

EXHIBIT H

T-Mobile's Response to Cal PA DRs 1-123 and 2-15

Data Request 1-123 (9/14/18).

Please provide a detailed list of all mergers and acquisitions to which You were a party to in California from 1990 to 2017.

Response to Data Request 1-123 (10/10/18).

T-Mobile objects to this Data Request on the ground it is overbroad in temporal scope; T-Mobile did not begin to provide wireless services in California until 2002. T-Mobile also objects to this Data Request on the grounds that this information is equally available to the Cal PA.

Subject to and without waiving its objections, T-Mobile responds that it was a party to the proposed 2011 transaction with AT&T which was not consummated. T-Mobile further responds that it was a party to the 2013 transaction with MetroPCS, which has been successful by any measure, as discussed at length in the PIS. MetroPCS customers were migrated to the T-Mobile network even more quickly than anticipated, merger synergies exceeded expectations, spectrum refarming was expedited, and MetroPCS customers enjoyed expanded coverage and better service. Indeed, MetroPCS's customer base has doubled since the merger and the number of employees has also increased substantially. See PIS at pp. 39-41, 82.

Data Request 2-15 (10/23/18).

How many Sprint customers in California currently use devices that are not compatible with T-Mobile's wireless network in California?

Response to Data Request 2-15 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrase "compatible." T-Mobile further objects to this Data Request on the grounds it is more appropriately directed to Sprint as this information is not in the direct custody, care or control of T-Mobile.

Subject to and without waiving its objections, T-Mobile responds that it does not have numbers for devices subscribed to the Sprint wireless network that are compatible with the T-Mobile network in California or nationwide. T-Mobile further responds that the Reply Declaration of John Saw, Chief Technology Officer, Sprint, filed with the Joint Opposition at the FCC states that the total number of Sprint devices nationwide across all brands and channels (including postpaid, prepaid, and wholesale) that are capable of accessing at least one T-Mobile LTE spectrum band while also supporting voice features on at least one of Sprint's or T-Mobile's voice networks (to the extent a device has voice functionality) is over 37 million. Sprint also expects the number of devices compatible with T-Mobile's network to grow over time as customers upgrade their older devices to newer, compatible ones.

CONFIDENTIAL EXHIBIT I

Migration Overview Presentation to the DOJ

ENTIRE DOCUMENT FILED UNDER SEAL

PUBLIC EXHIBIT J

T-Mobile's Responses to Cal PA DRs 4-22, 4-24 to 4-27, and 7-3 to 7-25

(without document production)

Data Request 4-22 (11/14/18).

Please provide a list of the applications loaded onto T-Mobile mobile phones between January 1, 2015 and September 30, 2018, for all devices and manufacturers. For each application:

- a. Please include the name of the application's developer; the name(s) of the devices (e.g. Android smartphone) and device manufacturers (e.g. Samsung or iPhone) on which the application comes pre-installed; and whether the developer continues to update the app or if it has been deprecated.*
- b. Please describe the process manufacturers or developers must go through in order to request and receive permission to have their application pre-installed on T-Mobile mobile devices. Please include copies of any forms, contracts, or other documents that manufacturers or developers must submit or agree to in order to request and receive permission to install their applications on T-Mobile mobile devices.*
- c. Please also describe what criteria, methods, or process T-Mobile uses when reviewing these applications in order to determine whether the request will be approved or denied.*
- d. Please describe what other processes, if any, T-Mobile has to ensure pre-installed apps do not pose any threat to T-Mobile customers. Please describe how pre-installed applications receive permission to collect or access specific components of, contents of, or data generated by customer phones (i.e., data or information stored in or collected by body sensors, calendars, camera, contacts, location, microphone, phone, sms, and storage). That is, do pre-installed applications receive permission to access customer data and information by default or as part of the terms and conditions of a customer's use, or do pre-installed applications receive permission only after a customer opens or uses the application?*

Response to Data Request 4-22 (12/3/18).

T-Mobile objects to this Data Request on the grounds it is overbroad in temporal scope, unduly burdensome as well as vague and ambiguous with respect to the phrase "loaded." T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the process used for pre-installing apps on wireless devices has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile further objects to this Data Request on the grounds it is duplicative of Cal PA DRs 1-110 and 1-111 and the Meet and Confer correspondence from Cal PA dated November 9, 2018.

Subject to and without waiving its objections, T-Mobile responds that, as noted in its earlier responses, the applications preloaded on a given device vary depending on manufacturer and model. See Responses and Supplemental Responses to DRs 1-110 and 1-111. T-Mobile provides consumers with information as to which consumer-facing apps are pre-installed on a

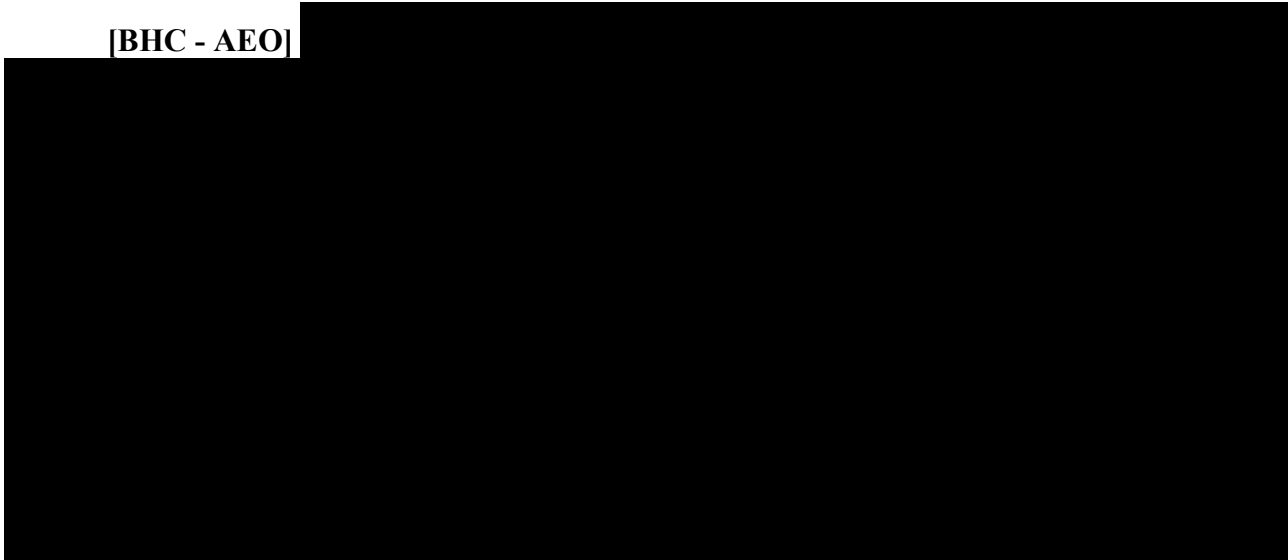
given device on our support pages. See Cal PA DR 004 Production Folder. By “pre-installation,” T-Mobile refers to situations where software is placed on devices before a user purchases the device.

With respect to any given device that T-Mobile sells, there are distinct stakeholders that dictate whether certain applications will be pre-installed on the device. Specifically, decisions about whether to pre-install apps can be made by the individual Original Equipment Manufacturer (“OEM”) that manufactures the device, the provider of the Operating System (“OS”) on which the device operates, and T-Mobile.

These three entities play different roles for different devices. For Apple devices, the device and the OS are produced by the same party, and Apple generally has sole control over what applications are pre-installed on those devices. Other OEMs may license an official version of the Android OS software from Google. Still others may create their own OS, which, in some cases, is a version of Android that uses open-source code. Generally, in cases where the OEM and the OS provider are not the same party, the agreement between the OEM and OS determines which party can make decisions about which consumer-facing apps are pre-installed.

Any OEM or OS provider associated with a particular device may, and often do, determine that certain applications come pre-installed. These applications may be developed by either the OEM, OS provider, or by third parties, with which the OEM or OS provider contracts. In general, the OEMs and OS providers require that certain applications come pre-installed in order to meet two goals: (1) to provide a consistent customer experience across carriers; and (2) to ensure that downstream applications that customers elect to install after purchase will be compatible with the OS and operate correctly on the device.

[BHC - AEO]



¹ See, e.g. <https://support.t-mobile.com/community/phones-tablets-devices/software-updates>; <https://support.t-mobile.com/thread/148905>

² T-Mobile’s network also includes free services that help block unwanted scam calls to consumers. <https://www.t-mobile.com/news/t-mobile-fights-scam-calls>.

REDACTED

REDACTED

[EHC - AEO] However, as noted above, T-Mobile does provide consumers with information about third-party apps and services available for use with devices and our network services at: <https://www.tmobile.com/responsibility/privacy/resources/device-apps>.

Supplemental Response to DR 4-22 re TRS 610 (12/21/18)

Subject to and without waiving its objections, T-Mobile responds to Cal PA's December 6, 2018 email request for additional documentation regarding T-Mobile form TRS 610 which was produced as part of the initial response to DR 4-22. In particular, Cal PA requested the following documents cross-referenced in TRS 610:

1. Enterprise Third Party (Supplier) Risk Assessment (ESRA) screening form
2. T-Mobile's Supplier Risk Management (SRM) questionnaire

Consistent with T-Mobile's communications with Cal PA on December 14, 2018 and December 17, 2018, T-Mobile notes that the TRS 610 has recently been updated (as of the first week of December) and a copy of the updated document is produced with this Supplemental Response. Also included is a copy of T-Mobile's new Cyber Assessment Questionnaire for vendors and suppliers that went into production in early October and entirely replaced the SRM Questionnaire, which was retired in November. See Supplemental Response Folder, documents beginning with Bates No. TMUS-CPUC-PA-00005629. In addition, T-Mobile is providing a copy of the legacy SRM Questionnaire referenced above. See Supplemental Response Folder, documents beginning with Bates No. TMUS-CPUC-PA-00005642. The ESRA Screening Form mentioned in the version of TRS-610 previously produced refers to the SRM Questionnaire, which was both the intake screening form and the cyber questionnaire under the legacy program.

Supplemental Response to DR 4-22 re TISS 310 (12/21/18)

On December 5, 2018, Cal PA sent an email request for additional documents listed in Section 8 of TISS 310 that was other produced as in the initial response to DR 4-22. Those six documents are identified below:

1. TISD-1000 Information Handling Procedure
2. TLP-200 Records Management Policy
3. TLS-210 Records Retention Schedule Standard
4. TLP-500 Customer Location Information Policy
5. Non T-Mobile Worker (NTW) Classification list
6. THRP-102 Non T-Mobile Worker (NTW) Policy

Subject and without waiving its objections above, T-Mobile further objects to the email request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the various internal policy and procedure documents have no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request on the grounds that the documents requested are not responsive to the Data Request regarding preloaded apps; as explained to Cal PA, T-Mobile often cross references documents for ease of internal reference. The requested documents address the various unrelated matters described in their titles such as documentation retention policies.

Notwithstanding any of these objections, and as a courtesy to Cal PA, T-Mobile has provided a copy of the requested documents. See Supplemental Response Folder, documents beginning with Bates No. TMUS-CPUC-PA-00005601.

Data Request 4-24 (11/14/18).

In response to Data Request no.001 Question 102, T-Mobile stated:

Response: *“Subject to and without waiving its objections, T-Mobile responds that T-Mobile does not seek nor collect any information to identify which devices are used by children, or which devices are used by adults on a given account. Also, T-Mobile does not seek, collect, or develop information necessary to determine a parental relationship between users on an account. Where options for data collection exist, those choices are for the primary account holder or, in some cases, individual users, to determine at their discretion.”*

The T-Mobile FamilyMode App allows “parents to monitor their family's internet on the T-Mobile cellular network and any Wi-Fi connection.”³ The app uses filters to control access to content on each device. According to your website, the default filters are as follows:

- *“High - Works for kids 6-12 years old. General platforms like education and kid-safe experiences are available by default while filtering out sites designed for older age groups, like social media.*
- *Medium - Crafted for teens 13-17 years old. Most platforms, categories, and apps are available while limiting access to many popular apps or sites that are 18+. Inappropriate categories are filtered and invisible by default.*
- *Low - Appropriate for ages 18 years old and up. Access to nearly all platforms, categories, and apps is available, though explicit and mature content is filtered out by default.*
- *None - Designed for profiles that you want FamilyMode to ignore, or just be able to Pause, and set BedTimes/OffTimes for. NOTE: Features such as Filtering, Time Limits, and Usage are not available for profiles set to None.”*

In addition to controlling access to platforms, apps, and categories of websites, do any of these filters control what advertisements T-Mobile shows (or allows to be shown) to the user? Do any of these filters alter how or how much data are collected from the device?

Response to Data Request 4-24 (12/3/18).

T-Mobile objects to this Data Request on the grounds set forth in its Response to Cal PA DR 1-102 and on the grounds it is vague and ambiguous with respect to the phrases “advertisements T-Mobile shows,” “alter,” and “data collected from the device.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither germane to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the type of advertisements that may

³ <https://support.t-mobile.com/docs/DOC-37524#app7>

appear on any given app has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that it does not control what advertisements are shown on a given third-party website or application. T-Mobile applications, such as the T-Mobile app and T-Mobile Tuesdays, do not show third-party ads (but do show T-Mobile specific offers for customers).

T-Mobile's parental control tools, known as FamilyMode, do control what advertisements are shown when users configure it to do so. That is, the FamilyMode app has a setting for "ad blocking" that filters out many sources of online ads, including from websites consumers visit;

The FamilyMode content filters do not alter what data is collected from the device except to the extent that if the filter blocks access to a given website. If a website is blocked, data that website would otherwise collect from the device is not collected.

T-Mobile does not have actual knowledge as to the ages of individuals to whom a FamilyMode user has applied any filtering.

Data Request 4-25 (11/14/18).

In the past few years, T-Mobile has experienced a number of data breaches affecting millions of customer records.^{4 5 6}

- a. Please describe, in detail, the specific steps T-Mobile has taken in response to these breaches to ensure customer data are secure and to prevent future breaches.*
- b. Please describe what specific plans, if any, T-Mobile has in place to ensure the security of existing T-Mobile and Sprint customer's data during the merger process and also after the merger is complete.*

Response to Data Request 4-25 (12/3/18).

- (a) T-Mobile responds that after the August 2018 and subsequent incidents, T-Mobile strengthened its protections to detect suspicious login attempts and “credential stuffing,” a technique whereby attackers test large sets of credentials to find pairs that match legitimate credentials. This attack exploited a vulnerability in an Application Program Interface (“API”); as a result, T-Mobile undertook a comprehensive review of APIs used in T-Mobile operations, to ensure proper authentication security for those APIs. T-Mobile also flagged impacted accounts for additional monitoring to detect suspicious activity. T-Mobile is also investing in further security controls for detecting and containing malicious traffic.

In the October 2017 incident, T-Mobile was able to resolve the vulnerability within 24 hours. T-Mobile was notified of the vulnerability by a security researcher. T-Mobile encourages researchers and others with security vulnerability information to follow a process of responsible coordinated disclosure and continues to respond promptly to such notifications. T-Mobile and its third-party forensic analyst confirmed no CPNI, financial data, SSN or payment card data was accessed, and T-Mobile had already alerted the limited set of customers, who could have been impacted.

As for the 2015 Experian data breach, T-Mobile clarifies that the incident occurred on Experian's systems. Experian, with oversight and input from T-Mobile, subsequently enhanced its security by improving its intrusion prevention system, changing account passwords on database servers, strengthening its network firewall rules, and increasing the complexity of its encryption key. In addition, Experian confirmed that it was properly segmenting its network, and performing logging and monitoring.

- (b) Regarding information security during the merger process, T-Mobile and Sprint remain independent operators during the pendency of the transaction. T-Mobile will maintain and continue to improve its information security program during that time. This program includes physical, technical, and administrative safeguards, tailored to the nature and uses

⁴ <https://www.theverge.com/2018/8/24/17776836/tmobile-hack-data-breach-personal-information-two-million-customers>

⁵ https://motherboard.vice.com/en_us/article/a37epb/t-mobile-alert-victims-sim-card-hack

⁶ <http://money.cnn.com/2015/10/01/technology/tmobile-experian-data-breach/index.html>

of information. Details on certain aspects of T-Mobile information security are included in its annual FCC certification statement, which is available online.⁷ After the merger is complete, New T-Mobile will work quickly to integrate the T-Mobile and Sprint security controls for the systems and data involved.

⁷ <https://ecfsapi.fcc.gov/file/10301273577183/2017%20T-Mobile%20CPNI%20Certification%20and%20Statement.pdf>

Data Request 4-26 (11/14/18).

T-Mobile's Privacy Policy states: "Where we allow third parties the capability of accessing data about your location that is derived from our network, we require those third parties to observe specific privacy and security protections consistent with this statement."

- *Please provide a copy of the third party contracts, agreements, or other documents that describe what specific data use, privacy, and security protections or practices you require when providing third parties access to customer data.*
- *Please describe how T-Mobile assesses, manages, and monitors risks posed by third party access to customer data.*

Response to Data Request 4-26 (12/3/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases "assess," "manages," "monitors," and "risks posed." T-Mobile further objects to this Data Request to the extent it is duplicative of DR 1-109. T-Mobile further objects to this Data Request on the grounds it seeks information which is neither germane to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile's specific requirements for third parties with the capability of accessing location data has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile further objects to this Data Request on the grounds the disclosure of such information could constitute a breach of its supplier contracts.

Subject to and without waiving its objections, T-Mobile further responds that its current privacy policies, practices, and disclosures fully comply with our obligations under all applicable federal and state laws. T-Mobile further responds that it maintains a supplier data security and risk management standard, which is a policy applicable to suppliers handling T-Mobile Customer Information. See <https://www.t-mobile.com/our-story/working-together/suppliers/supplier-code-of-conduct> for that enterprise risk management standard, along with T-Mobile's supplier code of conduct.

T-Mobile further responds that it observes privacy standards and complies with applicable laws that require certain contractual safeguards for supplier processing of personal information (as defined in those applicable laws). It is T-Mobile's standard practice to use its contract forms and templates. Where suppliers require use of their own contract forms, T-Mobile compares the supplier's contract form to its own to ensure appropriate clauses and concepts are addressed sufficiently, including with respect to data security. For relationships with suppliers where the supplier will have access to T-Mobile's confidential information, including customer information, and that use T-Mobile's contract forms, T-Mobile uses a data security template that sets forth the supplier's obligations to maintain the security of that information. This template is typically included as "Exhibit B" to a master services agreement with that supplier. See Cal PA DR 004 Production Folder. The Exhibit B template is tailored to the individual needs of the supplier relationship during the context of negotiations. For example, for suppliers that provide

cloud computing services or software development, T-Mobile may include additional data security terms. Similarly, if a supplier does not process payments, certain terms governing the processing of payment card data may be omitted if they do not apply. The terms in the Exhibit B template work in tandem with the supplier security policy noted above.

Additionally, T-Mobile Third Party Risk Management (“TPRM”) processes utilize an objective framework to rank the findings and risk information gleaned from third-party due diligence reviews and assessments. Risk information is escalated, where warranted, for evaluation and decision as to whether to approve, reject, or condition a supplier engagement.

Data Request 4-27 (11/14/18).

T-Mobile's Privacy Policy states: "We may provide information that does not identify you personally to third-parties for marketing, advertising or other purposes."

- *Please describe your specific process for de-identifying customer data. If the process differs depending on the data type or category, please explain the process for each.*

Response to Data Request 4-27 (12/3/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases "process for de-identifying," "data type," and "category." T-Mobile further objects to this Data Request on the grounds it seeks information which is neither germane to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the various processes used for de-identification or anonymization of data has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile further objects to this Data Request on the grounds it is unduly burdensome and disclosure of the requested information could compromise T-Mobile's cybersecurity measures and ability to protect its customers' data. T-Mobile also objects to this Data Request to the extent that it is duplicative of Cal PA DR 1-99.

Subject to and without waiving its objections, T-Mobile responds that T-Mobile uses reasonable commercial methods for de-identification appropriate to the nature of the data at issue. One example is hashing, where an algorithm is applied to convert identifiable text into strings of digits (which cannot then be re-converted to identifiable text).

The de-identification method differs for different types of data. For example, where de-identified data is provided to service providers who perform marketing analytics on behalf of T-Mobile, hash algorithms are used typically to de-identify information. This permits T-Mobile to pass user information to a third party without exposing personal information and also without compromising data integrity (knowing that a data element and its value have not been modified). The third-party service provider does not require identifiable data in order to perform analytics. In another example, T-Mobile uses truncation to de-identify credit card information on payment receipts in a retail context, just as many other retail providers do. In this instance, the truncation of the payment card account number provides enough de-identification to prevent theft while still allowing the customer to recognize the payment method.

For a general description of de-identification techniques used by industry, see Future of Privacy Forum, "A Visual Guide to Practical Data De-Identification," online at: <https://fpf.org/issues/deid/>.

T-Mobile further responds that T-Mobile's current privacy policies, practices, and disclosures fully comply with our obligations under all applicable federal and state laws. See <https://www.t-mobile.com/responsibility/privacy/privacy-choice/tmo-insights>. See also Response to Cal PA DR 1-99.

Data Request 7-3 (12/21/18).

Does T-Mobile specify what information suppliers must provide to T-Mobile in the event of a data breach involving T-Mobile's, or T-Mobile customers', confidential information? Please provide examples of the notifications T-Mobile receives from suppliers when suppliers experience a breach involving T-Mobile's, or T-Mobile customers', confidential information.

Response to Data Request 7-3 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases "suppliers," "must provide," "data breach," "T-Mobile's, or T-Mobile customers' confidential information" and "notifications." T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, information received by T-Mobile in the case of a potential data breach has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent it is duplicative of Cal PA DRs 4-25 and 4-26.

Subject to and without waiving its objections, T-Mobile responds that, as described in its response to Cal PA DR 4-26, for relationships with suppliers where the supplier will have access to T-Mobile's confidential information, including customer information, and that use T-Mobile's contract forms, a data security template sets forth the supplier's obligations to maintain the security of that information. This template is typically included as "Exhibit B" to a master services agreement with that supplier. This template was previously produced in T-Mobile's Response to Cal PA Data Request 004; see document beginning with Bates No. TMUS-CPUC-PA-13000073 ("Exhibit B").

Section 3.2 of Exhibit B requires that [BHC – AEO]

REDACTED

AEO]

[EHC –

Data Request 7-4 (12/21/18).

Are suppliers required to notify T-Mobile when a subcontractor experiences a data breach?

Response to Data Request 7-4 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “suppliers,” “subcontractor,” and “experiences a data breach.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, information received by T-Mobile in the case of a potential data breach has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent it is duplicative of Cal PA DRs 4-25 and 4-26.

Subject to and without waiving its objections, T-Mobile responds that it requires that a supplier may only use a subcontractor with T-Mobile’s written consent and that the supplier remain fully responsible for the performance of all of the supplier’s obligations under its agreement with T-Mobile, including the requirement to provide notice of security breaches as discussed in response to DR 7-3 above.

Data Request 7-5 (12/21/18).

Does the Enterprise Third Party (Supplier) Risk Assessment (ESRA) screening occur before, during, or after T-Mobile approves a contract with a new supplier?

Response to Data Request 7-5 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “Third Party (Supplier) Risk Assessment (ESRA) screening” and “new supplier.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent it is duplicative of Cal PA DR 4-22.

Subject to and without waiving its objections, T-Mobile responds that the ESRA is no longer in use. Under the current practice, suppliers are required to complete a Cyber Assessment Questionnaire if the supplier will have any access to confidential or restricted T-Mobile customer data. T-Mobile conducts supplier screening prior to a new contractual engagement with a new or existing supplier. Additional screening also occurs after engagement as needed. See also Response to Cal PA DRs 7-12 and 7-13 below; see also Supplemental Response to Cal PA DR 4-22.

Data Request 7-6 (12/21/18).

What information does the ESRA screening form assess?

Response to Data Request 7-6 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “information” and “ESRA screening form.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to the Data Request to the extent it is duplicative of information provided in its Supplemental Response to Cal PA DR 4-22.

Subject to and without waiving its objections, T-Mobile responds the ESRA is no longer in use. As noted above, under the current practice, suppliers are required to complete a Cyber Assessment Questionnaire if the supplier will have any access to confidential or restricted T-Mobile customer data. The information requested by the Cyber Assessment Questionnaire is contained in the forms themselves. See Bates no. TMUS-CPUC-PA-00005641 previously produced in T-Mobile’s Supplemental Response to Cal PA DR 4-22.

Data Request 7-7 (12/21/18).

Who is responsible for filling out the form initially?

Response to Data Request 7-7 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “responsible” and “the form.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to the Data Request to the extent it is duplicative of information provided in its Supplemental Response to Cal PA DR 4-22.

Subject to and without waiving its objections, T-Mobile responds that it is the responsibility of the supplier to complete the Cyber Assessment Questionnaire.

Data Request 7-8 (12/21/18).

Who is responsible for reviewing the form and making decisions regarding T-Mobile's relationship with that supplier?

Response to Data Request 7-8 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases “responsible for reviewing the form,” “making decisions” and “relationship.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile's risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to the Data Request to the extent it is duplicative of information previously provided in its Supplemental Response to Cal PA DR 4-22.

Subject to and without waiving its objections, T-Mobile responds that it has a dedicated team within the company⁸ that is responsible for, among other things, reviewing Cyber Assessment Questionnaires and otherwise has the authority to make decisions regarding T-Mobile's relationships with third-party suppliers. See also Response to Response to Cal PA DR 4-22, 7-10, 7-11 and 7-14, and 7-15.

⁸ The team is the Third-Party (Supplier) Risk Management Program (the “TPRM Program”) referenced in the most recent version of TRS-610 produced in its Supplemental Response to Cal PA DR 4-22.

Data Request 7-9 (12/21/18).

TRS-610 Section 3.1.1 specifies that the ESRA may “trigger” a Supplier Risk Management Review (SRMR). Please explain what, specifically, triggers T-Mobile to conduct a SRMR.

Response to Data Request 7-9 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases “ESRA” and “SRMR.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that the ESRA and the version of the TRS-610 referenced in the Data Request are no longer in use as described in T-Mobile’s Supplemental Response to Cal PA DR 4-22. T-Mobile further responds that under the legacy program, the “SRMR” was the cyber assessment that suppliers with access to confidential or restricted T-Mobile data would have been required to complete. Under the current program, suppliers are required to complete a Cyber Assessment (which replaced the SRMR) if certain conditions are present, including if the supplier will have any access to confidential or restricted T-Mobile customer data.

Data Request 7-10 (12/21/18).

Who is responsible for conducting the SRMR?

Response to Data Request 7-10 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases “conducting” and “SRMR.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that the TPRM Program has ultimate oversight and strategic responsibility for the supplier assessment processes, including the Cyber Assessment (formerly known as the SRMR); see Response to Cal PA DR 7-8 above.

Data Request 7-11. (12/21/18)

How is the SRMR used to make decisions regarding third party supplier relationships?

Response to Data Request 7-11 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases “SRMR” and “decisions regarding third party relationships.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that it has developed a comprehensive methodology for evaluating suppliers and engagement risks using a multi-tiered approach that considers the inherent risk of engagement attributes (e.g., network access or access to CPNI), and the residual risk of using a particular supplier on an engagement based on risk scores, entity attributes, and completed assessments. T-Mobile prescribes risk assessments based on inherent risk and evaluates residual risk both at an assessment level (e.g., financial, compliance, cyber) and in the aggregate across all risk domains evaluated. By assessing risk both horizontally and vertically, T-Mobile obtains a more complete picture of a supplier’s ability to successfully perform the engagement and protect T-Mobile information. For example, a supplier who scores lower risk levels on each of the individual risk assessments may, when viewed in the aggregate, trigger the need for further analysis. The evaluation process takes into account numerous risk issues and factors that the TPRM Program is specifically trained to analyze, flag, and escalate.

Data Request 7-12 (12/21/18).

After establishing a relationship with a supplier, does T-Mobile conduct subsequent or periodic screenings or reviews of supplier security practices and procedures?

Response to Data Request 7-12 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “establishing a relationship” and “supplier security practices and procedures.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that it periodically re-reviews suppliers throughout the course of the engagement on a cadence that depends on any issues or concerns that were identified in the initial review of the Cyber Assessment, and/or in response to intervening events such as a reported breach or other incident where the TPRM Program may determine that an additional review is necessary.

Data Request 7-13 (12/21/18).

If so, are screenings or reviews conducted regularly or only when triggered? If screenings or reviews are conducted regularly, please indicate their frequency. If screenings or reviews are conducted only when triggered, please describe what conditions would trigger a review.

Response to Data Request 7-13 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases “screenings or review” and “triggered.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that new Cyber Assessments are performed regularly (e.g., on three-year, 18-month, 12-month or 6-month cycles) for all suppliers depending on their initial Cyber Assessment. New Cyber Assessments may also be required of a supplier in various circumstances including in response to a reported event, change in control, or for some other issue or concern that may come to T-Mobile’s attention. See also Response to Cal PA DR 7-12 above.

Data Request 7-14 (12/21/18).

Who is responsible for conducting subsequent or periodic screenings or reviews and implementing any decisions or action items that might result?

Response to Data Request 7-14 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases “conducting subsequent screenings or reviews” and “implementing any decisions or action items.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent it is duplicative of Cal PA DR 7-10.

Subject to and without waiving its objections, T-Mobile responds that the TPRM Program has the ultimate responsibility for conducting subsequent or periodic screenings or reviews and implementing any decisions or action items that might result. See also Response to Cal PA DR 7-10 above.

Data Request 7-15 (12/21/18).

In response to Public Advocates Office Data Request (DR) 004, Question 26 T-Mobile stated that, "Risk information is escalated, where warranted, for evaluation and decision as to whether to approve, reject, or condition a supplier engagement." Please describe the process for escalating risk information: Who escalates the risk and to whom? Who decides whether to approve, reject, or condition a supplier engagement? What circumstances would warrant escalation of risk information?

Response to Data Request 7-15 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope. T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile's risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent it is duplicative of Cal PA DR 7-8.

Subject to and without waiving its objections, T-Mobile responds that the TPRM Program has the authority to reject, condition, or recommend termination of onboarding activities for prospective third-parties for risk-based issues. See also Response to Cal PA DR 7-8 above.

Data Request 7-16 (12/21/18).

Does T-Mobile have an inventory of all suppliers that have access to T-Mobile customer information?

Response to Data Request 7-16 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “inventory” and “access to T-Mobile customer information.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s supplier tracking practices have no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that it categorizes a supplier’s data elements and access types as part of the initial due diligence process, including whether a supplier will have access to customer information. T-Mobile has not historically maintained an inventory of all suppliers that have access to T-Mobile customer information but is currently preparing to implement the requirements of the California Consumer Privacy Act (“CCPA”), including those related to “Service Providers.”

Data Request 7-17 (12/21/18).

Does T-Mobile have an inventory of all subcontractors that have access to T-Mobile customer information?

Response to Data Request 7-17 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “inventory” and “access to T-Mobile customer information.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s supplier tracking practices have no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that it requires that a supplier may only use a subcontractor with T-Mobile’s written consent and the supplier must remain fully responsible for the performance of all of the supplier’s obligations under its agreement with T-Mobile, including the requirements concerning customer information. T-Mobile further responds that T-Mobile has not historically maintained an inventory of all suppliers that have access to T-Mobile customer information but is currently preparing to implement the requirements of the CCPA, including those related to “Service Providers.”

Data Request 7-18 (12/21/18).

[BHC – AEO]

Response to Data Request 7-18 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrase “outcome of these reviews.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s contractual relationships with its suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent it is duplicative of information provided in its Response to Cal PA DR 4-26.

Subject to and without waiving its objections, T-Mobile responds that Section 2.1 of Exhibit B [BHC – AEO]

REDACTED

[EHC – AEO]

Data Request 7-19 (12/21/18).

[BHC – AEO]

[EHC – AEO]

Response to Data Request 7-19 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is overbroad and vague and ambiguous with respect to the phrase “any related documents.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s contractual relationships with its suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent it is duplicative of information provided in its Response to Cal PA DR 4-26.

Subject to and without waiving its objections, T-Mobile responds that it does not instruct suppliers on how to [BHC – AEO]

REDACTED

[EHC – AEO]

Data Request 7-20 (12/21/18).

[BHC – AEO]
REDACTED
[EHC – AEO]

Response to Data Request 7-20 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is overbroad and vague and ambiguous with respect to the phrase “ensures,” “evaluates the results,” “follow up,” and “gaps or deficiencies.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile’s contractual relationships with its suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent it is duplicative of information provided in its Response to Cal PA DR 4-26.

Subject to and without waiving its objections, T-Mobile responds that it relies primarily on its initial and subsequent Cyber Assessments, as well as its comprehensive methodology for evaluating suppliers and engagement risks as established in the TPRM Program, to manage, evaluate and address potential risk issues associated with its suppliers on an ongoing basis. See also T-Mobile’s Response to Cal PA DRs 7-11 to 7-13; see also Responses to Cal PA DRs 7-5 to 7-10 and 7-15.

Data Request 7-21 (12/21/18).

T-Mobile's 2018 Proxy Statement website (<https://explore.t-mobile.com/2018-proxy-statement/board-and-governance/risk-management>) describes the Board of Director's role in Risk Management. Does the Board of Directors play a role in managing third party supplier and subcontractor risk? If so, please describe that role.

Response to Data Request 7-21 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is overbroad and vague and ambiguous with respect to the phrases “play a role” and “third party supplier and subcontractor risk.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the activities of T-Mobile's Board of Directors and T-Mobile's risk management processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that, as provided in the 2018 proxy statement, “[w]hile the full Board has overall responsibility for risk oversight, the Board has delegated risk oversight responsibility for certain risks to committees of the Board,” including the Audit Committee, the Compensation Committee, the Executive Committee, and the Nominating and Corporate Governance Committee. “On a regular basis, reports of all committee meetings are presented to the Board and the Board periodically conducts deep dives on key enterprise risks.”

It further provides that “[t]he Audit Committee has primary responsibility for overseeing the Company's various risk assessment and risk management policies. The Audit Committee considers and discusses policies with respect to risk assessment and risk management, including the Company's major financial risk exposures and the steps management has taken to monitor and control such exposures....The Audit Committee reviews all risk assessments, provides feedback to executive management and shares the risk assessments with the Board.”

Data Request 7-22 (12/21/18).

Does the Board of Directors and/or senior managers receive periodic updates from staff regarding supplier risks or T-Mobile's supplier risk management process?

Response to Data Request 7-22 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is overbroad and vague and ambiguous with respect to the phrases "senior managers," "updates," "staff," "regarding supplier risks." T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the activities of T-Mobile's Board of Directors and T-Mobile's risk management processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that senior management, via their participation in the Information Security and Privacy Council and the Enterprise Risk and Compliance Committee, receive periodic updates regarding supplier risks and the TPRM Program; and the Board of Directors and applicable committees, receive periodic updates on significant risks which from time to time could include supplier risks and the matters within the purview of TPRM Program.

Data Request 7-23 (12/21/18).

Does the Board of Directors consider third party risk management to be a company-wide priority? If so, please provide copies of any relevant documentation indicating third party risk management is a company-wide priority.

Response to Data Request 7-23 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is overbroad and vague and ambiguous with respect to the phrases “third party risk management,” “company-wide priority” and “any relevant documentation.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the activities of T-Mobile’s Board of Directors and T-Mobile’s risk management processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds by referencing its Responses to Cal PA DRs 7-5 to 7-22 above.

Data Request 7-24 (12/21/18).

Does T-Mobile's Board of Director's "Information Security and Privacy Council" have any role in T-Mobile's Third-Party Supplier Risk Management process? If so, please describe.

Response to Data Request 7-24 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrase "Third-Party Supplier Risk Management process." T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the activities of T-Mobile's Board of Directors and T-Mobile's risk management processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds the Information Security and Privacy Council is not a committee of the Board of Directors. TPRM regularly reports to the Information Security and Privacy Council on those aspects of the TPRM Program that relate to protection of TMO data, information security practices and policies for overseeing third party handling of TMO/customer data.

Data Request 7-25 (12/21/18).

Does T-Mobile have an active, ongoing supplier relationship with the company LocationSmart? If so, please describe that relationship. Please provide a copy of T-Mobile's contract with LocationSmart.

Response to Data Request 7-25 (01/03/19).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrase “active, ongoing supplier relationship.” T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile's contractual relationship with any give third party has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that it has provided LocationSmart with formal notice of termination of the companies' relationship, and all operations with LocationSmart are scheduled to end in March 2019.

EXHIBIT K

T-Mobile's Response to Cal PA DRs 6-1 and 6-2

(without document production)

Data Request 6-1 (12/11/18).

Please provide all economic models and associated data You provided to the Federal Communications Commission as part of Docket 18-197. Please include any data and information explaining the economic models.

Response to Data Request 6-1 (12/17/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “economic models,” “associated data,” and “any data and information explaining the economic models.” T-Mobile also objects to this Data Request to the extent it is duplicative of DRs 1-6, 1-122, and 3-3.

Subject to and without waiving its objections, and pursuant to a telephone conversation with Cal PA representatives on Monday, December 17, 2018, T-Mobile responds that it is providing a copy of the IKK Economic Model (aka the Compass Lexecon Model) and the Cornerstone Economic Study on a specially-prepared laptop computer with the understanding that the data provided will not otherwise be copied or reproduced. In addition, T-Mobile is providing copies of various documents provided to the FCC and/or the DOJ to explain the models. A list of those confidential materials, including those materials already provided to Cal PA in response to previous data requests, is provided below:

Date	Document Description	Bates Nos.
	Compass Lexecon/IKK Economic Model	Provided on Laptop
9/17/2018	Joint Opposition - FCC	TMUS-CPUC-PA-00001090 (Previously produced in response to DRs 1-6 and 1-122, 10/10/18)
9/17/2018	Joint Opposition - FCC, Appendix F, Compass Lexecon Declaration	TMUS-CPUC-PA-00001225 (Previously produced in response to DRs 1-6 and 1-122, 10/10/18)
10/30/2018	IKK Presentation to DOJ	TMUS-CPUC-PA-00004881
11/2/2018	Ex Parte (presentation to FCC re Compass Lexecon model)	TMUS-CPUC-PA-11008040 (Previously produced in response to DR 3-3, 11/5/18)
11/15/2018	Ex Parte (follow up discussion with FCC re Compass Lexecon model)	TMUS-CPUC-PA-00004936
12/14/2018	Ex Parte (additional information for FCC from Israel, Katz, and Keating)	TMUS-CPUC-PA-00004939
	Cornerstone Economic Model	Provided on Laptop
11/6/2018	Cornerstone Report (Supplement to FCC Information Request)	TMUS-CPUC-PA-00004950
12/4/2018	Cornerstone Presentation to DOJ	TMUS-CPUC-PA-00005096

12/6/2018	Ex Parte (presentation to FCC re Cornerstone Economic Model)	TMUS-CPUC-PA-00005298
-----------	---	-----------------------

Data Request 6-2 (12/11/18).

Please provide all economic models and associated data You provided to the U.S. Department of Justice as part of its review of Your proposed acquisition of Sprint Corporation. Please include any data and information explaining the economic models.

Response to Data Request 6-2 (12/17/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “economic models,” “associated data,” and “any data and information explaining the economic models.”

Subject to and without waiving its objections, T-Mobile references its Response to DR 6-1 above.

PUBLIC EXHIBIT L

T-Mobile's Responses to Cal PA DRs 1-20, 1-55, 2-7, 2-18 to 2-24, 5-10, and 5-12 to 5-15

(without document production)

Data Request 1-20 (9/14/18).

Please identify any and all wholesale services You currently provide to third parties in California, including:

- a. Name of product/service*
- b. Description*
- c. Speeds, where applicable*
- d. Price*
- e. Number of subscribers per product/service*

Response to Data Request 1-20 (10/10/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrase “wholesale services.” T-Mobile also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information. T-Mobile also objects to this Data Request to the extent that it is duplicative of information sought in DR 1-2.

Subject to and without waiving its objections, T-Mobile responds that T-Mobile provides mobile wireless services to Mobile Virtual Network Operators (“MVNOs”), M2M/IoT solution provider partners, and resellers by offering access to T-Mobile’s network at wholesale rates (*i.e.*, wholesale services). These services are provided on a nationwide basis and not exclusively in California. T-Mobile also works directly with M2M/IoT solution providers to connect the solution provider’s IoT services to the T-Mobile network (*e.g.*, GPS fleet tracking).

T-Mobile further responds it does not track the per unit prices that it charges MVNOs or its M2M/IoT partners for each of their subscribers’ usage. These prices are defined by contracts with complex pricing structures and, in the ordinary course of business, they have not been reduced to per unit figures.

Similarly, T-Mobile does not track the speed it offers its wholesale customers, as these speeds are also dependent on complex contract structures.

T-Mobile provides the number of subscribers or connections of its wholesale customers based on data it collects from its network. These data include separate M2M/IoT connections from MVNO subscribers and Mobile Virtual Network Aggregator (“MVNA”) subscribers. These data are provided as the end of month number of subscribers in June 2018. See Confidential PA Production Folder.

Supplemental Response to Data Request 1-20 (12/3/18).

With respect to DR 1-20, the California Public Advocates Office’s Meet and Confer Letter dated November 9, 2018, provided as follows:

Please provide the total number of wholesale MVNOs, wholesale MVNAs, and wholesale M2M/IOT customers you serve directly.

Also, please clarify whether the retail subscribers of MetroPCS are included in your “tot_eom_subs” counts, as shown in “DR_1-20.xlsx.”

Subject to and without waiving its objections, and in response to the Meet and Confer letter and the follow up telephone conference with representatives of Cal PA on November 14, 2018, T-Mobile further responds that this information was previously provided with respect to MVNOs and MVNAs in response to DRs 2-19 and 2-20, noting that T-Mobile serves 13 MVNOs and MVNAs. As noted in those Responses, T-Mobile does not have a direct relationship with MVNOs’ end-user customers and therefore cannot determine whether they reside within California. The information provided in Response to DR 2-21 reflected the number of unique devices that belong to MVNO customers’ end users that were identified on the network in California at least one time over a 30-day period; it does not include information on the NPA-NXX of the end user, the residence or billing address of that end user or the identity of the MVNO.

T-Mobile further responds that it serves [BHC-AEO [REDACTED] EHC-AEO] wholesale M2M/IoT customers nationwide.

Retail subscribers of MetroPCS are customers of T-Mobile. They are not included in the subscriber counts (under column labeled “tot_eom_subs”) shown in DR_1-20.xlsx, submitted with the bates number TMUS-CPUC-PA-90001299. This spreadsheet only shows counts of end users for T-Mobile’s wholesalers. MetroPCS is not a wholesale customer of T-Mobile; it is a wholly owned subsidiary. Further, MetroPCS does not have wholesale customers of its own.

Data Request 1-55 (9/14/18).

How do You categorize and define different types of customers (e.g., residential, small or medium sized business, or whatever designation of customers You use) for the following services?

- a. *Broadband*
- b. *Voice over Internet Protocol (VoIP)*
- c. *Voice over Long Term Evolution (VoLTE)*
- d. *Wireless Voice Service*

Response to Data Request 1-55 (10/10/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “categorize” and “define.” The Data Request is unclear how that varies from “Wireless Voice Service.” T-Mobile further objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information as how or whether T-Mobile distinguishes among customers has no reasonable bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request on the grounds it seeks information regarding broadband, which is an exclusively interstate service that is subject to the FCC’s – not the Commission’s – jurisdiction.

Subject to and without waiving its objections, T-Mobile responds that for the sake of its response to the California Public Utilities Commission, it provides its services (including the four services identified) to customers that are divided into four categories: (1) Government, (2) Enterprise, (3) Consumer, and (4) Wholesale. The definitions are as follows:

- **Government.** Sales to federal, state, and local governments. This category includes sales to school districts.
- **Enterprise.** Sales to private enterprises, defined as services to billing accounts with more than 25 subscriber lines or more. Note: Small Businesses with less than 25 Subscriber line are generally treated under the Consumer channel.
- **Consumer.** Sales to a customer for his or her personal use or to a small business for the small business’ use. These customers have no contractual obligation to purchase services or devices from T-Mobile. Consumer is split into two categories:
 - *Consumer Prepaid*, defined as sales to a Consumer customer who pays in advance for his or her service.
 - *Consumer Postpaid*, defined as sales to a Consumer customer who pays for the service at the end of a monthly billing cycle.
- **Wholesale.** Sales to customers who purchase minutes of voice or blocks of data for resale to their own customers, such as Mobile Virtual Network Operators (MVNOs) or sellers of connected devices (Machine-to-Machine (“M2M”) or internet of things (“IoT”).

T-Mobile offers Broadband, VoIP, VoLTE, and Mobile Voice Service to all four of the above categories provided the customer has a device which can use such services.

Data Request 2-7 (10/23/18).

What effect will the merger have on the fees You charge Mobile Virtual Network Operators (MVNOs), Mobile Virtual Network Aggregators (MVNAs) and other customers for wholesale access to Your spectrum?

Response to Data Request 2-7 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “fees You charge” and “wholesale access to Your spectrum.” T-Mobile further objects to this Data Request on the grounds it seeks information that is dependent on decisions which will not and cannot be finalized until the transaction can be consummated. T-Mobile also objects to this Data Request to the extent that it is duplicative of Cal PA DRs 1-20 and 1-122.

Subject to and without waiving its objections, T-Mobile responds that the merger will have a positive impact on wholesale MVNOs and MViNAs (collectively referred to as “MVNOs”) because New T-Mobile will be offering a vastly superior service than either standalone company could provide. T-Mobile further notes that New T-Mobile has the same competitive incentives with respect to, and will bring the same network benefits to, its relationships with MVNOs. As an initial matter, MVNOs operate with long-term contracts that will allow them to continue to flourish post-merger, because the contracts are generally at wholesale rates and provide for added capacity that will allow MVNOs to compete and expand their subscriber bases. The company is committed to maintaining those contracts.

As Peter Ewens states in his declaration accompanying the PIS, T-Mobile has historically been supportive of its MVNO customers, because, among other reasons, “MVNOs have marketing and distribution advantages in attracting and reaching customers from particular segments.” Moreover, New T-Mobile will have significant added network capacity and will have the incentive to partner with MVNOs that can offer unique value propositions or better reach unique customer segments.

Further, as outlined in the PIS, an economic analysis conducted by Dr. Evans shows that the transaction would substantially lower the price per GB of data. Dr. Evans’ findings are further supported by the merger simulation conducted by Compass Lexecon. This analysis indicates that the merger will enable New T-Mobile to achieve lower marginal costs of providing services and offer higher quality services than would either party operating on its own. Because of the lower marginal costs and higher product quality, customers—including wholesale customers—will benefit from New T-Mobile’s economic incentives to offer better and cheaper services, as well as from the competitive pressures created for rival service providers to reduce prices and improve their services in response.

Moreover, the Applicants believe the transaction will allow New T-Mobile to enhance the value proposition of MVNOs that use its network—the benefits that accrue from the new, advanced network to New T-Mobile’s subscribers are advantages that New T-Mobile’s MVNOs can also use to compete more effectively.

T-Mobile further responds that several notable MVNOs have filed in support of the merger at the FCC. They recognize that the first nationwide 5G network offers a strong competitor to AT&T and Verizon and will drive down costs.

- Tracfone: “TracFone expects that the New T-Mobile will increase the MNO wholesale competition for TracFone’s business and thus reduce wholesale costs.”
- Ultra Mobile and Mint Mobile: The merger “will help create networks with better coverage, more capacity, greater throughput, and lower latency than would otherwise be available” and “will drive down prices, reducing wireless connectivity costs for both the MVNOs and U.S. consumers they serve.”
- Prepaid Wireless Group: The network investment New T-Mobile will make as a result of the merger “will promote MVNO competition in the near term with improved 4G coverage and lead to a competitive 5G market going forward across the entire nation, including in rural areas.”
- Republic Wireless: “A stronger and more affordable third network, run by leaders with a strong track record of openness towards partnering with new entrants, will provide the necessary foundation for the development and delivery of next-generation mobile products and services.”

See also Response to Cal PA DR 1-20 and Initial and Supplemental Responses to Cal PA DR 1-122.

Data Request 2-18 (10/23/18).

In terms of the metrics identified below, what is Your estimate of the total size of the market for wholesale spectrum in California? Please provide all Data You relied upon to support your answer.

- a) *Quantity of wholesale customers (i.e., the total number of MVNOs, MVNAs, and other customer of wholesale spectrum.)*
- b) *Total supply of available spectrum.*
- c) *Total demand of available spectrum.*
- d) *Total wholesale revenue (dollars).*

Response to Data Request 2-18 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases “estimate,” “market for wholesale spectrum in California,” “other customer of wholesale spectrum,” and “available spectrum.” T-Mobile further objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information T-Mobile’s estimate of the size of the wholesale wireless market in California has no rational bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request on the ground it seeks information which is equally available to Cal PA. T-Mobile also objects to this Data Request to the extent that it is duplicative of Cal PA DRs 1-20, 1-55 and 1-122.

Subject to and without waiving its objections, T-Mobile responds as follows:

MVNOs rely on wholesale access to a facilities-based carriers’ network (like T-Mobile’s network) in order to provide Mobile Wireless Services. MVNO agreements with T-Mobile, and in the industry at large, are not executed on the basis of access to spectrum. Rather, T-Mobile, and it believes other carriers, develop wholesale agreements for access to the network on a volume basis in minutes (in the case of voice) and bytes (in the case of data). The technology behind an MVNO arrangement is similar to the technology behind roaming agreements, but the contracts between the network provider and the MVNO allow the MVNO to resell services. Further, some contracts between network providers and MVNOs allow the resale of branded services. As of the first quarter of 2018, T-Mobile understands approximately 100 independent MVNOs operated in the United States. As of the end of 2017, according to *Prepaid Phone News*, the total number of MVNO retail end users was approximately 50.5 million.

T-Mobile does not have access to information on the total number of MVNO subscribers or the total revenues of MVNOs in California. For purposes of responding to this DR, however, T-Mobile has collected nationwide information for each MVNO or MVNA with which T-Mobile has a contract with respect to the total number of MVNO customers using the T-Mobile network, and for these customers, minutes used, SMS messages sent or received, data used (in megabytes), and the total revenue collected from the MVNO or MVNA. Where available, this data is provided for each month from January 2015 through July 2018. Not all MVNO customers have purchased wholesale mobile wireless services from T-Mobile in every month

since 2015. Monthly customer observations are excluded where the MVNO customer did not purchase wholesale mobile wireless services from T-Mobile. Furthermore, information is not available for some MVNOs that are no longer in business. See Cal PA DR 002 Production Folder, documentation beginning with Bates stamp TMUS-CPUC-PA-11008145.

In addition, because some MVNO customers also provide IoT services to their end users, the “Service” field distinguishes between the two kinds of mobile wireless service. The “Total Subscribers” field for the IoT observations should be interpreted as the total number of IoT connections.

T-Mobile further responds that its total revenue for 2018 from the sale of MVNO services nationwide is [BHC-AEO]REDACTED [EHC-AEO]. T-Mobile does not have insight into the operations of other carriers or the revenue they generate from the sale of wholesale services. T-Mobile also does not have insight into the MVNOs’ operations or the revenues that they generate. Therefore, T-Mobile does not know the total wholesale revenues of MVNOs in California.

Data Request 2-19 (10/23/18).

Please provide the following information for each MVNO that You sell wholesale services to in California:

- a) The MVNO's name.*
- b) The MVNO's "Do Business As" name or retail-brand name.*
- c) The locations where the MVNO offers retail service. (Please disclose the locations at the most specific/granular level available, i.e., census block, census block group, city, county, or zip code).*
- d) The total number of retail customers the MVNO serves in California utilizing spectrum acquired from You. Please disclose the most recent data available.*

Response to Data Request 2-19 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases "MVNOs," "sell wholesale service to in California," "locations where the MVNO offers retail service," and "utilizing spectrum acquired from You." T-Mobile further objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information; the identity of T-Mobile's wholesale customers, their retail locations and how many California consumers they provide service to on the T-Mobile network, has no rational bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent that it is duplicative of Cal PA DRs 1-20, 1-55 and 1-122.

Subject to and without waiving its objections, and not including any MVNOs that might otherwise be using T-Mobile's network under an arrangement with an MVNA, T-Mobile responds as follows:

- (a) T-Mobile does not maintain information on where its MVNO customers provide service in the ordinary course of business. This question is more appropriately directed toward the MVNO customer itself. Below is a list of all the MVNOs and MVNAs (denoted by * below) to which T-Mobile provides service.

[BHC-AEO]

REDACTED

REDACTED

[EHC-AEO]

- (b) Please see (a) above.
- (c) This data is not maintained by T-Mobile. This question is more appropriately directed toward the MVNO itself.
- (d) T-Mobile does not have a direct relationship with MVNOs' end-user customers and therefore cannot determine whether they reside within California. However, the total customers served by each of T-Mobile's MVNO partners nationally (using the T-Mobile network) is provided in response to DR 2-18 above.

Data Request 2-20 (10/23/18).

How many MVNOs do You sell wholesale services to nationwide?

Response to Data Request 2-20 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrase “sell wholesale services to nationwide.” T-Mobile also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information; the number of MVNOs that have contractual arrangements with T-Mobile has no rational bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that it sells wholesale services to 13 MVNOs and MVNAs nationwide.

Data Request 2-21 (10/23/18).

Please provide the name of each MVNA that You sell wholesale services to in California.

Response to Data Request 2-21 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrase “sell wholesale services to in California.” T-Mobile also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information; the number and names of MVNAs that have contractual arrangements with T-Mobile has no rational bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile further objects to this Data Request to the extent it seeks information that would violate the privacy rights of its customers and is otherwise inconsistent with state and federal laws protecting customer privacy including but not limited to Public Utilities Code Section 2891 and Article 1 of the California Constitution.

Subject to and without waiving its objections, T-Mobile responds that it does not maintain information on where its MVNA customers (or their underlying MVNOs) provide service in the ordinary course of business. This question is more appropriately directed toward the MVNA itself. See Response to Cal PA DR 2-19 above.

Data Request 2-22 (10/23/18).

How much of Your mobile network capacity in California did you sell on a wholesale basis to MVNOs each year from 2012 through 2018 to date?

Response to Data Request 2-22 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “mobile network capacity in California” and “sell on a wholesale basis.” T-Mobile also objects to this Data Request on the grounds it is overbroad in temporal scope and unduly burdensome. T-Mobile further objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information; the historical usage patterns of MVNO subscribers with respect to voice, text and data has no rational bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent that it is duplicative of Cal PA DR 1-20.

Subject to and without waiving its objections, MVNO agreements with T-Mobile, and in the industry at large, are not executed on the basis of “network capacity.” Rather, carriers develop wholesale agreements for access to the network on a volume basis in minutes (in the case of voice) and bytes (in the case of data). T-Mobile responds that it does not maintain data in the format requested above in the ordinary course of business. However, T-Mobile has calculated the number of MVNO/MVNA devices on its network in California as of December 31, 2017 and September 30, 2018, in an effort to further respond to this DR.

As of December 31, 2017, approximately [BHC-AEO] [REDACTED] EHC-AEO] percent of devices on its network in California were MVNO devices. In September 2018, approximately [BHC-AEO] [REDACTED] EHC-AEO] percent of devices on its network in California were MVNO devices. These percentages reflect the number of unique devices that belong to MVNO customers’ end users that were identified on the network in California at least one time over a 30-day period. The analysis considered several markets, including Los Angeles North, Los Angeles, Sacramento, San Diego, San Francisco, and Southern California. T-Mobile does not retain network data to calculate possible estimates for earlier years.

See also Response to Cal PA DR 1-20.

Data Request 2-23 (10/23/18).

How much of Your mobile network capacity in California did you sell on a wholesale basis to MVNAs each year from 2012 through 2018 to date?

Response to Data Request 2-23 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “MVNAs,” “mobile network capacity in California” and “sell on a wholesale basis.” T-Mobile also objects to this Data Request on the grounds it is overbroad in temporal scope and unduly burdensome. T-Mobile further objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information; the historical usage patterns of MVNO subscribers (whose MVNO operates under an MVNA) with respect to voice, text and data has no rational bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent that it is duplicative of Cal PA DR 1-20.

Subject to and without waiving its objections, MVNA agreements with T-Mobile, and in the industry at large, are not executed on the basis of “network capacity.” Rather, carriers develop wholesale agreements for access to the network on a volume basis in minutes (in the case of voice) and bytes (in the case of data). T-Mobile responds that it does not maintain data in the format requested above in the ordinary course of business. However, T-Mobile has calculated the number of MVNO/MVNA devices on its network in California as of December 31, 2017 and September 30, 2018, in an effort to further respond to this DR.

In particular, in December 2017, approximately [BHC-AEO [REDACTED] EHC-AEO] percent of devices on its network in California were MVNA devices. In September 2018, approximately [BHC-AEO [REDACTED] EHC-AEO] percent of devices on its network in California were MVNA devices. These percentages reflect the number of unique devices that belong to MVNO customers’ end users that were identified at least once on the network in California at least one time over a 30-day period. The analysis considered several markets, including Los Angeles North, Los Angeles, Sacramento, San Diego, San Francisco, and Southern California. T-Mobile does not retain network data to calculate possible estimates for earlier years.

See also T-Mobile’s Response to Cal PA DR 2-22 above and its previous Response to Cal PA DR 1-20.

Data Request 2-24 (10/23/18).

How much of Your mobile network capacity in California did you sell on a wholesale basis to all customers each year from 2012 through 2018 to date?

Response to Data Request 2-24 (11/7/18).

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “mobile network capacity in California” and “sell on a wholesale basis,” and “all customers.” T-Mobile also objects to this Data Request on the grounds it is overbroad in temporal scope and unduly burdensome. T-Mobile further objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information; the historical usage patterns of wholesale customers (and their subscribers where applicable) with respect to voice, text and data has no rational bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request to the extent that it is duplicative of Cal PA DR 1-20.

Subject to and without waiving its objections, MVNO agreements with T-Mobile, and in the industry at large, are not executed on the basis of “network capacity.” Rather, carriers develop wholesale agreements for access to the network on a volume basis in minutes (in the case of voice) and bytes (in the case of data). T-Mobile refers to its Response to Cal PA DRs 2-22 and 2-23. See also Response to Cal PA DR 1-20.

Data Request 5-10 (11/19/18).

Please provide any and all studies and data comparing the price levels for postpaid wireless services among AT&T, Verizon, Sprint and T-Mobile over the period 2012 through 2018.

Response to Data Request 5-10 (12/11/18).

T-Mobile objects to this Data Request on the grounds it is overbroad in temporal scope and vague and ambiguous with respect to the phrases “any and all studies and data” and “price levels.” T-Mobile also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information as pricing studies related to these carriers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request on the grounds the information is equally available to Cal PA.

Subject to and without waiving its objections, T-Mobile responds by producing various pricing studies, including:

- *@Work Performance*
- *@Work Weekly Acquisition Metrics*
- *Global Data*
- *Wave 7*
- *Competitive Intelligence Headlines*
- *Pricing Cheat Sheet*
- *Marketing Learning System*
- *Brand Equity Monitor (“BEM”)*
- *Ace Metrics*
- *Rapid Offer*
- *Weekly Performance Highlights Advertising Campaign Reports*

See Cal PA DR 005 Production Folder, confidential documents beginning with Bates no. TMUS-CPUC-PA-14000001.

Data Request 5-12 (11/19/18).

Please provide any and all studies and data comparing the price levels for prepaid wireless services offered directly by Sprint and T-Mobile and by MVNOs that utilize the Sprint and/or T-Mobile networks over the period 2012 through 2018.

Response to Data Request 5-12 (12/11/18).

See Response to DR 5-10.

Data Request 5-13 (11/19/18).

Please provide any and all studies and data comparing the price levels for prepaid wireless services offered directly by AT&T and Verizon and by MVNOs that utilize the AT&T and/or Verizon networks over the period 2012 through 2018.

Response to Data Request 5-13 (12/11/18).

See Response to DR 5-10.

Data Request 5-14 (11/19/18).

Please provide any and all studies and data comparing the price levels for postpaid wireless services offered directly by Sprint and T-Mobile and by MVNOs that utilize the Sprint and/or T-Mobile networks over the period 2012 through 2018.

Response to Data Request 5-14 (12/11/18).

See Response to DR 5-10.

Data Request 5-15 (11/19/18).

Please provide any and all studies and data comparing the price levels for postpaid wireless services offered directly by AT&T and Verizon and by MVNOs that utilize the AT&T and/or Verizon networks over the period 2012 through 2018.

Response to Data Request 5-15 (12/11/18).

See Response to DR 5-10.