Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
T-Mobile US, Inc.	)	File Nos.: EB-TCD-21-00032661;
	)	EB-TCD-23-00034726;
	)	EB-TCD-23-00035152;
	)	EB-TCD-23-00035233
	)	CD Acct. No.: 202432170007
	)	FRN: 0014194476

ORDER

Adopted: September 27, 2024 **Released: September 30, 2024**

By the Chief, Enforcement Bureau:

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission) has entered into a Consent Decree resolving the Bureau's investigations into whether T-Mobile US, Inc. (T-Mobile or Company): (i) failed to meet its duty to protect the confidentiality of customer proprietary information (PI); (ii) impermissibly used, disclosed, or permitted access to individually identifiable customer proprietary network information (CPNI) without customer approval; (iii) failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI; (iv) engaged in unjust and unreasonable information security practices; and (v) made misrepresentations to its customers regarding its information security practices.

2. The Communications Act of 1934, as amended (the Act), and the Commission's rules impose various duties on telecommunications carriers. These duties include specific requirements that carriers protect customer information as well as proprietary information of other carriers,[1] and an overarching obligation that carriers' practices be "just and reasonable."[2] The Commission has made clear that it expects telecommunications carriers to take "every reasonable precaution" to protect their customers' proprietary or personal information.[3] The Commission has also explained that the statutory obligation to employ "just and reasonable" practices extends to carriers' information security practices.[4]

3. T-Mobile suffered data breaches in 2021, 2022, and 2023. Combined, these breaches affected millions of current, former, or prospective T-Mobile customers and millions of end-user customers of T-Mobile wireless service resellers, which operate on T-Mobile's network infrastructure and are known as mobile virtual network operators (MVNOs). The customer information exposed in these incidents included PI (such customers' names, addresses, dates of birth, Social Security numbers, and driver's license numbers) and CPNI (such as the features customers subscribed to and the number of lines their accounts).

---

[1] *See* 47 U.S.C. § 222; 47 CFR § 64.2001 *et seq*.

[2] 47 U.S.C. § 201(b).

[3] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64, n.198 (2007) (citing 47 U.S.C. § 222(a)).

[4] *See TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13335-37, paras. 31-35 (2014), *consent decree adopted*, *TerraCom, Inc. and YourTel America, Inc*, Order, 30 FCC Rcd 7075 (2015) (reaching settlement in which companies paid civil penalty of $3.5 million).

4. The failure to protect the confidentiality of customers' PI and the PI of other carriers violates a carrier's statutory duty under the Act[5] to protect that information. Moreover, impermissibly using, disclosing, or permitting access to individually identifiable CPNI without customer approval and failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI violate a carrier's statutory duty under the Act and the requirements of the Commission's CPNI rules, respectively.[6] These failures also constitute an unjust and unreasonable practice in violation of the Act, as do misrepresentations regarding a carrier's information security practices.[7]

5. To settle these investigations, T-Mobile will pay a civil penalty of $15,750,000 and commit to spending an additional $15,750,000 over the next two years to strengthen its cybersecurity program, and develop and implement a compliance plan to protect consumers against similar data breaches in the future. Specifically, T-Mobile will be required to improve its privacy, data security, and cybersecurity practices by, among other things:

(i) **Corporate Governance:** designating a Chief Information Security Officer who will report regularly to the Board of Directors on cybersecurity matters;

(ii) **Modern Zero-Trust Architecture:** moving towards a "zero trust" security framework and segmenting its network to limit the blast radius when a breach occurs;

(iii) **Identity and Access Management:** implementing phishing-resistant multifactor authentication (MFA) to secure its networks and systems;

(iv) **Data Minimization and Deletion:** adopting data minimization, data inventory, and data disposal processes designed to limit its collection and retention of customer information;

(v) **Critical Asset Inventory:** identifying and promptly tracking critical assets on its network to prevent misuse or compromise; and

(vi) **Independent Third Party Assessments:** conducting independent third-party assessments of its information security practices.

6. Implementing these practices will require significant—and long overdue—investments. To do so at T-Mobile's scale will likely require expenditures an order of magnitude greater than the civil penalty here. The Commission will hold T-Mobile accountable for making these mandatory changes to comply with statutory and regulatory obligations going forward and to ensure that T-Mobile does not create unnecessary cybersecurity risk for others through its business practices (e.g., mergers and acquisitions and facilities-based services for MVNOs).[8] When organizations that have data on individuals fail to act as responsible stewards for this data, they externalize the costs onto everyday Americans.[9] By compelling T-Mobile to make these changes to its business practices, the Commission supports a whole-

[5] 47 U.S.C. § 222(a).

[6] *Id.* § 222(c); 47 CFR § 64.2010(a).

[7] 47 U.S.C. § 201(b).

[8] For example, T-Mobile discloses that it "acquired and continue[s] to acquire companies with cybersecurity vulnerabilities or unsophisticated security measures, which exposes [T-Mobile] to significant cybersecurity, operational, and financial risks." Sec. & Exch. Comm'n, Form 10-K filed by T-Mobile US, Inc. (Feb. 2, 2024), https://www.sec.gov/Archives/edgar/data/1283699/000128369924000008/tmus-20231231.htm. T-Mobile does not bear these cybersecurity risks alone but may also expose its customers and other carriers to unnecessary risks through such acquisitions.

[9] White House, *National Cybersecurity Strategy* (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf ("When organizations that have data on individuals fail to act as responsible stewards for this data, they externalize the costs onto everyday Americans.").

of-government strategy to shift the consequences of poor cybersecurity away from the consumers who entrust their sensitive data with telecom service providers.[10]

7. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest would be served by adopting the Consent Decree and terminating the referenced investigations regarding T-Mobile's compliance with sections 201(b) and 222 of the Act, and section 64.2010(a) of the Commission's CPNI rules.

8. In the absence of material new evidence relating to these matters, we do not set for hearing the question of T-Mobile's basic qualifications to hold or obtain a Commission license or authorization.

9. Accordingly, **IT IS ORDERED** that, pursuant to section 4(i) of the Act, 47 U.S.C. § 154(i), and the authority delegated by sections 0.111 and 0.311 of the Commission's rules, 47 CFR §§ 0.111, 0.311, the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

10. **IT IS FURTHER ORDERED** that the above-captioned matters **ARE TERMINATED**.

11. **IT IS FURTHER ORDERED** that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Edward Smith, Senior Vice President for Government Affairs, T-Mobile, 601 Pennsylvania Ave. NW, Suite 800, Washington, DC 20004; Christopher Koegel, Director, Federal Regulatory Affairs, T-Mobile, 601 Pennsylvania Ave. NW, Suite 800, Washington, DC 20004; and Megan L. Brown, Partner, Wiley Rein LLP, 2050 M Street NW, Washington, DC 20036.

FEDERAL COMMUNICATIONS COMMISSION

Loyaan A. Egal
Chief
Enforcement Bureau

[10] *See id.* at 19. ("We will shift the consequences of poor cybersecurity away from the most vulnerable, making our digital ecosystem more worthy of trust.")

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	File Nos.: EB-TCD-21-00032661;
T-Mobile US, Inc.	)	EB-TCD-23-00034726;
	)	EB-TCD-23-00035152;
	)	EB-TCD-23-00035233
	)	CD Acct. No.: 202432170007
	)	FRN: 0014194476

CONSENT DECREE

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (FCC or Commission) and T-Mobile US, Inc. (T-Mobile or Company), by their authorized representatives, hereby enter into this Consent Decree to resolve the Bureau's investigation into whether T-Mobile violated sections 201(b) and 222 of the Communications Act of 1934, as amended (Communications Act or Act),[1] and section 64.2010(a) of the Commission's Rules[2] in connection with multiple data breach incidents in 2021, 2022, and 2023. To resolve this matter, T-Mobile agrees to implement a comprehensive security program and pay a civil penalty in the amount of $15,750,000, with an additional $15,750,000 in cybersecurity spending over the next two years to further strengthen its cybersecurity program.

I. DEFINITIONS

2. For the purposes of this Consent Decree, the following definitions shall apply:

(a) "Act" means the Communications Act of 1934, as amended.[3]

(b) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(c) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(d) "CD Acct No." means account number 202432170007, associated with payment obligations described in Paragraph 45 of this Consent Decree.

(e) "Commission" and "FCC" mean the Federal Communications Commission and all of its bureaus and offices.

(f) "Communications Laws" means collectively, the Act, the Rules, and the published and promulgated orders and decisions of the Commission to which T-Mobile is subject by virtue of its business activities, including but not limited to the CPNI Rules.

(g) "Compliance Plan" means the compliance obligations, program, and procedures described in this Consent Decree at Paragraph36(a).

(h) "Compensating Control" means a mechanism that can be put in place as an alternative to satisfying a cybersecurity measure, where the cybersecurity measure is determined to be impractical or unreasonable to implement due to technical, business, or other constraints. Such alternative mechanism must (a) meet the intent

[1] *See* 47 U.S.C. §§ 201, 222.

[2] *See* 47 CFR § 64.2010(a).

[3] 47 U.S.C. § 151 *et seq.*

and rigor of the original stated requirement; (b) provide a similar level of security as the original stated requirement; (c) be consistent with industry accepted security protocols; and (d) be commensurate with the additional risk imposed by not adhering to the original stated requirement. Compensating Controls shall be reevaluated for security effectiveness not less than annually to determine whether to retain the Compensating Control as an appropriate security measure.

(i) "Consumer" means a natural person whose Covered Information is in T-Mobile's possession as the result of a prior, ongoing, or prospective purchase of goods or services from T-Mobile.

(j) "Covered Incident" means any cybersecurity incident for which T-Mobile is required to notify, pursuant to a statutory or regulatory requirement, any United States federal, state, or local governmental entity that Covered Information was, or is Reasonably believed to have been, without authorization or exceeding authorization, accessed, acquired, used, or disclosed.

(k) "Covered Individuals" means all persons who, on behalf of T-Mobile, have authorized access to Covered Information on the T-Mobile Network pursuant to T-Mobile system credentials.

(l) "Covered Information" means CPNI. Covered Information shall not include CPNI that has been aggregated, anonymized, masked, or tokenized.[4]

(m) "Covered Third Party" means any third party that accesses, collects, processes, or stores Covered Information on behalf of T-Mobile, pursuant to a contractual agreement with T-Mobile. "Covered Third Party" shall not include: (1) any third party that only accesses, collects, or stores de minimis amounts of Consumer Covered Information on behalf of T-Mobile; and (2) third-party dealers, which, for purposes of this Consent Decree, refers to third parties that sell T-Mobile products and services pursuant to a contractual relationship with T-Mobile, that are not wholly owned or wholly controlled by T-Mobile.

(n) "CPNI Rules" means 47 CFR §§ 64.2001 – 64.2011.

(o) "Critical Assets" means all assets within the T-Mobile Network deemed most critical to T-Mobile's ongoing business and/or operational functions. "Critical Assets" shall not include customer-owned or -managed equipment.

(p) "Customer Proprietary Network Information" or "CPNI" shall have the meaning set forth at 47 U.S.C. § 222(h).

(q) "Effective Date" means the date by which both the Bureau and T-Mobile have signed the Consent Decree and the Bureau has released an Adopting Order.

(r) "Encrypt," "Encrypted," or "Encryption" means rendering data unreadable or indecipherable using an algorithm commensurate with the sensitivity of the data at issue.

(s) "Investigations" shall mean the Federal Communications Commission Enforcement Bureau investigations with case file numbers EB-TCD-21-00032661, EB-TCD-23-00034726, EB-TCD-23-00035152, and EB-TCD-23-00035233.

[4] For the purposes of this Consent Decree, Covered Information does not include information about an individual that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

(t) "Operating Procedures" means the standard internal operating procedures and compliance policies established by T-Mobile to implement the Compliance Plan.

(u) "Parties" means T-Mobile and the Bureau, each of which is a "Party."

(v) "Reasonable," "Reasonably," "Reasonableness" shall mean a level of care or effort that is commensurate with industry norms or, as applicable, a Risk Assessment, both in terms of quality and scope of effort, as well as the timing of performance.

(w) "Rules" means the Commission's regulations found in Title 47 of the Code of Federal Regulations.

(x) "T-Mobile" means, subject to the exceptions below, T-Mobile US, Inc., and any successor-in-interest, affiliate, wholly or partially owned subsidiary, and all respective directors and officers acting in their official capacities. "T-Mobile" shall not include: (1) any affiliates or subsidiaries whose networks are not integrated; and (2) Secure Federal Operations.

(y) "T-Mobile Network" means, subject to the exclusions stated herein, all networking equipment, databases or data stores, applications, servers, and endpoints that: (1) are capable of using and sharing software, data, and hardware resources; (2) are owned, operated, or controlled by T-Mobile in support of its business operations; and (3) collect, process, or store Covered Information. "T-Mobile Network" does not include: any portions of T-Mobile's network that supports wireless or internet-based communications services, data services, or commercial fiber services. "T-Mobile Network" also does not include networking equipment, databases or data stores, applications, servers, and endpoints to the extent they support the operations, administration, and maintenance of the underlying portions of T-Mobile's network that provide the services discussed in this Paragraph.

II. BACKGROUND

A. Legal Framework

3. The Act and the Commission's rules impose various duties on telecommunications carriers. These duties include specific requirements that carriers protect certain customer information and an obligation that carriers' practices be "just and reasonable."[5]

4. Section 222(c) of the Act, entitled "Confidentiality of Customer Proprietary Network Information," restricts carriers' use and disclosure of CPNI, which includes both: (a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (b) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (other than subscriber list information).[6] Section 222(c)(1) only permits a carrier to disclose, permit access to, or use a customer's individually identifiable CPNI to provide telecommunications services, or other services "necessary to, or used in," the carrier's telecommunications service, unless otherwise authorized by the customer or required by law.[7] The Commission has adopted rules implementing Section 222(c)'s protections of CPNI.

[5] 47 U.S.C. § 201(b).

[6] *See id.* §§ 222(c), 222(h)(1).

[7] *Id.* § 222(c)(1).

5. The Commission has issued regulations implementing the requirements of section 222 and has amended those rules over time. In the *2007 CPNI Order*,[8] the Commission amended its Rules relating to CPNI. Section 64.2010(a) of the Commission's Rules requires that "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[9] What constitutes a reasonable practice is highly fact-dependent. The Commission expects carriers to employ effective protections of customer data in their own systems.

6. Section 222(a) of the Act states that every telecommunications carrier "has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers . . . and customers."[10]

7. Section 201(b) of the Act states, in pertinent part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."[11] The Commission has interpreted section 201(b) to apply to carriers' practices for protecting CPNI against unauthorized access, use, or disclosure.[12]

B. Factual Background

8. T-Mobile is a telecommunications carrier that provides wireless communications services to 119.7 million post-paid and prepaid customers throughout the United States. T-Mobile is incorporated in Delaware and has its principal office in Bellevue, Washington.

1. Cybersecurity Incidents

9. T-Mobile suffered cybersecurity incidents in 2021, 2022, and 2023 as a result of the criminal acts of third parties. These breaches were varied in their nature, exploitations, and apparent methods of attack. The Bureau and T-Mobile disagree about whether T-Mobile's network and data security program and policies in place at the relevant times violated any standard of care or regulation then applicable to T-Mobile, but in the interest of resolving these investigations, and in the interest of putting consumer security first, the parties enter into this negotiated consent decree.

---

[8] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (2007 CPNI Order).

[9] 47 CFR § 64.2010(a).

[10] 47 U.S.C. § 222(a); *see also In the Matter of T-Mobile USA*, Inc., File No.: EB-TCD-18-00027702, NAL/Acct. No.: 202032170003, FRN: 0006945950, Forfeiture Order (Apr. 29, 2024) ("Section 222(a) of the Act imposes a general duty on telecommunications carriers to "protect the confidentiality of proprietary information" of "customers."). This assertion about the reach and meaning of Section 222(a) is presently subject to challenge in multiple court proceedings. *See e.g., AT&T v. FCC*, No. 24-60223 (5th Cir. filed May 5, 2024) (petition for review pending); *Texas Association of Business v. FCC*, *et. al*, No. 24-3206 (6th Cir. filed Mar. 8, 2024) (disputing *Data Breach Reporting Requirements*, WC Docket No. 22-21, Report and Order, FCC 23-111 (rel. Dec. 21, 2023)).

[11] 47 U.S.C. § 201(b).

[12] *See, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information et al.*, Docket Nos. 96-115, 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, para. 15 (1998) ("Based on the Act's grant of jurisdiction, the Commission has historically regulated the use and protection of CPNI by AT&T, the BOCs, and GTE, through the rules established in the Computer III proceedings. Sections 4(i), 201(b), and 303(r) of the Act authorize the Commission to adopt any rules it deems necessary or appropriate to carry out its responsibilities under the Act, so long as those rules are not otherwise inconsistent with the Act.").

a. 2021 Incident

10. On August 12, 2021, T-Mobile became aware of a potential attack on its systems and launched an internal investigation.[13] T-Mobile confirmed on August 15, 2021, that it had suffered a cyber attack and hired an outside vendor to conduct a forensic investigation.[14] On August 16, 2021, T-Mobile made a public announcement on its website regarding the 2021 incident,[15] followed by additional public announcements on August 17 and 20,[16] and a blog post on August 27.[17]

11. In the 2021 Incident, a criminal hacker accessed T-Mobile's network and customer data. Specifically, in 2021, a threat actor was able to gain access to a T-Mobile lab environment via a piece of telecommunications equipment by impersonating a legitimate connection to the piece of equipment. Prior to achieving this access, the threat actor appears to have engaged in reconnaissance over a period of months. The threat actor was able to exploit this initial access and successfully guess passwords for certain servers, and then moved across network environments. As a result, the threat actor was able to access another lab environment, in which the threat actor engaged in additional network scanning and password-spraying attacks. This enabled the threat actor to access other environments containing database backup files and other information. Forensic review confirmed the threat actor was able to exfiltrate data from these environments including a limited amount of CPNI.

12. In terms of data impacted, the threat actor accessed information including: (a) first and last names, addresses, dates of birth, Social Security numbers, and driver's license numbers of 7.8 million current T-Mobile customers and approximately 40 million former, and prospective customers.[18] The threat actor accessed the names, dates of birth, and ID numbers of an additional 1.9 million former and prospective customers; and names, dates of birth, and in many cases addresses of 6.1 million former and prospective customers. The threat actor also accessed, for some customers, device identifiers and account PINs. T-Mobile confirmed that no customer financial information such as credit card or debit card information was exposed in the 2021 Incident. For purposes of its class action settlement of the 2021 Incident, the number of impacted consumers was 76.6 million, of which only a very small portion had CPNI impacted.

13. T-Mobile detected the 2021 Incident in August 2021.[19] From August 15, 2021, through October 8, 2021, T-Mobile implemented various measures to cut off the intruder's access to T-Mobile's systems.[20] Thereafter, T-Mobile took a number of actions to minimize the impact of the incident and protect consumers.[21] The last evidence of intruder activity was on August 13, 2021.

14. In addition to various immediate containment actions taken (rotating network passwords, implementing additional firewall rules, disconnecting equipment) to shut down threat actor access, T-

---

[13] Response to Initial Letter of Inquiry, from T-Mobile, USA, Inc. to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 12-13 (Nov. 12, 2021) (on file in EB-TCD-21-00032661) (Nov. 2021 LOI Response).

[14] Nov. 2021 LOI Response at 13.

[15] T-Mobile, *T-Mobile Cybersecurity Incident Update* (Aug. 16, 2021), https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021.

[16] T-Mobile, *T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack* (Aug. 17, 2021), https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation.

[17] Mike Sievert, *The Cyberattack Against T-Mobile and Our Customers: What Happened, and What We Are Doing About It*, T-Mobile (Aug. 27, 2021), https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers.

[18] Nov. 2021 LOI Response at 32, 34.

[19] *Id.* at 12.

[20] *Id.* at 19.

[21] *Id.* at 30-31.

Mobile took steps intended to mitigate potential harm to consumers, including making identity theft protection available to "all individuals" regardless whether they were ever a T-Mobile customer,[22] directing customers to tools offered by T-Mobile that customers could use to protect themselves,[23] and taking steps to minimize unauthorized SIM swaps following the breach.[24] Finally, the Company created a dedicated webpage linking to the various available tools, as well as to FTC and state attorney-general websites.[25] T-Mobile has not identified any fraudulent activity that relates to data compromised in the 2021 Incident.[26]

15. In addition to the containment steps taken and consumer protections made available, T-Mobile engaged forensic experts to help it evaluate the incident and it engaged global leaders in cybersecurity risk management to help the company assess its overall posture and develop a multi-year plan to elevate cybersecurity planning, defenses and strategies. That program remains ongoing and T-Mobile has kept the Bureau informed.[27]

16. T-Mobile contacted Bureau staff regarding the incident on August 16, 2021, and participated in an initial call on August 17. T-Mobile filed a report in the CPNI Data Breach Reporting Portal on August 24, 2021.[28] The Bureau began its investigation based on (1) initial talks with the Company, (2) publicly available information posted on T-Mobile's website, and (3) the report submitted by T-Mobile to the CPNI Data Breach Portal.

17. The Bureau sent T-Mobile a letter of Inquiry on August 27, 2021,[29] followed by supplemental letters of inquiry on April 5, 2022;[30] July 8, 2022;[31] and September 16, 2022.[32] T-Mobile responded to each letter of inquiry.[33]

---

[22] *Id.* at 40.

[23] *See id.* at 40-41. These tools included Scam Shield (meant to protect customers from scammers and robocalls) and Account Takeover Protection (which added additional security to a customer's account).

[24] *See* Nov. 2021 LOI Response at 40-41, 43-44.

[25] *See* Nov. 2021 LOI Response at 40; T-Mobile, *Online Safety: Resources for identity theft and internet fraud prevention*, https://www.t-mobile.com/privacy-center/education-and-resources/online-safety#moduleSteps (last visited Sept. 27, 2022).

[26] Nov. 2021 LOI Response at 42-43.

[27] *Id.* at 13-14.

[28] *See* T-Mobile CPNI Breach Report, Reference Number 2021-7560 (Aug. 24, 2021) (on file in EB-TCD-21-32661).

[29] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (Aug. 27, 2021) (on file in EB-TCD-21-00032661) (Initial LOI).

[30] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (Apr. 5, 2022) (on file in EB-TCD-21-00032661).

[31] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (July 8, 2022) (on file in EB-TCD-21-00032661).

[32] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (Sept. 16, 2022) (on file in EB-TCD-21-00032661).

[33] *See, e.g.*, Nov. 2021 LOI Response; Response to First Supplemental Letter of Inquiry, from T-Mobile, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (June 6, 2022) (on file in EB-TCD-21-00032661); Response to Second Supplemental Letter of Inquiry, from T-Mobile, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Sept. 6, 2022) (on file in EB-TCD-21-00032661); Response to Third Supplemental Letter of Inquiry, from T-Mobile, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Oct. 10, 2022) (on file in EB-TCD-21-00032661); Response to Third Supplemental Letter of Inquiry, from T-Mobile, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Oct. 31, 2022) (on file in EB-TCD-21-

(continued….)

b. Platform Access Incident

18. In late 2022, a threat actor gained unauthorized access to a management platform that T-Mobile provides to its mobile virtual network operator ("MVNO") resellers to enable the MVNO resellers to provision services to their end-user customers. That platform contains MVNOs' customers' information.

19. Unauthorized access to the platform appears to have involved a few different tactics, including an illegal SIM swap of a T-Mobile employee, a phishing attack on another T-Mobile employee, and at least one compromise of unknown origin.

20. The Bureau learned of the incident on January 10, 2023, when one of the MVNOs that was affected submitted a report to the CPNI Breach Reporting Portal. After investigating the incident, on February 6, 2023, T-Mobile submitted a report via the CPNI Breach Reporting Portal.[34] The Bureau issued a letter of inquiry to T-Mobile on April 24, 2023,[35] to which T-Mobile responded on July 17, 2023.[36] The Bureau issued a supplemental letter of inquiry to T-Mobile on November 30, 2023;[37] T-Mobile submitted its response on March 8, 2024.[38] T-Mobile has been cooperating with the Bureau's investigation of this incident.

c. Sales Application Incident.

21. In early 2023, a threat actor used stolen T-Mobile account credentials to access a frontline sales application for which remote access had been enabled to maintain operations during the COVID-19 pandemic and view certain customer data, including a limited amount of CPNI.

22. T-Mobile became aware of the breach in late February 2023, when the Company noticed an increase in customer port-out complaints.[39] The Company launched an investigation that, on or about March 30, 2023, revealed that a threat actor had obtained the account credentials for several dozen T-Mobile retail employees.[40] T-Mobile believes that the threat actor obtained those credentials through a targeted phishing campaign.[41]

00032661); Response to Follow Up Questions to the Third Supplemental Letter of Inquiry, from T-Mobile, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Nov. 22, 2022) (on file in EB-TCD-21-00032661).

[34] CPNI Data Breach Reporting Portal Report No. 2023-731 (on file in EB-TCD-23-00035152).

[35] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (Apr. 24, 2023) (on file in EB-TCD-23-00035152).

[36] *See* Response to Letter of Inquiry, from T-Mobile, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Jul. 17, 2023) (on file in EB-TCD-23-00035152).

[37] Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (Nov. 30, 2023) (on file in EB-TCD-23-00035152).

[38] *See* Response to Supplemental Letter of Inquiry, from T-Mobile, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Mar. 8, 2024) (on file in EB-TCD-23-00035152).

[39] Response to Letter of Inquiry, from T-Mobile, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Aug. 31, 2023) (on file in EB-TCD-23-00035233) (Aug. 2023 LOI Response).

[40] *Id.* at 5.

[41] *Id.* at 2.

23. T-Mobile filed a report in the CPNI Data Breach Reporting Portal on April 11, 2023.[42] The Bureau issued a Letter of Inquiry on May 24, 2023.[43] T-Mobile submitted its response on August 31, 2023.[44]

d. Application Programming Interface (API) Incident.

24. In early January 2023, T-Mobile discovered a data breach involving one of the Company's APIs.[45] Human error led to a misconfiguration in permissions settings that allowed a threat actor to submit queries and obtain T-Mobile customer account data. The API was able to access a limited set of certain customer account data, including name, billing address, email, phone number, date of birth, T-Mobile account number, and information such as the number of lines on the account and plan features.[46] T-Mobile's investigation indicated that the threat actor obtained data from this API for approximately 37 million current postpaid and prepaid customer accounts, though many of these accounts did not include the full data set.[47]

25. T-Mobile reported the breach to the Commission on January 13, 2023, via the CPNI Data Breach Reporting Portal.[48] On January 19, 2023, T-Mobile filed a Form 8-K report with the Securities and Exchange Commission disclosing the breach.[49] The Bureau sent a letter of inquiry to T-Mobile on January 25, 2023,[50] to which T-Mobile responded on March 31, 2023.[51] The Bureau sent a supplemental letter of inquiry to T-Mobile on August 21, 2023,[52] to which T-Mobile responded on October 20, 2023.[53]

---

[42] CPNI Data Breach Reporting Portal Report No. 2023-2362 (on file in EB-TCD-23-00035233).

[43] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (May 24, 2023) (on file in EB-TCD-23-00035233).

[44] *See* Aug. 2023 LOI Response.

[45] An API is "a set of software instructions and standards that allows machine to machine communication—like when a website uses a widget to share a link on Twitter or Facebook." Gray Brooks, Gen. Services Admin., *What are APIs?* (Apr. 30, 2013), https://digital.gov/2013/04/30/apis-in-government/. *See* Nat'l Inst. of Standards and Tech., *Application Programming Interface (API)*, https://csrc.nist.gov/glossary/term/application_programming_interface (last visited May 29, 2024) ("A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.").

[46] *See* Response to Letter of Inquiry, from T-Mobile USA, Inc., to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau at 23-24 (Mar. 31, 2023) (on file in EB-TCD-23-00034726) (Mar. 2023 LOI Response).

[47] *See* Response to Supplemental Letter of Inquiry, from T-Mobile USA, Inc., to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau at 10 (Oct. 20, 2023) (on file in EB-TCD-23-00034726) (Oct. 2023 Supplemental LOI Response).

[48] CPNI Data Breach Reporting Portal Report No. 2023-247 (on file in EB-TCD-23-00034726).

[49] *See* T-Mobile US, Inc., SEC Form 8-K (Jan. 19, 2023), https://www.sec.gov/Archives/edgar/data/1283699/000119312523010949/d641142d8k.htm.

[50] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (Jan. 25, 2023) (on file in EB-TCD-23-00034726).

[51] *See* Mar. 2023 LOI Response.

[52] *See* Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to T-Mobile US, Inc. (Aug. 21, 2023) (on file in EB-TCD-23-00034726).

[53] *See* Oct. 2023 Supplemental LOI Response.

2. T-Mobile's Cybersecurity Program

26. T-Mobile has spent significant additional resources voluntarily enhancing its security program since 2021, engaging internal and outside experts to further enhance controls and processes.[54]

27. T-Mobile has made major financial and operational commitments in the course of its cybersecurity transformation and in response to FCC oversight. It has publicly committed to a multi-year investment working with leading external cybersecurity experts to enhance cybersecurity capabilities and transform its approach to cybersecurity.

28. T-Mobile has implemented processes for overseeing and identifying material risks from cybersecurity threats, and its cybersecurity processes are integrated into the Company's overall risk management system and processes. This includes use of the National Institute of Standards and Technology's Cybersecurity Framework ("NIST CSF") as a guide in cyber risk management. In addition, several senior leaders and board committees review enterprise risks and compliance issues.

29. Over the course of these Bureau investigations, T-Mobile has provided the Bureau information about its program, policies, network, and technologies that support cyber risk management.

3. Resolution of the Investigations

30. T-Mobile and the Bureau subsequently engaged in settlement negotiations. In the interest of prioritizing the security of T-Mobile consumers and resolving these Investigations, the parties enter into this negotiated Consent Decree and agree to the following terms and conditions.

III. TERMS OF AGREEMENT

31. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order

32. **Jurisdiction**. T-Mobile agrees that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree. Nothing in this agreement shall be construed to limit or expand the FCC's jurisdiction.

33. **Effective Date**. The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

34. **Termination of Investigations**. In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigations. The Bureau further agrees that it will not use the facts developed in the Investigations through the Effective Date in any subsequent investigation or proceeding.[55]

35. **Corporate Governance.**

(a) *Chief Information Security Officer*

i. T-Mobile must designate a senior executive or officer who will be responsible for maintaining and monitoring the Information Security Program (hereinafter referred to as the "Chief Information Security Officer" or "CISO" (but may be differently titled in an equivalently ranked position, and whose responsibilities, including those as specified herein, may be carried out by one or more executives or officers, or may be delegated, as necessary)). The Chief Information Security Officer must possess or have access to the authority, reporting lines, independence, resources, education, qualifications, and experience in information security appropriate to the level, size, and complexity of the position's role in maintaining and monitoring the Information Security

[54] Nov. 2021 LOI Response at 13-14.

[55] *See* 47 CFR § 1.93(b).

Program. Nothing herein requires all employees with security-related responsibilities to report to the CISO.

ii. The role of the CISO will include regular and direct reporting to the Chief Executive Officer or their designee, and the Board of Directors, or an appropriate subcommittee of the Board, concerning T-Mobile's cybersecurity posture, the cybersecurity risks faced by T-Mobile, and the cybersecurity implications of T-Mobile's line of business.

iii. The Chief Information Security Officer will report to the Chief Executive Officer or their designee, and the Board of Directors, or an appropriate subcommittee of the Board, any confirmed Covered Incident impacting more than 500 Consumers no later than forty-eight (48) hours after confirmation.

iv. T-Mobile must provide the Chief Information Security Officer and the Information Security Program with the resources and support Reasonably necessary for the Information Security Program to function as required by this Consent Decree.

36. **Compliance Plan**.

(a) **Compliance Plan.** T-Mobile must, within one hundred and eighty (180) days after the Effective Date, develop and implement a Compliance Plan designed to facilitate compliance with the Consent Decree.

37. **Information Security Program**.

(a) **General**.

i. T-Mobile must maintain a comprehensive written information security program ("Information Security Program") that is Reasonably designed to protect the confidentiality, integrity, and availability of Covered Information that T-Mobile owns, licenses, maintains, collects, stores, or transmits on the T-Mobile Network. The Information Security Program must contain administrative, technical, and physical safeguards Reasonably appropriate to:

A. The size and complexity of T-Mobile's operations;

B. The nature and scope of T-Mobile's activities; and

C. The sensitivity of the Covered Information within the T-Mobile Network.

ii. The Information Security Program must be documented. Nothing herein shall prevent the Information Security Program from being distributed across one or more documents, provided that T-Mobile maintains a comprehensive index of any such documents.

iii. The Information Security Program must be regularly reviewed and revised not less than annually.

(b) **Training**.

i. T-Mobile must provide notice of this Consent Decree to Covered Individuals at the Vice President level or higher within ninety (90) days of the Effective Date.

ii. T-Mobile must provide Covered Individuals with annual training on safeguarding Covered Information. T-Mobile must provide the training required under this Paragraph to such employees within ninety (90) days of their starting their responsibilities related to Covered Information. T-Mobile may delay such training until the next annual cycle for any such employees who have already received such training in the twelve months prior to the Effective Date, or for any such employees on leave.

iii. T-Mobile will annually select, based on a Risk Assessment, a subset of Covered Individuals to receive additional role-based training.

(c) **Segmentation**.

i. T-Mobile must maintain, to the extent technically feasible, a hybrid zero-trust framework with respect to T-Mobile-issued employee phones, tablets, virtual workstations, and desktops.

ii. The T-Mobile Network shall be segmented in a way Reasonably designed to provide that only authorized communication channels are opened between segments. As used herein, "communications channels" refers to ports on firewalls located between segments. Communications channels between segments may be authorized and enabled only to the extent necessary to perform relevant business and/or operational functions. When a change in communications channels across segments is made within the T-Mobile Network, T-Mobile must review and revise, at a level appropriate to the scope of that change, the communications channels that are opened between those segments.

iii. T-Mobile must maintain documentation for ports that are prospectively opened on firewalls between segments as follows: For the first two years after the Effective Date, such documentation must include information sufficient to identify the opened port that underwent a state change to open. For the period beginning two years after the Effective Date, such documentation must include both information sufficient to identify the opened port that underwent a state change to open and the business purpose for opening that port.

iv. For those segments within the T-Mobile Network between which communications channels are opened for a legitimate business and/or operational purpose subsequent to the Effective Date, T-Mobile must perform a Risk Assessment consistent with Paragraph 37(l) below.

v. T-Mobile must conduct a review of exceptions to the segmentation protocols and policies applicable to the T-Mobile Network consistent with Paragraph 37(l) below to determine whether the exception is still required and that the risk level is still acceptable.

vi. T-Mobile must take Reasonable steps to separate its production environments and non-production environments in the T-Mobile Network in a manner designed to reduce the risk of unauthorized movement into or out of such environments. Such requirement can be met through the use of firewalls, access control lists, endpoint software, or other similar techniques.

vii. After the Effective Date, to the extent T-Mobile uses Covered Information in a non-production environment for an extended period of time, and the circumstances necessitating such use permit, T-Mobile shall use Compensating Controls on such non-production environment to increase its security in a manner commensurate with the sensitivity of the specific stored Covered Information. Such Compensating Controls can include, without limitation, enhanced monitoring, enhanced logging, access restrictions or other appropriate types of security measures. To the extent a non-production environment requires Internet connectivity, T-Mobile will monitor such connection with intrusion detection, intrusion prevention, or similar technologies. T-Mobile may not permanently maintain Covered Information within non-production environments.

(d) **Network Access Controls**.

i. T-Mobile must regularly conduct vulnerability scans on external-facing ports on the T-Mobile Network. To the extent that a production environment and a non-production environment are separated by one or more firewalls, T-Mobile must regularly conduct vulnerability scans on such firewall(s).

(e) **Account and Password Management**.

i. T-Mobile must require Covered Individuals to use phishing-resistant multi-factor authentication methods in order to access networks, systems, or assets on the T-Mobile Network that store Covered Information, except where such use is technically or otherwise infeasible, or unreasonably burdensome or disruptive.

ii. T-Mobile must maintain policies, procedures, and controls Reasonably designed to manage access to, and use of, accounts with access to Covered Information stored or maintained on the T-Mobile Network. Such policies, procedures, and controls must be consistent with applicable best practices and standards, including, but not limited, to those identified by the National Institute of Standards and Technology (NIST).

iii. T-Mobile must take Reasonable measures to prevent administrative-level passwords from being stored in plaintext. Within two years of the Effective Date, T-Mobile must maintain Reasonable measures to Encrypt or securely store administrative-level passwords. Such measures could include, without limitation, scanning for plaintext and default passwords, automated checking for passwords in code check-in, password vaults, privileged access management, password leak detection, passwordless authentication, multifactor authentication enforcement, or equal or greater security tools that are generally accepted by the security industry.

iv. T-Mobile must maintain operating procedures Reasonably designed to change or disable default system credentials for internal systems within the T-Mobile Network that contain Covered Information. Such requirement to disable can be met by removing default credentials, enabling multifactor authentication or other technical measures that render default credentials ineffective for their intended purpose, or revoking access to systems that contain Covered Information.

(f) **Logging and Monitoring**.

i. T-Mobile must maintain intrusion prevention and detection systems, endpoint protection systems, threat monitoring systems, or similar technologies Reasonably designed to detect and restrict unauthorized access or connections to, and anomalous activities within, the T-Mobile Network. T-Mobile must periodically, but not less than annually, review the tuning of these systems to assess their effectiveness.

ii. T-Mobile must take Reasonable steps to log and monitor in real time activities on the T-Mobile Network that reflect a Reasonable likelihood of compromise to the confidentiality, integrity, or availability of Covered Information.

iii. T-Mobile must maintain a triaging process to prioritize alerts based on criticality and timely respond to security events.

iv. T-Mobile must retain, for not less than 12 months, logs of alerts that indicate suspicious or malicious activity.

v. T-Mobile must periodically, but not less than annually, review the tuning of the systems that generate alerts to verify that the T-Mobile Network is adequately monitored.

(g) **Data Retention, Minimization, and Deletion**.

i. Data Collection

A. T-Mobile must limit the collection of a Consumer's Covered Information to what is Reasonably necessary for a legitimate business or legal purpose(s). Subsequent use of the collected Covered Information must be consistent with such purposes unless T-Mobile has obtained the Consumer's consent or the use is otherwise permitted by law or regulation.

ii. Retention Schedule

A. T-Mobile must maintain, and regularly review and revise as necessary, policies that provide for the destruction, anonymization, or removal of Consumer Covered Information that is no longer necessary for legitimate business purpose(s), subject to the limitations of the inventory process of Paragraph 38, except where such information is otherwise required to be maintained by law or regulation.

iii. Covered Information Minimization

A. T-Mobile must maintain data reduction processes aimed at Reasonably minimizing T-Mobile's long-term storage of Covered Information within the T-Mobile Network (to the extent such storage is not otherwise required to be maintained by law or regulation), subject to the limitations of the inventory process of Paragraph 38.

B. Within one year from the Effective Date, T-Mobile must maintain an attestation process for business owners of databases within the T-Mobile Network that contain Covered Information to verify the owners' efforts to comply with applicable data retention and disposal policies. Such attestations shall be documented and retained by T-Mobile pursuant to the Recordkeeping requirements in Paragraph 43.

(h) **Third-Party Oversight**.

i. T-Mobile must manage Covered Third Parties that access, migrate, duplicate, or otherwise modify Covered Information on the T-Mobile Network.

ii. T-Mobile must maintain, and regularly update as necessary, a centralized inventory that categorizes and ranks Covered Third Parties in accordance with a risk-scoring protocol based on the particularized service the Covered Third Party provides to T-Mobile and specific categories of Covered Information that the Covered Third Party accesses, transmits, uses, or maintains on the T-Mobile Network.

iii. T-Mobile must use Reasonable measures to protect Covered Information maintained by or made available to Covered Third Parties, including (a) exercising due diligence in selecting Covered Third Parties; and (b) prospectively contractually obligating Covered Third Parties to comply with requirements to protect Consumer Covered Information, either by including these requirements expressly, or by mandating compliance with T-Mobile policies, industry standards, or similar that already have such requirements, except where: (i) a Covered Third Party is already subject to negotiated and agreed-upon security terms, or (ii) T-Mobile, after performing a Risk

Assessment, has granted an exception to a security requirement during or subsequent to the contracting process.

(i) **Critical Asset Inventory Process**.

i. T-Mobile must maintain a process to inventory all Critical Assets. The asset inventory must, at a minimum, identify the Critical Asset's: (i) name; (ii) assignment group; (iii) "managed by" group; (iv) location within the T-Mobile Network; (v) IP address; and (vi) serial number (where applicable). T-Mobile must maintain a process Reasonably designed to maintain a log of the disposition of any Critical Assets removed from the T-Mobile Network. Critical Assets shall remain in the log for three years after removal from the T-Mobile Network.

ii. T-Mobile must take Reasonable steps to disable and/or remove, consistent with T-Mobile's asset management policies, Critical Assets that are no longer necessary for a legitimate business or operational purpose.

(j) **Patch and Security Update Management**.

i. T-Mobile must maintain administrative and technical controls Reasonably designed to address the potential impact that security patches and security updates may have on the T-Mobile Network. T-Mobile must maintain appropriate patch management solutions within the T-Mobile Network.

ii. T-Mobile must schedule and install any security update or security patch, considering (without limitation) the severity of the vulnerability for which the update or patch has been released, the severity of the issue in the context of the T-Mobile Network, the impact on T-Mobile's ongoing business and network operations, whether the vulnerability is being actively exploited by threat actors, and the risk ratings articulated by the Cybersecurity and Infrastructure Security Agency (CISA) or other relevant governmental authority and/or an equivalent United States Department of Homeland Security (DHS) agency designated as responsible for cybersecurity.

(k) **Vulnerability Management**.

i. T-Mobile must implement and maintain a program reasonably designed to identify, assess, and remediate security vulnerabilities within the T-Mobile Network.

ii. T-Mobile must rate and rank the criticality of vulnerabilities, in accordance with an industry-standard framework (e.g., NVD, CVSS, or equivalent standard), revealed as a result of testing and scanning. For each vulnerability rated as critical, T-Mobile must take Reasonable steps to commence remediation planning and execution consistent with T-Mobile's risk remediation policies.

(l) **Risk Assessments**.

i. T-Mobile must maintain and regularly review and revise as necessary, a risk-assessment program Reasonably designed to identify, assess, prioritize, and manage material cybersecurity risks to the T-Mobile Network. The program must include methods and criteria for assessing material cybersecurity risks that are consistent with a risk assessment method that is provided by a nationally-recognized information security body ("Risk Assessment Method") and must also identify the levels of formal approval required to accept a material cybersecurity risk (if any) and the specific documentation required to be created and maintained of the review process and acceptance (if any). The level of

formal approval and documentation prescribed by the Risk Assessment Method shall be commensurate with the level of risk, with increasing levels of risk requiring more formal approval or documentation and lesser levels of risk requiring less (or no) approval or documentation.

ii. The Risk Assessment Method must provide, at a minimum, that:

A. T-Mobile take Reasonable steps to assess and document, at least annually and at a level appropriate to the risk, internal and external material cybersecurity risks to the confidentiality, integrity, and availability of Covered Information; and

B. T-Mobile take Reasonable steps to assess and document, at least annually, the sufficiency and effectiveness of any safeguards in place to address identified material cybersecurity risks and modify such safeguards as necessary.

iii. For those material cybersecurity risks that require documentation, T-Mobile must generate and retain a report (which may be reflected in one or more documents or electronic records) for at least three years demonstrating how such risk is to be managed in consideration of, among other things, the cost to T-Mobile or difficulty in implementing effective countermeasures. T-Mobile must maintain a process to monitor accepted material cybersecurity risks that is consistent with T-Mobile's risk assessment policies.

38. **Consumer Data Inventory Process**.

(a) T-Mobile must maintain a process to inventory its Consumers' Covered Information maintained in databases on the T-Mobile Network ("Consumer Data Inventory Process"). The Consumer Data Inventory Process must be Reasonably designed to facilitate minimization and appropriate retention and disposal of Consumer Covered Information, subject to the capabilities and limitations of automated and manual inventory control solutions.

39. **Forensic Reports**.

(a) Following a Covered Incident that affects 10,000 or more Consumers, T-Mobile must obtain, and furnish to the Bureau upon formal written request, a forensic report memorializing the facts of the Covered Incident, including how it occurred and the scope of the compromise ("Forensic Report"). Each Forensic Report must be prepared by a qualified professional with at least five (5) years of experience conducting forensic analyses of data security incidents.

(b) Nothing contained in this Consent Decree shall directly or indirectly in any way whatsoever impair, prejudice, or otherwise adversely affect T-Mobile's right at any time to assert attorney-client privilege, work product privilege, or any other applicable privilege, doctrine, protection, or immunity, nor the Bureau's right to dispute, contest, or challenge any such assertion.

40. **Representations to Consumers**.

(a) **Prohibitions on Misrepresentations**.

i. T-Mobile shall not misrepresent in its privacy policies, statements on its website, its subscriber agreements, or other communications or representations made to Consumers, the extent to which T-Mobile Reasonably protects the privacy or security of Consumers' Covered Information.

(b) **Privacy Policies**.

i. The privacy policies and statements on T-Mobile's website regarding Consumer privacy and the security of Consumers' Covered Information must (A) comply with applicable law, and (B) reflect T-Mobile's data security and privacy practices and be updated routinely to reflect any material changes.

41. **Independent Third-Party Assessment**.

(a) T-Mobile must obtain an assessment of T-Mobile's compliance with the terms of this Consent Decree (the "First Third-Party Assessment"). Such assessment will not cover Paragraphs 37(c)(iii) (documentation requirements related to prospectively-opened ports) and 37(e)(iii) (measures to prevent administrative-level passwords from being stored in plaintext). Following implementation of the prospective requirements contained in Paragraphs 37(c)(iii) and 37(e)(iii), T-Mobile must obtain a follow-up assessment addressing T-Mobile's compliance with Paragraphs 37(c)(iii) and 37(e)(iii) (the "Second Third-Party Assessment," and together with the First Third-Party Assessment, the "Third-Party Assessments").

(b) T-Mobile will be responsible for all costs associated with the Third-Party Assessments.

(c) The Third-Party Assessments required by this Section must be conducted by an independent third-party (the "Third-Party Assessor") who: (1) is a United States citizen; (2) uses procedures and standards generally accepted in the profession; (3) conducts an independent review; and (4) retains all documents relevant to each Assessment for three (3) years after completion of such Assessment.

(d) T-Mobile must provide the Bureau with the name, affiliation, and qualifications of the proposed Third-Party Assessor. The Bureau shall inform T-Mobile of any objection, based on demonstrated good cause, to the proposed Third-Party Assessor no later than fourteen (14) calendar days after the Bureau has received notice of T-Mobile's proposed candidate. T-Mobile shall have fourteen (14) calendar days to respond to the Bureau's objection(s). If the Bureau then stands on its objection that the proposed candidate is not qualified to serve as the Third-Party Assessor, T-Mobile shall then propose an additional candidate(s) within thirty (30) calendar days of the Bureau's determination. This process shall continue until a Third-Party Assessor acceptable to the Bureau and T-Mobile is selected.

(e) The reporting period for the First Third-Party Assessment must commence 180 days after the Effective Date and must cover the first three hundred and sixty-five (365) days that begins after expiration of the 180-day period following the Effective Date. The reporting period for the Second Third-Party Assessment must cover the three hundred and sixty-five (365) days following the First Third-Party Assessment.

(f) The findings of the First Third-Party Assessment must be documented in an individual report (the "First Third-Party Assessor's Report"). The First Third-Party Assessor's Report must, to the extent possible with a Reasonable effort:

i. Identify the specific administrative, technical, and physical safeguards maintained by T-Mobile;

ii. Document the extent to which the identified administrative, technical and physical safeguards are Reasonable considering T-Mobile's size and complexity, the nature and scope of T-Mobile's activities, and the sensitivity of the Covered Information maintained by T-Mobile on the T-Mobile Network;

iii. Assess and certify the extent to which the administrative, technical, and physical safeguards that have been maintained by T-Mobile Reasonably meet the requirements of the Information Security Program; and

iv. Specifically review and evaluate T-Mobile's compliance with the requirements set forth in Paragraphs 35, 36, 37(a) – (b); 37(c)(i) – (ii); 37(c)(iv) – (vii); 37(d), 37(e)(i) – (ii); 37(e)(iv); 37(f) – (l); 38, 39, 40, 42 – 43 of this Consent Decree regarding the Information Security Program.

(g) The findings of the Second Third-Party Assessment must also be documented in an individual report (the "Second Third-Party Assessor's Report"). The Second Third-Party Assessor's Report must, to the extent possible with a Reasonable effort, specifically review and evaluate T-Mobile's compliance with the requirements set forth in Paragraphs 37(c)(iii) and 37(e)(iii) of this Consent Decree.

(h) T-Mobile must provide a copy of each Third-Party Assessor's Report to the Bureau within thirty (30) days of the completion of the Third-Party Assessment. The Bureau shall, to the extent permitted by applicable laws and regulations, treat each Third-Party Assessor's Report as confidential and exempt from disclosure under the relevant public records laws.

(i) To the extent that a Third-Party Assessor's Report purports to identify any areas of non-compliance, T-Mobile will have ninety (90) days from the date of the report's receipt to identify any objections related thereto. In the event of any such objections, T-Mobile's compliance obligations will be considered satisfied upon the delivery of a written explanation to the Bureau of the good-faith basis for the objections.

(j) No penalties, remedies, or actions for noncompliance with this Consent Decree will be exercised by the Bureau, provided that:

i. The noncompliance has not caused harm to Consumers;

ii. T-Mobile develops a compliance plan to remediate any purported areas of noncompliance to which T-Mobile has not objected;

iii. That compliance plan is developed and implemented within a Reasonable period of time; and

iv. The compliance plan is reviewed and remediation is timely verified to Reasonably address the area of noncompliance by the Third-Party Assessor.

(k) In connection with each Third-Party Assessment, T-Mobile must take Reasonable steps to:

i. Provide or otherwise make available to the Third-Party Assessor all information and material in its possession, custody, or control that is relevant and proportional to the Third-Party Assessment for which there is no claim of privilege;

ii. Provide or otherwise make available to the Third-Party Assessor information about the information technology assets deemed within the scope of the Third-Party Assessment; and

iii. Disclose material facts to the Third-Party Assessor, and not intentionally misrepresent any fact material to the Third-Party Assessment.

42. **Reporting Noncompliance**.

(a) T-Mobile shall report any material noncompliance with the terms of this Consent Decree within thirty (30) calendar days after discovery of such noncompliance, if

such noncompliance cannot be remedied or otherwise addressed after such discovery.

(b) All reports of material noncompliance shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 45 L Street NE, Washington, DC 20554, with a copy submitted electronically to Michael.Epshteyn@fcc.gov, James.Graves@fcc.gov, Shana.Yates@fcc.gov, and EB-TCD-Privacy@fcc.gov.

(c) No penalties, remedies, or actions for reported material noncompliance with the terms of this Consent Decree will be exercised by the Bureau, provided that:

i. The noncompliance has not caused harm to Consumers; and

ii. T-Mobile has a Reasonable compliance plan in place to achieve compliance and Reasonably executes such plan.

43. **Recordkeeping**.

(a) T-Mobile must retain the reports, records, and information required by this Consent Decree for three (3) years from the date of their creation or receipt. Upon sufficient prior written request of the Bureau, T-Mobile shall make available any reports, records, or information maintained pursuant to this Section. Such records shall include:

i. The index of documents required to be maintained pursuant to Paragraph 37(a)(ii);

ii. The documentation of prospectively-opened ports required to be created pursuant to Paragraph 37(c)(iii);

iii. The attestations required to be made by business owners of databases pursuant to Paragraph 37(g)(iii)(B);

iv. The Risk Assessments required to be documented pursuant to Paragraph 37(l);

v. The logs of removed Critical Assets required to be maintained pursuant to Paragraph 37(i)(ii); and,

vi. The Forensic Reports required to be created pursuant to Paragraph 39.

(b) Nothing contained herein shall directly or indirectly in any way whatsoever impair, prejudice, or otherwise adversely affect T-Mobile's right at any time to exercise attorney-client privilege, work product privilege, or any other applicable privilege, doctrine, or immunity.

44. **Termination Date**. The requirements set forth in this Consent Decree shall expire three (3) years after the Effective Date.

45. **Civil Penalty**. T-Mobile will pay a civil penalty to the United States Treasury in the amount of $15,750,000 within thirty (30) calendar days of the Effective Date. T-Mobile acknowledges and agrees that upon execution of this Consent Decree, the Civil Penalty shall become a "Claim" or "Debt" as defined in 31 U.S.C. § 3701(b)(1).[56] Upon an Event of Default, all procedures for collection as permitted by law may, at the Commission's discretion, be initiated. T-Mobile shall send electronic notification of payment to EB-TCD-Privacy@fcc.gov on the date said payment is made. Payment of the Civil Penalty must be made by credit card using the Commission's Registration System (CORES) at https://apps.fcc.gov/cores/userLogin.do, ACH (Automated Clearing House) debit from a bank account, or by wire transfer from a bank account. The Commission no longer accepts Civil Penalty payments by

[56] Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, 110 Stat. 1321, 1358 (Apr. 26, 1996).

check or money order. Below are instructions that payors should follow based on the form of payment selected:[57]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. In the OBI field, enter the FRN(s) captioned above and the letters "FORF". In addition, a completed Form 159[58] or printed CORES form[59] must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 or CORES may result in payment not being recognized as having been received. When completing FCC Form 159 or CORES, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[60] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the CD Acct. No. The bill number is the CD Acct. No. with the first two digits excluded (e.g., CD 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.

46. Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the CD Acct. No. The bill number is the CD Acct. No. with the first two digits excluded (e.g., CD 1912345678 would be associated with FCC Bill Number 12345678). Finally, choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

47. **Cybersecurity Investment**. T-Mobile will invest $15,750,00 in additional incremental spend for data security and related technology and operations during the first two years covered by this consent decree to implement the requirements of this Consent Decree. Such spending will be used on, but is not limited to the following Consent Decree provisions: § III (Terms of Agreement), ¶ 37 (Information Security Program), (c) (Segmentation), ii (documentation relating to prospectively opened ports); § III (Terms of Agreement), ¶ 37 (Information Security Program), (e) Account and Password Management); iii (secure storage of administrative-level passwords); § III (Terms of Agreement), ¶ 37 (Information Security Program), (g) (Data Retention, Minimization, and Deletion), iii (covered information minimization), B (business owner attestations). T-Mobile shall Reasonably memorialize its investment

[57] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6).

[58] FCC Form 159 is accessible at https://www.fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159.

[59] Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form 159. CORES is accessible at https://apps.fcc.gov/cores/userLogin.do.

[60] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

pursuant to this paragraph and shall provide a declaration to that effect to the Bureau upon written request.

48. **Event of Default.** T-Mobile agrees that an Event of Default shall occur upon the failure by T-Mobile to pay the full amount of the Civil Penalty on or before the due date specified in this Consent Decree.

49. **Interest, Charges for Collection, and Acceleration of Maturity Date**. After an Event of Default has occurred under this Consent Decree, the then unpaid amount of the Civil Penalty [*or any Installment Payment*] shall accrue interest, computed using the U.S. Prime Rate in effect on the date of the Event of Default plus 4.75%, from the date of the Event of Default until payment in full. Upon an Event of Default, the then unpaid amount of the Civil Penalty [*or any Installment Payment*], together with interest, any penalties permitted and/or required by the law, including but not limited to 31 U.S.C. § 3717 and administrative charges, plus the costs of collection, litigation, and attorneys' fees, shall become immediately due and payable, without notice, presentment, demand, protest, or notice of protest of any kind, all of which are waived by T-Mobile.

50. **Waivers**. As of the Effective Date, T-Mobile waives any and all rights it may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this Consent Decree and the Adopting Order. T-Mobile shall retain the right to challenge Commission interpretation of the Consent Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the Consent Decree or the Adopting Order, neither T-Mobile nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and T-Mobile shall waive any statutory right to a trial *de novo*. T-Mobile hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act[61] relating to the matters addressed in this Consent Decree.

51. **Severability**. The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

52. **Invalidity**. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

53. **Subsequent Rule, Order, Law, or Regulation**. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or order adopted by the Commission (except an order specifically intended to revise the terms of this Consent Decree to which the Company does not expressly consent), or any federal law or regulation, that provision will be superseded by such Rule, order, law, or regulation.

54. **Successors and Assigns**. T-Mobile agrees that the provisions of this Consent Decree shall be binding on its successors, assigns, and transferees.

55. **Final Settlement**. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigation. The Parties further agree that this Consent Decree does not constitute either an adjudication on the merits or a factual or legal finding regarding any compliance or noncompliance with the requirements of the Communications Laws. This Consent Decree shall not be used as evidence or precedent in any action or proceeding, except an action to enforce this Consent Decree.

56. **Modifications**. This Consent Decree cannot be modified without the advance written consent of both Parties.

[61] *See* 5 U.S.C. § 504; 47 CFR §§ 1.1501–1.1530.

57. **Paragraph Headings**. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

58. **Authorized Representative**. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

59. **Counterparts**. This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

_____
Loyaan A. Egal
Chief
Enforcement Bureau

_____
Date

_____
Edward Smith
Senior Vice President for Government Affairs
T-Mobile

_____
Date