; and

C. Record the date(s) of each Vendor engagement's completed risk assessments.

T-Mobile shall maintain and continue to implement a risk scoring protocol for evaluating its Vendor engagements, given the particularized service the Vendor will provide to T-Mobile and specific categories of Consumer Personal Information that the Vendor accesses, transmits, processes, collects, uses, maintains, or stores. Based on a risk score assigned to Vendor engagements pursuant to T-Mobile's risk scoring protocol, T-Mobile will identify appropriate Vendor engagements as "critical" based on a risk analysis as defined in the risk scoring protocol.

16. **Vendor Contracts- Specific Security Requirements**: Except as provided for in subparagraph C, in all contracts entered into after the Effective Date of this Assurance but before

five (5) years from the Effective Date, that are not already subject to negotiated and agreed-upon security terms, T-Mobile shall require Vendors to implement specific requirements for protecting Consumer Personal Information, including compliance with appropriate industry norms and practices that include cybersecurity or data security-related requirements. These requirements may refer to specific standards, as appropriate, such as the National Institute of Standards and Technology's Cybersecurity Framework, specific policies, or other appropriate benchmarks, as deemed reasonable by security personnel with appropriate qualifications and access to information to make such determinations. In particular:

A. T-Mobile shall contractually obligate its Vendors to comply with the following data security requirements, either by including these requirements expressly, or by mandating compliance with T-Mobile policies, industry standards, or similar that already have such requirements:

   i. In a multi-tenant environment, data stores holding Consumer Personal Information must be segmented from others, or otherwise appropriately protected where segmentation is not possible and where such alternative protections are reasonable based on the nature and quantity of data stored.

   ii. Consumer Personal Information must be accessed, collected, retained, transmitted, used, stored, and shared only to the minimum extent necessary to satisfy legitimate business purposes.

iii. Cryptographic keys must never be stored in locations that do not meet secure key management requirements (e.g., log files, ticket tracking systems, knowledge management systems, or training documentation) as per industry best practices.

iv. Passwords used to protect cryptographic keys must be as strong as the keys they protect.

v. Any software vulnerabilities that may materially impact security as it relates to T-Mobile systems and data must be (a) reported promptly (without unreasonable delay) to T-Mobile; and (b) patched promptly after the release of the software patch, subject to appropriate testing and a confirmation that such patch will not have unintended performance consequences.

vi. All network and information systems used for T-Mobile, in conjunction with the terms of any contractual agreements, must be auditable and includes but not limited to System/OS logs, Application logs, Database logs and Security Control logs.

B. T-Mobile may grant exceptions to the above contractual security requirements during or subsequent to the contracting process; however, the determination to implement an exception 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 CISO

or his or her designee(s) agree(s) with both the risk analysis and the determination that the risk is acceptable.

C. To the extent a Vendor will not or cannot agree to contractually obligate itself to appropriate security safeguards appropriate to the level of risk and data in scope, T-Mobile will consider such risk in assessing the Vendor for engagement, including requiring mitigation or remediation of such risk(s). T-Mobile shall further require that Vendors agree to flow-down T-Mobile's security requirements to their subcontractors and sub-suppliers ("Fourth Parties") who process Consumer Personal Information on behalf of T-Mobile and shall contractually obligate that Vendors have reasonable policies and procedures in place to monitor Fourth Parties' compliance with such requirements. Any non-compliance with these requirements shall be considered a risk factor in assessing the Vendor for engagement, including requiring mitigation or remediation of such risk(s).

17. **Vendor Assessment & Monitoring Mechanisms**: T-Mobile shall utilize a variety of security assessment and monitoring practices to confirm that Vendors are able to comply with T-Mobile's security requirements to safeguard Consumer Personal Information, such as Vendor self-assessments and attestations, third-party audits, formal certifications, risk assessments, penetration tests and/or on-site visits. The frequency, type, and robustness of such assessments shall be based on each Vendor engagement's inherent risk rating and consistent with the requirements of this Assurance.

18. **Vendor Self-Assessments**: Where T-Mobile allows Vendors to provide self-assessments during pre-engagement or ongoing monitoring, T-Mobile shall utilize other layers of review to obtain corroboration of such assessments as appropriate based on the particular circumstances of each situation. The additional layers of review may include, for example, reviewing information provided through commercially available intelligence tools or requesting specific documents from a Vendor, such as reports relating to third party certifications.

19. **Vendor Security Events:** T-Mobile shall require that each Vendor promptly provide notice to T-Mobile whenever that Vendor has experienced a suspected or confirmed Security Event. T-Mobile shall include in its Vendor contracts entered into following the Effective Date of this Assurance the roles and responsibilities to be undertaken by T-Mobile and the Vendor in the event of a Security Event, including obligations for providing notice to Consumers. To the extent feasible, T-Mobile shall amend existing contracts with Vendors rated as critical to include such roles and responsibilities as such contracts come up for renewal.

20. **Vendor Non-Compliance**: T-Mobile shall retain appropriate contractual rights to enforce a Vendor's compliance with T-Mobile's security safeguards and policies, which may include notice and cure procedures or termination of the Vendor's contract and/or data access as may be appropriate. Appropriate action shall include consideration of the totality of the circumstances, including but not limited to, any failure of the Vendor to perform any of its contractual and legally required security and privacy obligations, the cost and risks involved in terminating such Vendor, and the existence of alternative Vendors to provide the same services. When a Vendor will not or cannot agree to the inclusion of the requirements of paragraphs 16

through 19 of this Assurance in any prospective contract with that Vendor, the absence of such requirements will be considered as part of any risk assessment of the Vendor engagement.

V. THIRD PARTY RISK MANAGEMENT PROGRAM ASSESSMENT

21. Not less than one (1) year, but within two (2) years of the Effective Date, T-Mobile shall conduct or obtain an assessment of T-Mobile's TPRM Program, and its compliance with the terms of this Assurance. T-Mobile shall prepare a report of the results of the assessment, which shall include descriptions of each of the processes in place or steps taken to comply with the specific requirements of this Assurance. T-Mobile shall provide a copy of the report to the Connecticut Attorney General within sixty (60) days of its completion.

A. Confidentiality: The Connecticut Attorney General's Office shall, to the extent permitted by the laws of the State of Connecticut, treat the report as confidential and exempt from disclosure under the relevant public records laws.

B. Signatory State Access to report: The Connecticut Attorney General's Office may provide a copy of the report to any other participating Attorneys General upon request, and each requesting Attorney General shall, to the extent permitted by the laws of the Attorney General's State, treat such report as confidential and exempt from disclosure under the relevant public records laws.

VI. DOCUMENT RETENTION

22. T-Mobile shall retain and maintain the policies, inventories, contracts, exceptions and related risk analyses, and other documentation required by this Assurance for a period of no less than three (3) years from the date of their creation.

VII. PAYMENT TO THE STATES

23. T-Mobile shall pay Two Million Four Hundred Thirty-Six Thousand One Hundred Ten Dollars and Seventy-One Cents ($2,436,110.71) to the Attorneys General. Said payment shall be divided and paid by T-Mobile directly to each of the Attorneys General in an amount designated by the Attorneys General and communicated to T-Mobile by the Leadership States. Each of the Attorneys General agrees that the Leadership States have the authority to communicate the designated amount to be paid by T-Mobile to each Attorney General and to provide T-Mobile 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 the Leadership States 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.

24. Of the total amount, T-Mobile will pay Sixty-Eight Thousand One Hundred Thirty-Seven Dollars and Fifteen Cents ($68,137.15) to the Ohio Attorney General. Said payment shall be used by the Ohio Attorney General for such purposes that may include, but are not limited to, being placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray 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 Ohio Attorney General.

VIII. RELEASE

25. Following full payment of the amounts due to the Ohio Attorney General under this Assurance, the Ohio Attorney General shall hereby release and discharge T-Mobile from all civil claims that the Ohio Attorney General could have brought under the Consumer Protection Acts, the Personal Information Protection Acts, and the Security Breach Notification Acts based on any action or inaction by T-Mobile or Experian related to the 2015 Experian Data Breach. Nothing contained in this paragraph shall be construed to limit the ability of the Ohio Attorney General to enforce the obligations that T-Mobile has under this Assurance. Further, nothing in this Assurance shall be construed to create, waive, limit, settle, or release, any claims related to T-Mobile's acts and practices in connection with data security incidents that commenced after the 2015 Experian Data Breach, including without limitation, the data security incident announced by T-Mobile in August 2021, or resolve any private right of action, including such private causes of action, claims or remedies that could be brought under the statutes listed in Appendices A or B, provided however, that nothing in this Assurance limits T-Mobile from raising any position or defense to oppose or limit liability or damages in connection with any Future Incidents.

IX. PRESERVATION OF AUTHORITY

26. 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 T-Mobile for conduct after or otherwise not covered by this Assurance, except to the extent expressly released by this Assurance. Further, nothing in this Assurance shall be construed to limit the ability of the Attorney General to enforce the obligations that T-Mobile has under this Assurance.

X. GENERAL PROVISIONS

27. The Parties understand and agree that this Assurance shall not be construed as an approval or a sanction by the Attorneys General of T-Mobile's business practices, nor shall T-Mobile 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. Further, nothing in this Assurance shall be construed or deemed to be an admission or concession or evidence of any liability or wrongdoing on the part of T-Mobile or of any fact or violation of any law, rule, or regulation, or any causal relationship between any action or inaction by T-Mobile and the 2015 Experian Data Breach.

28. Nothing in this Assurance shall be construed as relieving T-Mobile of the obligation to comply with all applicable 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.

29. As to each individual signatory Attorney General, this Assurance shall be governed by the laws of that Attorney General's state without regard to any conflict of laws principles.

30. T-Mobile 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 Chief Information Security Officer, and each member of its Board of Directors within ninety (90) days of the Effective Date. T-Mobile 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 T-Mobile.

31. In states where statute requires that this Assurance be filed with and/or approved by a court, T-Mobile consents to the filing of this Assurance and to its approval by the court and authorizes the Attorneys General in such states to represent that T-Mobile does not object to the request that the court approve the Assurance. T-Mobile further consents to be subject to the jurisdiction of such courts for the exclusive purposes of having such courts approve or enforce this Assurance. To the extent that there are any court costs associated with the filing of this Assurance, T-Mobile agrees to pay such costs.

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

33. 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.

34. The undersigned T-Mobile representatives state that they are authorized to enter into and execute this Assurance on behalf of T-Mobile and further agree to execute and deliver all authorizations, documents, and instruments which are necessary to carry out the terms and conditions of this Assurance.

35. T-Mobile 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 T-Mobile further waives any right to attorneys' fees related to this Assurance that may arise under such statute, regulation, or rule.

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

XI. SEVERABILITY

37. 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.

XII. NOTICE/DELIVERY OF DOCUMENTS

38. Any notices or other documents required to be sent pursuant to this Assurance shall be sent to the following addresses 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 Ohio Attorney General:

Melissa S. Smith
Assistant Section Chief
Ohio Attorney General's Office, Consumer Protection Section
30 E. Broad Street, Floor 14
Columbus, OH 43215
614.466.6112
Melissa.S.Smith@OhioAGO.gov

Michael S. Ziegler
Principal Assistant Attorney General
Ohio Attorney General's Office, Consumer Protection Section
30 E. Broad Street, Floor 14
Columbus, OH 43215
614.466.3980
Michael.Ziegler@OhioAGO.gov

For T-Mobile:

Bradley I. Ruskin
Nolan M. Goldberg
Proskauer Rose LLP
Eleven Times Square
New York, NY 10036-8299
bruskin@proskauer.com
ngoldberg@proskauer.com

Consented and agreed to by:

T-Mobile USA, Inc.

By: */s/ Rachel A. Adams* Date: 11/01/2022

Rachel A. Adams
Senior Vice President, Legal Affairs
3625 132nd Avenue, SE
Bellevue, WA 98006

As Duly Authorized Representative of T-Mobile USA, Inc.

By: */s/ Bradley I. Ruskin* Date: 10/31/2022

Bradley I. Ruskin
Partner, Proskauer Rose LLP
Eleven Times Square
New York, NY 10036

Counsel to T-Mobile USA, Inc.

Approved:

Dave Yost, Attorney General, State of Ohio

By: */s/ Melissa S. Smith* Date: 11/07/2022

Melissa S. Smith
Assistant Section Chief
Ohio Attorney General's Office, Consumer Protection Section
30 E. Broad Street, Floor 14
Columbus, OH 43215
614.466.6112
Melissa.S.Smith@OhioAGO.gov

Michael S. Ziegler
Principal Assistant Attorney General
Ohio Attorney General's Office, Consumer Protection Section
30 E. Broad Street, Floor 14
Columbus, OH 43215
614.466.3980
Michael.Ziegler@OhioAGO.gov

Appendix A

STATE	CONSUMER PROTECTION ACTS
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.*
Delaware	Consumer Fraud Act, 6 Del. C. §§ 2511 *et seq*
District of Columbia	Consumer Protection Procedures Act, D.C. Code §§ 28-3901 *et seq.*
Florida	Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes
Georgia	Georgia Fair Business Practices Act, O.C.G.A. §§ 10-1-390 through 408
Hawaii	Uniform Deceptive Trade Practice Act, Haw. Rev. Stat. Chpt. 481A and Haw. Rev. Stat. Sect. 480-2
Idaho	Idaho Consumer Protection Act, Idaho Code §§ 48-601 *et seq.*
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 *et seq.*
Iowa	Iowa Consumer Fraud Act, Iowa Code § 714.16
Kansas	Kansas Consumer Protection Act, K.S.A §§ 50-623 *et seq.*
Kentucky	Kentucky Consumer Protection Act, KRS §§ 367.110-.300, 367.990
Louisiana	Unfair Trade Practices and Consumer Protection Law, La. R.S. §§ 51:1401 *et seq.*
Maine	Maine Unfair Trade Practices Act, 5 M.R.S.A. §§ 205-A *et seq.*
Maryland	Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101 *et seq.* (2013 Repl. Vol and 2021 Supp.)
Massachusetts	Mass. Gen. Laws ch. 93A
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
Mississippi	Miss. Code Ann. § 75-24-1 *et seq.*
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.*

Appendix A

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 Hampshire	NH RSA 358-A
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 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.*
Oklahoma	Oklahoma Consumer Protection Act, 15 O.S. §§ 751 *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.*
Rhode Island	Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws §§ 6-13.1-1 *et seq.*
Tennessee	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 to -134
Texas	Texas Deceptive Trade Practices – Consumer Protection Act, Tex. Bus. & Com. Code Ann.§§ 17.41 – 17.63
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
Wisconsin	Fraudulent Representations. Wis. Stat. § 100.18(1)

Appendix B

STATE	PERSONAL INFORMATION PROTECTION ACTS & SECURITY BREACH NOTIFICATION ACTS
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
Delaware	Delaware Data Breach Notification Law, 6 Del. C. § 12B-100 *et seq.*
District of Columbia	District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851 *et seq.*
Florida	Florida Information Protection Act, Section 501.171, Florida Statutes
Georgia	Georgia Personal Identity Protection Act, O.C.G.A §§ 10-1-910 through 915
Hawaii	Security Breach of Personal Information, Haw. Rev. Stat. Chpt. 487N; Personal Information Protection, Haw. Rev. Stat. Chpt. 487J
Idaho	Identity Theft, Idaho Code §§ 28-51-104 *et seq.*
Illinois	Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.*
Indiana	Disclosure of Security Breach Act, Indiana Code §§ 24-4.9 *et seq.*
Iowa	Personal Information Security Breach Protection Act, Iowa Code § 715C
Kansas	The Wayne Owen Act, K.S.A. § 50-6,139b; Security Breach Notification Act, K.S.A. §§ 50-7a01 *et seq.*
Kentucky	KRS 365.732
Louisiana	Database Security Breach Notification Law, La. R.S. §§ 51:3071 *et seq.*
Maine	Maine Notice of Risk to Personal Data Act, 10 M.R.S.A. §§ 1346 *et seq.*
Maryland	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501 *et seq.* (2013 Repl. Vol and 2021 Supp.)
Massachusetts	Mass. Gen. Laws ch. 93H; 201 Code Mass. Regs. 17.00 *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
Mississippi	Miss. Code Ann. § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500

Appendix B

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 *et seq.*
New Hampshire	NH RSA 359-C: 19-21
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 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.*
Oklahoma	Security Breach Notification Act, 24 O.S. §§ 161 *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.*
Rhode Island	Rhode Island Identity Theft Protection Act, R.I. Gen. Laws §§ 11-49.3-1 *et seq.*
Tennessee	Tennessee Identity Theft Deterrence Act of 1999, Tenn. Code Ann. §§ 47-18-2101 to -2111
Texas	Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. § 521.001 – 152
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
Wisconsin	Notice of Unauthorized Acquisition of Personal Information. Wis. Stat. § 134.98