Docket No.:	A.18-07-011 and A.18-07-012
Exhibit No.:	T-Mobile-
Hearing Date:	
Witness:	Susan Brye
ALJ:	Karl Bemesderfer
Commissioner:	Clifford Rechtschaffen

REBUTTAL TESTIMONY OF SUSAN BRYE

SENIOR DIRECTOR, THIRD-PARTY RISK MANAGEMENT PROGRAM
T-MOBILE USA, INC.

ON BEHALF OF T-MOBILE USA, INC.

JANUARY 29, 2019

—PUBLIC VERSION—

TABLE OF CONTENTS

ATTACHMENTS

I.IDENTIFICATION OF WITNESS

Q: Please state your name, occupation, and business address.

A: My name is Susan Brye. I am the Senior Director of T-Mobile US, Inc.'s (T-Mobile) Third-Party Risk Management (TPRM) Program, which is housed within our Internal Audit and Risk Management Department. The TPRM Program is a dedicated team within T-Mobile focused on managing regulatory, legal and operational risks arising from doing business with third parties. TPRM evaluates a broad range of potential third-party engagement risks, including cybersecurity and data handling, privacy, financial condition, legal and regulatory compliance, business continuity and other areas of potential concern.

My business address is 12920 SE 38th Street, Bellevue, Washington 98006.

Q: Please describe your professional qualifications.

A: Prior to joining T-Mobile in 2017, I was Director, Corporate Counsel at Starbucks Coffee Company with responsibilities in the areas of intellectual property, cybersecurity, privacy, government investigations and complex commercial litigation. I previously worked in the financial services industry as Assistant General Counsel, Vice President for JPMorgan Chase & Co/JPMorgan Chase Bank and as First Vice President & Senior Counsel at Washington Mutual Bank supporting complex litigation, intellectual property and government investigations. Before moving in-house, I was in private practice at Lane Powell, PC where I represented lenders and secured creditors in business bankruptcies and reorganizations, commercial litigation and monetization of intellectual property.

Q: Have you ever provided testimony before this Commission.

A: No, I have not.

II.PURPOSE OF TESTIMONY

Q: What is the purpose of your rebuttal testimony?

A: The purpose of my testimony is to respond to Cal PA testimony which purports to characterize T-Mobile's third-party risk management processes and, in that context, to provide further information on the TPRM program and the extent to which T-Mobile reviews and monitors third-party vendor relationships, including protocols for identifying and managing third parties with access to T-Mobile customer and employee data.

Q: Can you summarize your testimony?

A: I respond to and provide clarification on the assertions raised by Cal PA regarding T-Mobile's approach to third-party risk management. T-Mobile does, in fact, prioritize and identify third-party risk management as a critical business function and accordingly has heavily invested in development of a mature, comprehensive program and methodology for evaluating and managing third-party risks. As discussed below, it is inaccurate to suggest that T-Mobile does not take third party risk management seriously.

Q: Are you generally familiar with these proceedings at the Commission?

A: Yes. I understand that T-Mobile and Sprint have filed two applications with the Commission. One seeks approval of the transfer to Sprint Communications, which I understand is a non-dominant wireline provider in the state, to T-Mobile. The other application provides the Commission with an opportunity to review the wireless transfer notification. My understanding is that the Commission has set these hearings to consider various issues related to those applications.

III.T-MOBILE THIRD-PARTY RISK MANAGEMENT

Q: Cal PA contends that "T-Mobile's new process for evaluating third-party data risks has some gaps." (Donnelly Testimony at p. 10.) As the senior director of T-Mobile's third party risk management group, how do you respond?

A: T-Mobile's Third-Party Risk Management (TPRM) Program is an established, comprehensive and robust program that T-Mobile implemented for the specific purpose of evaluating third party risks. The TPRM function includes 1 senior director, 1 director, 5 managers and 12 analysts, including 8 specially-trained in cybersecurity issues to review prospective third-party engagements. The TPRM program was designed in accord with industry best practices with well-defined procedures for determining what information to collect and how to assess risks to inform engagement decisions and set parameters to protect T-Mobile (including Metro) and its customers. T-Mobile designed a proprietary, customized program to manage vendor risks specific to our business to more thoroughly protect T-Mobile data compared to "off the shelf" TPRM solutions commercially available. Although we are continuously improving and recalibrating the TPRM Program to reflect changing business needs, our program is comprehensive and particularly robust.

The scope of TPRM's pre-engagement review varies based on the inherent risk presented by the proposed third-party engagement. The higher the inherent risk of an engagement, the more assessments and oversight TPRM requires as a condition to engagement. The TPRM Program evaluates every engagement with a new or existing supplier, which allows us to assess individualized risks at an engagement level as those may differ across multiple engagements with the same supplier.

TPRM review includes, among other assessments, a "Cyber Assessment" that is required for all vendor engagements where the supplier will have access to restricted or confidential T-Mobile data or access to any T-Mobile network. The Cyber Assessment is a detailed cybersecurity and data handling review and is triggered and required by TPRM for every proposed supplier who will have access to T-Mobile customer or other personal data. For example, an IT managed services supplier must submit to a Cyber Assessment prior to execution of any agreement, whereas a HVAC operator or landscaper—neither of which would have logical access to T-Mobile networks or systems—would not.

TPRM uses an objective framework for evaluating vendor risks. TPRM has adopted a comprehensive risk scoring protocol for evaluating vendors and engagement risks using a multi-tiered approach. The scope of TPRM's risk reviews depends on the inherent risk of engagement attributes (*e.g.*, network access, access to Customer Proprietary Network Information (CPNI)). The results of the individual risk assessments the supplier completes creates a residual risk score and is based on the supplier's responses, entity attributes, and any prior assessments, all of which collectively inform the risk profile of the supplier for that intended engagement. By assessing risk both horizontally (across the assessments) and vertically (within each assessment), T-Mobile obtains a more complete picture of a vendor's ability to successfully perform the engagement and protect T-Mobile information. TPRM supplements assessments completed by the supplier with commercially-available licensed tools and market-based diligence resources that inform and enhance intelligence obtained through the vendor risk assessment process.

TPRM and its subject matter experts evaluate assessment data and responses on engagements. If material risk issues are identified, the TPRM team makes recommendations to the business, internal legal counsel and the procurement team on how to proceed and any requirements for engagement to reduce the engagement risk profile. I also, by charter, have centralized decision-making authority at T-Mobile to reject a vendor for risk-based issues. That centralized accountability allows T-Mobile to assess vendor risks in a disciplined way and harmonize risk-based decision making across the enterprise.

Q: At what point in the onboarding process does T-Mobile review prospective third party relationships in its TPRM program? (Donnelly Testimony at p. 10.)

A: TPRM review is required *before* engagement with any supplier. We have internal controls in place to prevent contract signature until after TPRM has certified our review is complete. Additionally, the TPRM Program includes pre-engagement due diligence in addition to re-review of the supplier throughout the engagement. TPRM re-reviews occur at least every three (3) years for lower inherent risk engagements if their initial residual risk scores were minor or insignificant. TPRM conducts more frequent re-reviews for higher inherent risk engagements and/or if the initial risk scores were moderate or higher. Re-reviews also may be triggered in response to triggering events such as a reported security breach; change in corporate control of

the vendor; negative news reports; documented poor service levels; or any other basis that in TPRM's business judgment warrants a refresh review. Moreover, for existing vendors that come up for a new engagement or renewal before the scheduled TPRM re-review is scheduled to occur, TPRM strikes the re-review in favor of a new pre-engagement due diligence assessment and resets the re-review cadence based on the new engagement date.

Q: Can you provide a brief overview of the information that the TPRM program reviews regarding third-party vendors and its process for reviewing such vendors?

A: Yes. TPRM review is required for *all* third-party suppliers, including promotions partners, consultants and service providers with whom T-Mobile is interested in working or partnering. This includes any supplier who may potentially have access to T-Mobile data or customer information.

The TPRM process evaluates supplier engagements against a number of "risk domains," or the categories of risks an organization may face or need to evaluate when doing business with third parties. T-Mobile's TPRM framework was designed with the assistance of an external consultant, Deloitte, who worked with T-Mobile to identify the risk domains most relevant to our business for coverage under the program. The risk domains evaluated by T-Mobile's TPRM team under the current program are: (1) Cyber / Security Risk; (2) Privacy Risk; (3) Related-Party Transactions; (4) Business Continuity / Disaster Recovery Risk; (5) Fourth Party (Subcontractor) Risk; (6) Reputational Risk; (7) Operational Risk; (8) Financial Risk; (9) Anti-Corruption Risk; (10) Regulatory / Compliance Risk; (11) Insurance Coverage Risk; (12) Geopolitical Risk; and (13) Office of Foreign Assets Control (OFAC) Screening. Many of these risk domains include additional sub-domain risks. The TPRM program periodically reviews its risk domains and underlying criteria and we update them as necessary to account for new categories of risk.

Supplier reviews incorporate the above risk domain coverage through (i) risk assessment questionnaires, some of which are issued to the supplier and some to the internal business sponsor for each engagement; and (ii) commercially-available tools TPRM utilizes to inform or confirm the accuracy of the questionnaire responses of the supplier.

When determining what assessment questionnaires are required for each engagement, TPRM first assigns the engagement an inherent risk score based on the particularized service the supplier will provide to T-Mobile. Those services are mapped to a prescription of assessments that assure coverage of all risk domains applicable to that engagement. The higher the inherent risk, the more risk questionnaires will be required, although lower inherent risk engagements are still prescribed a set of risk assessments that adequately cover risk domains applicable to all vendor engagements, such as Related-Party Risk, Financial Risk, Fourth-Party Risk, Operational Risk, *etc*.

While the TPRM program generally relies on suppliers to provide accurate and complete information in response to questionnaires, we have included a number of checks and balances to ensure that TPRM review is comprehensive and that information provided by a supplier is accurate and complete. The internal business sponsor for each engagement must complete a supplier assessment to verify alignment on the scope of services, including data access granted to the supplier and how access will be managed. It is also common for the TPRM analyst to contact the supplier directly for additional input or information if its answers are inconsistent with other representations or to clarify its procedures and controls.

Q: Do you use any other resources to verify the information you receive from third-party vendors in this process?

A: Yes we do. TPRM also utilizes commercially-available licensed tools to verify certain representations, including Lexis Diligence to identify sanctions activities, regulatory action, or investigations concerning the entity and its insiders. We also utilize Lexis' Intelligize platform to identify potential related parties and corporate filings and activities. TPRM also pulls an Experian, Creditsafe or PitchBook report to validate the third party's affiliates and representations regarding its financial condition and a BitSight score as part of the Cyber Assessment to validate cyber resiliency representations. The Digital Security Organization may also require pre-engagement penetration testing of a third party's environment using Veracode or another tool, and may seek certifications for specific services where business requirements merit third-party attestation or compliance testing evaluation such as Payment Card Industry Data

Security Standard (PCI-DSS), Sarbanes-Oxley Act (SOX), Telecommunications Act (U.S. Code Title 47 § 222), CPNI rules, or similar certifications or audits.

Q: Cal PA makes repeated references to a TRS 610 form and an SRM (Donnelly Testimony at pp. 10-12). Can you explain what that is?

A: Cal PA's assertions refer to processes referenced in legacy policy TRS-610 (Enterprise Third-Party (Supplier) Risk Management Standard) that no longer governs required security requirements for suppliers. That risk standard has been replaced with TISS-610 (Third-Party (Supplier) Information Security Requirements) the new governing information security standard for T-Mobile suppliers. The "Enterprise Third Party (Supplier) Risk Assessment (ESRA) Screening Form" mentioned in retired TRS-610 refers to T-Mobile's Supplier Risk Management (SRM) Questionnaire, which was both the intake screening form and the cybersecurity questionnaire under the prior vendor review program. Under that legacy program (e.g., before the current TPRM program), the Supplier Risk Management Review (SRMR) was the cybersecurity assessment that suppliers with access to confidential or restricted T-Mobile data would have been required to complete. Under the TPRM program, however, suppliers are now required to undergo an even more comprehensive review, including a detailed 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. New TISS-610 better aligns with NIST standards, technology advancements, and security industry best practices.

Q: Cal PA asserts that supplier risk management should be a company priority (Donnelly Testimony at 13). How would you describe T-Mobile's approach?

A: Supplier risk management is a critical function and important business priority at T-Mobile. T-Mobile has invested in and designed a mature TPRM program and that commitment and operational processes will carry over into New T-Mobile. Years ago, T-Mobile's senior leadership recognized the need for a comprehensive third-party risk program at T-Mobile and tasked the business to develop and manage a defensible third-party risk program to drive engagement risk strategy across the enterprise to protect T-Mobile and our customers. That executive initiative resulted in the current TPRM Program and the Board of Directors and T-

Mobile's senior leadership have dedicated significant financial, operational and personnel resources necessary to mature the function. T-Mobile's Information Security and Privacy Council and Enterprise Risk and Compliance Committee receive routine updates regarding supplier risks and the TPRM Program, and the Board of Directors and the Audit Committee receive periodic updates on third-party risks and how TPRM's operational controls and program are progressing.

Q: Cal PA asserts that T-Mobile "should create an inventory of all third-party suppliers and subcontractors who have or will have access to New T-Mobile customer data" (Donnelly Testimony at 18). Can you comment?

A: Yes. In fact, my team has been and is actively engaged in creating an additional comprehensive inventory specifically of our vendors who have access to T-Mobile customer data. That work is ongoing and it is our expectation that it will only further reinforce our cybersecurity efforts discussed above.

Q: Cal PA states that T-Mobile's third-party data breach notification requirements should go further, arguing specifically that "New T-Mobile should require third parties to notify New T-Mobile staff within 24 hours of a data breach or suspected breach, whether the breach originates with the third party or their subcontractor." (Donnelly Testimony at p. 19.) What does T-Mobile currently require of its third-party suppliers?

A: T-Mobile requires its third-party suppliers to contact T-Mobile immediately in the event of a data breach that could involve confidential company information or that of its customers. For relationships with third-party suppliers where the supplier will have access to T-Mobile's confidential information, including customer information, 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, and I have included a copy with my testimony as Attachment A. That template requires, among other things, that **[BHC – AEO]** [redacted]

[redacted] **[EHC – AEO]** Moreover, in Section 4.2 of new TISS-610 applicable to all supplier engagements, T-Mobile suppliers must: (1) have the capacity to immediately notify T-Mobile of any security breach; (2) assist T-Mobile in investigating any such breach; (3) have technical, physical and administrative measures in place so that vulnerabilities are disclosed responsibly; and (4) not publicly disclose any information about the security breach unless authorized by T-Mobile.

Q: Does that conclude your rebuttal testimony?

A: Yes.

ATTACHMENT A

—PUBLIC VERSION—
(ENTIRE ATTACHMENT SUBMITTED UNDER SEAL)