IN ARBITRATION BEFORE THE AMERICAN ARBITRATION ASSOCIATION

Case No.:

[redacted] [redacted] an individual;

Claimant,

v.

T-MOBILE USA, INC., a Delaware corporation;

Respondent.

_____/

STATEMENT OF CLAIM

Claimant [redacted] [redacted] an individual ("Claimant" or "[redacted] by and through undersigned counsel, hereby brings the following Statement of Claim against T-MOBILE USA, INC., a Delaware corporation ("Respondent" or "T-MOBILE"), for damages and for equitable relief. In support thereof, Claimant alleges as follows:

PRELIMINARY STATEMENT

1. This action is brought by Claimant, a T-MOBILE customer who lost hundreds of thousands of dollars in an incident of a rapidly-emerging identity theft crime: "SIM swapping" or "SIM hijacking."

2. A subscriber identity module, widely known as a "SIM card," stores user data in phones on the Global System for Mobile (GSM) network -- the radio network used by T-MOBILE to provide cellular telephone service to its subscribers.

3. SIM cards are principally used to authenticate cellphone subscriptions; as without a SIM card, GSM phones are not able to connect to T-MOBILE's telecommunications network.

4. Not only is a SIM card vital to using a phone on the T-MOBILE network, the SIM card also holds immeasurable value as a tool to identify the user of the phone -- a power that can be corrupted to steal the identity of that user.

5. According to the U.S. Federal Trade Commission (FTC), there were 1,038 reported incidents of SIM swap identity theft in January 2013. By January 2016, that number had ballooned to 2,658. However, those numbers represent just a small fraction of the actual incidents of SIM swap identity theft, as data from the Identity Theft Supplement to the 2014 National Crime Victimization Survey conducted by the U.S. Department of Justice suggests that less than one percent (1%) of identity theft victims reported the theft to the FTC.

6. On its website, T-MOBILE expressly acknowledges that T-MOBILE customers "*have a right, and T-Mobile has a duty, to protect the confidentiality of your account information.*" T-MOBILE further states on its website: "*We take this obligation seriously and do everything possible to ensure that your account information is not shared with others without your consent.*" Those statements are consistent with T-MOBILE's duties and obligations under the Federal Communications Act of 1934 and the pertinent implementing regulations.

7. Moreover, T-MOBILE was well aware of the pervasive harm posed by SIM swapping, as T-MOBILE sent a mass text in February 2018 warning customers of the "industry-wide" threat and assuring those customers that T-MOBILE was exercising adequate measures to prevent unauthorized SIM swapping from happening to its accountholders.

8. Notwithstanding T-MOBILE's knowledge of the prevalence of SIM swapping and its assurance that it was actively protecting its customers, those measures did not adequately protect Claimant from the harm he suffered. **In fact, T-MOBILE affirmatively conceded to Claimant that despite those measures, it erroneously effectuated multiple SIM swaps on Claimant's T-MOBILE account.**

9. As a result of T-MOBILE's failures if not active participation in SIM swap theft that was inflicted upon him, Claimant has had over Four Hundred Thousand Dollars ($400,000.00) of assets stolen from him.

10. Claimant seeks compensatory and equitable relief restoring to him the assets and funds that were illegally taken from him.

GENERAL ALLEGATIONS

THE PARTIES

Claimant

11. Claimant [redacted] ("[redacted] is an individual domiciled in [redacted], New Jersey and is *sui juris*. Since in or about June 2016, [redacted] has been an accountholder and subscriber with T-MOBILE.

Respondent

12. Respondent T-MOBILE USA, INC. is a Delaware for-profit corporation which lists its principal place of business in Bellevue, Washington. T-MOBILE USA, INC. is the United States operating entity of T-Mobile International A.G. & Co., the mobile communications subsidiary of Deutsche Telekom AG & Co. K.G. T-MOBILE provides wireless service to subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands.

Other Liable Persons/Entities

13. In addition to the entity set forth as Respondent herein, there are likely other parties who may well be liable to Claimant, but respecting whom Claimant currently lacks specific facts to permit him to name such person or persons as a party defendant. By not naming such persons or entities at this time, Claimant is not waiving his right to amend this pleading to add such parties, should the facts warrant adding such parties.

JURISDICTION AND VENUE

14. The American Arbitration Association ("AAA") has jurisdiction over this matter and over Respondent pursuant to the Terms and Conditions to which Claimant was required to subscribe in connection with opening and maintaining his account at T-MOBILE (the "T-MOBILE T&C"). Specifically, the T-MOBILE T&C provides, in pertinent part:

> **Dispute Resolution and Arbitration. YOU AND WE EACH AGREE THAT, EXCEPT AS PROVIDED BELOW, ANY**

> **AND ALL CLAIMS OR DISPUTES IN ANY WAY RELATED TO OR CONCERNING THE AGREEMENT, OUR PRIVACY POLICY, OUR SERVICES, DEVICES OR PRODUCTS, INCLUDING ANY BILLING DISPUTES, WILL BE RESOLVED BY BINDING ARBITRATION OR IN SMALL CLAIMS COURT.** * * *
>
> **If the arbitration provision applies or you choose arbitration to resolve your disputes, then either you or we may start arbitration proceedings.** * * * The arbitration of all disputes will be administered by the American Arbitration Association ("AAA") under its Consumer Arbitration Rules in effect at the time the arbitration is commenced.

(Emphasis in original).

15. The T-MOBILE T&C further provides: "Arbitration or court proceedings must be in the county and state in which your billing address in our records is located, but not outside the U.S.; or Puerto Rico." Therefore, the instant proceeding must be conducted in [redacted], New Jersey, which is where Claimant's billing address (and his residence) is.

16. A full and complete copy of the T-MOBILE T&C in effect at the time this arbitration is commenced is attached hereto as **Exhibit "A"**.

FACTUAL ALLEGATIONS APPLICABLE TO ALL COUNTS

T-Mobile's Business and Customer Assurances

17. T-MOBILE markets and sells wireless telephone service through standardized wireless service plans at various retail locations, online, and over the telephone.

18. In connection with its wireless services, T-MOBILE maintains wireless accounts enabling its customers to have access to information about the services they purchase from T-MOBILE.

19. It is widely recognized that mishandling of customer wireless accounts can facilitate identify theft and related consumer harms.

20. Among other things, T-MOBILE's sales and marking materials state: "*We have implemented various policies and measures to ensure that our interactions are with you or those you authorize to interact with us on your behalf – and not with others pretending to be you or claiming a right to access your information.*"

21. T-MOBILE's sales and marking materials further state that, unless T-MOBILE can verify the caller's identity through certain personal information or a PIN if requested by the customer, T-MOBILE's policy is not to release any account-specific information.

22. Despite these statements and other similar statements, T-MOBILE fails to provide reasonable and appropriate security to prevent unauthorized access to customer accounts.

23. Under T-MOBILE's procedures, an unauthorized person -- including T-MOBILE's own agents and employees acting without the customer's permission -- can easily impersonate the identity of the accountholder and then access and make changes to all the information that a legitimate customer could access and to which the customer could make changes if the customer were so authorized. For example, a simple Google search may reveal the information used to verify the identity of an accountholder, such as an address, zip code, telephone number, and/or email address.

24. As set forth in this Statement of Claim, T-MOBILE also fails to disclose or discloses misleadingly that its automated processes or human performances often fall short of its express and implied representations or promises.

How SIM Swapping Works

25. "SIM swapping," or "SIM hijacking" is a growing crime in the telecommunications world that requires little more than a thorough Google search, a willing telecommunications carrier representative, and an electronic or in-person impersonation of the victim.

26. To perpetrate the theft, T-MOBILE allows an unauthorized person access to a wireless telephone account without the knowledge of the account holder.

27. Typically, the theft begins when an unauthorized person contacts T-MOBILE's technical support department on the phone, or walks into a T-MOBILE store, pretending to be the accountholder.

28. Claiming that he wants to activate a "new" phone, the thief convinces T-MOBILE to create a new SIM card to install in the thief's "new" phone.

29. Whether acting as a co-conspirator to the theft or through abject negligence, T-MOBILE then transfers (or "ports") to the unauthorized person the T-MOBILE accountholder's wireless telephone number -- disconnecting the telephone number from the actual T-MOBILE accountholder's wireless phone's SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

30. From there, the victim loses T-MOBILE service, given that only one SIM card can be connected to T-MOBILE's network with any given telephone number at a time.

31. The thief then attempts to gain entry into the victim's email accounts by entering the victim's email address on Outlook, Gmail, or any other email provider, selecting the "Forgot Password" option, and then receiving a text message intended for the accountholder with a password reset code. Once inside the victim's email account, the thief then scours information stored on the victim's email account. The thief may also search for information stored on the victim's wireless phone -- which has been wirelessly delivered to him by T-MOBILE -- to find information such as passwords or other identifying information that would grant the thief access into the victim's e-mail, banking, and investment accounts.

32. Additionally, using the victim's T-MOBILE telephone number, the thief then diverts to himself access to the victim's banking and investment accounts by using the victim's T-MOBILE telephone number as a "recovery method" -- even if the victim had two-factor authentication activated as a security measure on his accounts.

T-Mobile's Statutory Obligation to Protect Customers' Personal Information

33. As a common carrier, T-MOBILE is obligated to protect the confidential personal information of its customers under Section 222 of the FCA [47 U.S.C. § 222].

34. Section 222(a) [47 U.S.C.§ 222(a)] provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers . . . ." The "confidential proprietary information" referred to in Section 222(a), is abbreviated herein as "CPI."

35. Section 222(c) [47 U.S.C. § 222(c)] additionally provides that:

> [e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

The "customer proprietary network information" referred to in Section 222(c) is abbreviated herein as "CPNI."

36. Section 222(h)(1) [47 U.S.C. § 222(h)(1)] defines CPNI as: "(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, except that term does not include subscriber list information."

37. The FCC has promulgated rules to implement Section 222 "to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or

disclosure of CPNI." *See*, 47 CFR § 64.2001 *et seq.* ("CPNI Rules"); CPNI Order, 13 FCC Rcd. at 8195 ¶ 193. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited circumstances (such as cooperation with law enforcement), none of which are applicable to the facts here. 47 CFR § 64.2005.

38. The CPNI Rules require carriers to implement safeguards to protect customers' CPNI. These safeguards include: (i) training personnel "as to when they are and are not authorized to use CPNI"; (ii) establishing "a supervisory review process regarding carrier compliance with the rules;" and (iii) filing annual compliance certificates with the FCC. 47 CFR § 64.2009(b), (d), and (e).

39. The CPNI Rules further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals. 47 CFR § 64.2010. For example, "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 CFR § 64.2010(a). Moreover, "carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit." *Id.* In the case of in-store access to CPNI, "[a] telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information." 47 CFR § 64.2010(d) (emphasis added). "Valid photo ID" is defined in 47 CFR § 64.2003(r) as "a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired."

40. More than a decade ago, the FCC was already aware that there was "a substantial need to limit the sharing of CPNI with others" because "[t]he black market for CPNI has grown exponentially with an increased market value placed on obtaining this data, and there is concrete evidence that the dissemination of this private information does inflict specific and significant harm on individuals, including harassment and the use of the data to assume a customer's identity." *See*,

In the Matter of Implementation of the Telecommunications Acts of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 FCC Rcd. 6927 (2007) ("**Pretexting Order**"), at Pg. 22 ¶39. The FCC referred to obtaining CPNI from customers through common social engineering ploys as "pretexting." Pretexting is "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records." *Id.*, at 6927 n. 1. Such "call detail" and "private communications" are CPI and CPNI under the FCA. *Id.* at 6928 *et seq.* The FCC concluded that "pretexters have been successful at gaining unauthorized access to CPNI" and that "carriers' record on protecting CPNI demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI." *Id.* at 6933. The FCC modified its rules to impose additional security for carriers' disclosure of CPNI and to require that law enforcement and customers be notified of security breaches involving CPNI. *Id.* at 6936-62.

41. In its Pretexting Order, the FCC stated that it "fully expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information." *Id.* at 6959, ¶ 64. The FCC further stated that "[w]e decline to immunize carriers from possible sanction for disclosing customers' private information without appropriate authorization." *Id.* at 6960, ¶ 66.

42. In a statement directly relevant to the facts alleged below, the FCC also stressed the fact that someone having obtained information fraudulently is strong evidence of the carrier's failure to satisfy the requirements of section 222. The FCC stated that "we hereby put carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer's CPNI that the carrier did not sufficiently protect that customer's CPNI. A carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue." *Id.* at 6959, ¶ 63 (emphasis added).

43. As further alleged below, T-MOBILE violated Section 222 of the FCA and the CPNI Rules and ignored the warning in the Pretexting Order on or before May 23, 2018, when its employees provided hackers with Claimant's SIM cards containing or allowing access to Claimant's personal information, including CPI and CPNI, without Claimant's authorization or permission and without requiring that the individual accessing Claimant's account present valid identification or comply with T-MOBILE's own procedures.

T-Mobile's Own Privacy Policy, Code of Business Conduct, and CPNI Policy Acknowledge T-Mobile's Obligations to Its Customers' Privacy and Security

44. In its Privacy Statement ("**Privacy Policy**")[1], its Code of Business Conduct ("**COBC**")[2], and in its Customer Proprietary Network Information Policy ("**CPNI Policy**")[3], T-MOBILE acknowledges its responsibilities to protect customers' "Personal Information" under the FCA, the CPNI Rules, and other regulations.

45. In its Privacy Policy, COBC, and CPNI Policy, T-MOBILE makes binding promises and commitments to Claimant, as its customer, that it will protect and secure his "Personal Information." The Privacy Policy defines "Personal Information" as "[i]nformation that we directly associate with a specific person or entity (for example, name; address; telephone numbers; e-mail address; Social Security Number; call records; wireless device location)." T-MOBILE states that, among the information that it collects from and about its customers, are "your name, address,

[1] *See*, https://www.t-mobile.com/website/privacypolicy.aspx, a true and correct copy of which is attached hereto as **Exhibit "B"**.

[2] *See*, http://investor.t-mobile.com/Cache/1500087866.PDF?O=PDF&T=&Y=&D=&FID=1500087866&iid=4091145, a true and correct copy of which is attached hereto as **Exhibit "C"**.

[3] *See*, https://www.t-mobile.com/responsibility/privacy/resources/cpni, a true and correct copy of which is attached hereto as **Exhibit "D"**.

telephone number, e-mail address" along with CPNI and service-related details such as payment history, security codes, service history, and similar information.

46. T-MOBILE also collects information relating to the use of its networks, products and services. "Personal Information" thus includes both CPI and CPNI under Section 222 of the FCA and the CPNI Rules.

47. In its Privacy Policy, T-MOBILE states: "We use a variety of physical, electronic, and procedural safeguards to protect Personal Information from unauthorized access, use, or disclosure while it is under our control."

48. Similarly, in its CPNI Policy, T-MOBILE promises that it "is committed to protecting the privacy and security of our customers' personal information and, as set forth in our Privacy Statement, we strive to be a leader in protecting all such personal information."

49. The T-MOBILE CPNI Policy further states:

> Although federal law has long-required telecommunications carriers to protect CPNI, in an Order released on April 2, 2007, the Federal Communications Commission ("FCC") issued revised and expanded CPNI rules in response to several high-profile incidents involving the activities of "data brokers" and "pretexters" who attempt to obtain unauthorized access to such information. **These rules became effective December 8, 2007[;] and T-Mobile has implemented polices and safeguard procedures to help ensure compliance.** T-Mobile continually reviews its compliance with such rules and annually certifies compliance to the FCC.

(emphasis added).

50. T-MOBILE's COBC also makes binding commitments to Claimant, as a T-MOBILE customer, that it will protect his Personal Information and that it will adhere to all its legal obligations. Those legal obligations include, by implication, Section 222 of the FCA, the CPNI Rules, and other legal obligations that govern protection of confidential and private information.

51. For example, T-MOBILE's COBC provide:

- "Customers entrust a lot of sensitive information to us -- credit card numbers, Social Security numbers, addresses, all sorts of things. * * * Here's the thing: We protect the confidentiality of our customers' information."

- "When it comes to customer information, we're also careful about access and disclosure: We access this information only when we need to when doing our job -- and only to the extent our job duties allow. * * * We share customer information only if the customer says we can or we're allowed to by the law, our Terms & Conditions, or Privacy policies."

52. As alleged herein, T-MOBILE flagrantly and repeatedly violated its commitments to Claimant in its Privacy Policy, COBC, and CPNI Policy, as well as its legal obligations under the FCA, the CPNI Rules, and other laws, by willingly turning over to hackers Claimant's wireless number that allowed hackers to access his "Personal Information" including CPNI.

T-Mobile Failed to Fulfill Its Statutory and Self-Acknowledged Duties -- Exposing Claimant to a SIM Swap and Theft of More Than $400,000.00 of His Assets

53. In the instant matter, T-MOBILE -- whether acting as a co-conspirator to the theft or through abject negligence -- transferred to a hacker Claimant's T-MOBILE telephone number, which led to the swift theft of more than Four Hundred Thousand Dollars ($400,000.00) in cryptocurrency assets from Claimant in or about May 2018.

54. On or about May 23, 2018, an unauthorized person contacted T-MOBILE and posed as Claimant to orchestrate a SIM swap.

55. Without properly verifying the person's identification, a T-MOBILE representative (Elias Polanco) transferred to the unauthorized person Claimant's wireless telephone number -- disconnecting the telephone number from Claimant's wireless phone's SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

56. On or about May 23, 2018, Claimant noticed that his cell phone was unable to connect to the T-MOBILE cellular network.

57. When Claimant contacted T-MOBILE to discuss the problem with his service, Claimant was informed that his SIM card had been switched remotely without his authorization by T-MOBILE representative Elias Polanco.

58. At Claimant's request, T-MOBILE changed the SIM card number back to Claimant's cell phone, restoring the phone service.

59. T-MOBILE also assured Claimant at that time that additional security measures would be implemented on Claimant's T-MOBILE account to prevent future unauthorized activity or SIM card swapping. Claimant was told by T-MOBILE that he would be afforded the highest level of security on his account and that no porting would be allowed unless the person making the request were fully vetted with proper identification.

60. Claimant relied upon T-MOBILE's promises that his account would be much more secure against hacking, including SIM swap fraud, after it implemented the increased security measures. Because of the implementation of such measures, Claimant retained his account with T-MOBILE.

61. But for these express promises and assurances, Claimant would have canceled his T-MOBILE account and contracted with a different cellular telephone provider.

62. On or about June 1, 2018, Claimant again noticed that he did not have the T-MOBILE service for which he had subscribed on his cell phone.

63. On or about that date, Claimant also noticed that the password to his e-mail account had been changed.

64. When Claimant contacted T-MOBILE to discuss the problem with his service, Claimant was informed that his SIM card had again been switched without his authorization by a T-MOBILE employee.

65. On this occasion, the switch took place at a T-MOBILE store in Avondale, Arizona when an imposter pretended to be Claimant's father.

66. The second SIM card switch was effectuated by a T-MOBILE representative named David Grande.

67. Upon further investigation, Claimant then learned that his cryptocurrency wallet and his accounts at several major cryptocurrency exchanges had been compromised following the first unauthorized SIM card swap done by T-MOBILE.

68. Specifically, the following assets were stolen from Claimant between May 23, 2018 and May 28, 2018 as a direct and proximate result of T-MOBILE's acts and omissions:

Date of Theft	Location from which Assets were Stolen	Cryptocurrency Assets Stolen	Approximate Value of Funds/Assets Stolen[4]
May 23, 2018	Ledger Nano S	568.863 Ether	$369,760.00
May 23, 2018	Ledger Nano S	0.7902744 bitcoin	$6,338.00
May 23, 2018	Ledger Nano S	30.41 ZCash	$10,187.00
May 23, 2018	Poloniex exchange	21.7548 Ether	$14,140.00
May 23, 2018	Poloniex exchange	20.5476 Monero	$3,678.00
May 28, 2018	Ledger Nano S	101.137 OmiseGo	$1,072.00
		TOTAL	$405,175.00

69. The theft from Claimant would not have occurred but for T-MOBILE's failure to adequately protect his T-MOBILE account and maintain proper security measures to prevent the unauthorized SIM swaps that took place.

70. In the course of a series of e-mail exchanges between Claimant and T-MOBILE's Business Care department on June 20, 2018, **a T-MOBILE Business Care representative (Michael**

[4] Valuation of the stolen funds/assets is determined as of the date of the theft. *See* www.coinmarketcap.com.

Fitzpatrick) conceded to Claimant that T-MOBILE's records show that "the previous SIM swaps were done in error by our sales team."

71. By its procedures, practices, and regulations, T-MOBILE engages in practices that, taken together, fail to provide reasonable and appropriate security to prevent unauthorized access to its customer wireless accounts, allowing unauthorized persons to be authenticated and then granted access to sensitive customer wireless account data.

72. In particular, T-MOBILE has failed to establish or implement reasonable policies, procedures, or regulations governing the creation and authentication of user credentials for authorized customers accessing T-MOBILE accounts, creating unreasonable risk of unauthorized access. As such, at all times material hereto, T-MOBILE has failed to ensure that only authorized persons have such access and that customer accounts are secure.

73. Among other things, T-MOBILE:

(a) fails to establish or enforce rules sufficient to ensure only authorized persons have access to T-MOBILE customer accounts;

(b) fails to establish appropriate rules, policies, and procedures for the supervision and control of its officers, agents, or employees;

(c) fails to establish or enforce rules, or provide adequate supervision or training, sufficient to ensure that all its employees or agents follow the same policies and procedures. For example, it is often possible to persuade one of T-MOBILE agents to not apply the stated security policy and allow unauthorized access without providing a PIN. Similarly, on information and belief, T-MOBILE agents or employees generally act on their own regardless of what is in the notes of a customer account, failing, among other things, to accommodate customers' security requests;

(d) to adequately safeguard and protect its customer wireless accounts, including that of Claimant, so wrongdoers were able to obtain access to his account;

(e) permits the sharing of and access to user credentials among T-MOBILE's agents or employees without a pending request from the customer, thus reducing likely detection of, and accountability for, unauthorized accesses;

(f) fails to suspend user credentials after a certain number of unsuccessful

access attempts. For example, wrongdoers would call numerous times trying to gain access to customer accounts before they finally got an agent on the line that would authorize access without requiring, for example, a PIN;

(g) fails to adequately train and supervise its agents and employees in such a manner that allows its agents or employees, without authorization or approval, to unilaterally access and make changes to customer accounts as if the customer were so authorized;

(h) allows porting out of phone numbers without properly confirming that the request is coming from the legitimate customers;

(i) lacks proper monitoring solutions and thus fails to monitor its systems for the presence of unauthorizes access in a manner that would enable T-MOBILE to detect the intrusion so that the breach of security and diversion of customer information was able to occur in Claimant's situation and continue until after his virtual currency account was compromised;

(j) fails to implement simple, low-cost, and readily-available defenses to identity thieves such as delaying transfers from accounts on which the password was recently changed or simply delaying transfers from accounts to allow for additional verifications from the customers; and

(k) fails to build adequate internal tools to help protect its customers against hackers and account takeovers, including compromise through phone porting and wrongdoing by its own agents or employees acting on their own behalf or on behalf or at the request of a third party.

74. By the security practices and procedures described here, T-MOBILE established user credential structures that created an unreasonable risk of unauthorized access to customer accounts, including that of Claimant.

75. Upon information and belief, T-MOBILE has long been aware about the security risks presented by, *inter alia*, its weak user credential structures or procedures. From prior attacks on customer accounts, T-MOBILE has long had notice of those risks. For example, the FCC published its Pretexting Order in 2007, the FTC's Chief Technologist published, "Your mobile phone account could be hijacked by an identity thief," in June 2016, and *Forbes* published an article about SIM swapping in December 2016. Nevertheless, T-MOBILE still does not use readily-available security measures to prevent or limit such attacks.

76. As a result of T-MOBILE's faulty security practices, an attacker could easily gain access to a customer's account and then use it to gain access to the customer's sensitive information such as bank accounts or virtual currency accounts, among other things.

77. As such, T-MOBILE's security measures were entirely inadequate to protect its customers, including Claimant.

78. Lack of adequate security in T-MOBILE's systems, practices, or procedures enabled the wrongdoers to access Claimant's wireless account, which then enabled the wrongdoers to access his virtual currency account and possibly other sensitive information.

79. As such, T-MOBILE failed the responsibility it owed to Claimant to protect his account and his phone number. Even if the subject incident was due to an "inside" job or human performance falling short, T-MOBILE is responsible for its agents. And, while T-MOBILE can outsource customer service functions, T-MOBILE cannot transfer accountability.

80. Had T-MOBILE provided adequate account security or exercised reasonable oversight, Claimant would not have lost his phone number or otherwise been damaged.

81. As a result of the foregoing acts, errors, and omissions by T-MOBILE, Claimant has been damaged in an amount that will be proven at trial.

82. Claimant has duly performed all of his duties and obligations, and any conditions precedent to Claimant bringing this action have occurred, have been performed, or else have been excused or waived.

83. To enforce his rights, Claimant has retained undersigned counsel and is obligated to pay counsel a reasonable fee for its services, for which T-MOBILE is liable as a result of its bad faith and otherwise.

COUNT I – DECLARATORY JUDGMENT (UNENFORCEABILITY OF T-MOBILE CONSUMER AGREEMENT AS UNCONSCIONABLE AND CONTRARY TO PUBLIC POLICY)

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

84. Claimant brings this claim for declaratory relief under 28 U.S.C. § 2201 to have the Panel declare that T-MOBILE's wireless customer agreement set forth in the T-MOBILE T&C (the "Agreement") is unconscionable, void against public policy, and unenforceable in its entirety.

85. The Agreement was presented to Claimant, like all other wireless users, on a take-it-or-leave-it basis. Claimant had no ability to negotiate any term of the agreement. In contrast, T-MOBILE has virtually unlimited power over its customers, including Claimant, as seen below by the fact that it purports to hold Claimant and all other wireless users to the terms of an agreement that they may well have never seen or read.

86. The version of the Agreement posted in September 2017 (which was in effect when Claimant suffered the SIM swaps detailed herein) purports to govern T-MOBILE's provision of wireless service to all customers, including Claimant.

87. The Agreement contains numerous unconscionable terms that renders it unenforceable in its entirety because its central purpose is tainted with illegality.

88. The Agreement states that it includes not only the T-MOBILE T&C but also "the additional terms found in your Rate Plan, your Data Plan, your Service Agreement, and provisions linked to from these T&C." The Agreement further obliquely references the applicability of T-MOBILE's Privacy Policy and Open Internet Policy.

89. Additionally, the Agreement states that T-MOBILE "may change, limit, suspend, or terminate your Service or this Agreement at any time . . . ." Through such language, T-MOBILE apparently contends that not only the Agreement, but all other agreements and terms referenced therein, bind all wireless customers, whether or not such customers have seen the Agreement or are

aware of its terms. In other words, every time (and at any time) T-MOBILE mints a new and more onerous version of its agreements, its unsuspecting customers are purportedly bound by the new terms. This practice highlights the fact that not only are these contracts not negotiable, they are invisible. What you don't see, you still get.

90. The Agreement is a classic contract of adhesion imposed by T-MOBILE upon a party with no bargaining power. In contrast, T-MOBILE has unchecked power to insist upon its own terms even if the consumer is unaware of the terms of the Agreement itself. There is no ability to negotiate any term of the Agreement. It is literally "take it or leave it."

91. The Agreement is void as against public policy as a contract of adhesion purporting to bind customers who have never heard or seen the agreement and most likely are entirely unaware of its provisions.

92. The Agreement is void and unenforceable in its entirety because it also contains exculpatory provisions, damage waivers, and an indemnification provision that purport to prevent consumers from bringing any claims against T-MOBILE obtaining redress for their claims -- even for intentional acts or gross negligence by T-MOBILE.

93. The exculpatory provision in the Agreement ("Exculpatory Provision") contains numerous provisions that are contrary to public policy because they attempt to exempt T-MOBILE from responsibility for its own gross negligence, fraud, and violations of law. In pertinent part, the Exculpatory Provision states that:

> **DISCLAIMER OF WARRANTIES:** Except for any written warranty that may be provided with a T-Mobile Device you purchase from us, and to the extent permitted by law, **the Services and Devices are provided on an "as is" and "with all faults" basis and without warranties of any kind**. We make no representations or warranties, express or implied, including any implied warranty of merchantability or fitness for a particular purpose concerning your Service or your Device. **We can't and don't promise uninterrupted or error-free service and don't authorize anyone to make any warranties on our behalf.**

* * *

> **LIMITATION OF LIABILITY: To the extent permitted by law, you and we each agree to limit claims for damages or other monetary relief against each other to direct and actual damages regardless of the theory of liability. This means that neither of us will seek any indirect, special, consequential, treble, or punitive damages from the other.**

(emphasis added).

94. The Exculpatory Provision renders the entire Agreement unenforceable on public policy grounds because it purports to exempt T-MOBILE from its gross negligence, statutory violations, and willful behavior, including the egregious conduct "with all faults" alleged herein.

95. The Exculpatory Provision is further against public policy because it purports to exempt T-MOBILE from violation of statutory obligations, including the obligation to maintain the confidentiality and security of its customers' private and personal information under Section 222 of the FCA.

96. Moreover, the Exculpatory Provision is invalid because it allocates all the risks to the consumer with T-MOBILE disclaiming numerous forms of damages for its own conduct -- even for fraud, gross negligence, and statutory violations, including those governed by the FCA.

97. Thus, even if T-MOBILE deliberately handed over a customer's CPNI to hackers in violation of Section 222 of the FCA, a customer would not be entitled to the full range of damages afforded by that statute under the Exculpatory Provision.

98. The Exculpatory Provision is contained in a lengthy form contract drafted by a domineering telecommunication provider with vast assets in a far superior bargaining position to the wireless user. Indeed, it is no exaggeration to say that the consumer has no bargaining power as regards T-MOBILE, particularly as to the Exculpatory Provision and other draconian provisions in the Agreement. Because the Exculpatory Provision is found in a document posted on a website that,

by fiat, is automatically made applicable to customers, customers may not even be aware that they have virtually no redress against T-MOBILE, unless they diligently monitor changes in the website.

99. Moreover, the Exculpatory Provision is contained in a complex and lengthy contract that provides essential wireless services -- without which most customers have no means of communication (including for emergency services), let alone essential computing, geolocation, texting, research or other services.

100. The Exculpatory Provision -- included in a contract of adhesion as to which T-MOBILE's users, including Claimant, have no bargaining authority -- is void because it is plainly unconscionable and against public policy.

101. The Exculpatory Provision is also substantively unconscionable because it allocates risks in an objectively unreasonable manner.

102. The allocation of risks under the Agreement is objectively unreasonable because T-MOBILE -- a telecommunications behemoth with billions of dollars of assets and tens of millions of customers -- takes upon itself virtually no liability and purports to exempt itself from virtually all damages, including those arising out of its own deliberate, grossly negligent, or fraudulent acts.

103. The Agreement is further unenforceable because customers are purportedly required to indemnify T-MOBILE for all claims arising out of the services provided by T-MOBILE, including claims that arise due to T-MOBILE's negligence, gross negligence, deliberate conduct, or statutory violations.

104. The indemnity provision in the Agreement ("Indemnification") states:

> **You agree to defend, indemnify, and hold us** and our directors, officers, and employees **harmless from any claims arising out of use of the Service** or Devices, **breach of the Agreement, or violation of any laws or regulations** or the rights of any third party by you, any person on your account, or any person you allow to use the Services or your Device.

(emphasis added).

105. Read literally, the Indemnification requires a consumer, such as Claimant, to hold T-MOBILE harmless for T-MOBILE's own negligence, deliberate behavior, gross negligence, statutory violations (including disclosure of CPNI under the FCA), or fraud for any conduct arising out of "use of the Service" or even T-MOBILE's "breach of the Agreement."

106. On its face, the indemnity provision in a contract of adhesion renders the entire Agreement unconscionable and unenforceable because if defeats the entire purpose of the contract by making it impossible for consumers to bring claims against T-MOBILE for the entire range of statutory rights to which a consumer, such as Claimant, is entitled.

107. Indeed, the Indemnification would totally obviate T-MOBILE's commitment to privacy in its Privacy Policy as well as its legal obligations under the FCA and the CPNI Rules.

108. Because the entire Agreement is unenforceable because the central purpose of the Agreement is tainted with illegality so that the contract as a whole cannot be enforced, the arbitration provision in the Agreement ("Arbitration Provision") is also enforceable.

109. The Arbitration Provision would require Claimant to arbitrate his claims without affording the full range of statutory remedies, including indirect, special, consequential, treble, or punitive damages that are available to him under the claims alleged herein. For example, Claimant, if required to arbitrate this claim, would be forced by the Exculpatory Provision to forego his statutory entitlement to punitive damages for T-MOBILE's fraud and negligence.

110. Moreover, the Arbitration Provision would require Claimant to forego the full range of damages to which he is entitled under his claim for relief under the Federal Communications Act § 222.

111. These defects render not only the Arbitration Provision, but also the entire Agreement, unenforceable.

112. Because the defenses raised by Claimant as to the unconscionability of the Agreement are "enforced evenhandedly" and do not "interfere[ ] with the fundamental attributes of arbitration,"

they do not run afoul of *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2010). The Court's decision in *Concepcion* did not abrogate the savings clause of the FAA that provides that arbitration agreements may be declared unenforceable "upon such grounds as exist at law or in equity for the revocation of any contract," including "generally applicable contract defenses, such as fraud, duress, or unconscionability." *Concepcion* at 339, quoting 9 U.S.C. § 2 and *Doctors Associates, Inc. v. Casarotto*, 517 U.S. 681, 687 (1996). For the reasons alleged in this claim, such defenses apply squarely to the Agreement.

113. There is an actionable and justiciable controversy between Claimant and T-MOBILE in that Claimant contends that the Agreement, including the Exculpatory Provision, Indemnification, and Arbitration Provision, is unenforceable in its entirety because it is unconscionable and void against public policy since it prevents consumers, such as Claimant, from obtaining redress against T-MOBILE even for deliberate acts in violation of its legal duties.

114. A declaration of the enforceability of the Agreement, including the Exculpatory Provision, Indemnification, and Arbitration Provision and all other provisions of the Agreement, is necessary and appropriate.

WHEREFORE, Claimant [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation declaring that the Agreement in its entirety is unenforceable as unconscionable and against public; or, in the alternative that: (a) the Exculpatory Provision is unenforceable as against Claimant; (b) the Indemnification is unenforceable as against Claimant; and (c) the Arbitration Provision is unenforceable as against Claimant. Claimant further requests entry of any and all other relief the Panel deems just and proper.

COUNT II – BREACH OF FEDERAL COMMUNICATIONS ACT [47 U.S.C. §§ 206, 222] (UNAUTHORIZED DISCLOSURE OF CUSTOMER CONFIDENTIAL PROPRIETARY INFORMATION AND PROPRIETARY NETWORK INFORMATION)

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

115. T-MOBILE is a "common carrier" engaging in interstate commerce by wire regulated by the Federal Communications Act ("FCA") and subject to the requirements, *inter alia*, of sections 206 and 222 of the FCA.

116. Under section 206 of the FCA, 47 U.S.C. § 206, "[i]n case any common carriers shall do, or cause or permit it to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney's fee, to be fixed by the court in every case of recovery, which attorney's fee shall be taxed and collected as part of the costs in the case."

117. Section 222(a) of the FCA, 47 U.S.C. § 222(a), requires every telecommunications carrier to protect, among other things, the confidentiality of proprietary information of, and relating to, customers ("CPI").

118. Section 222(c)(1) of the FCA, 27 U.S.C. § 222(c)(1) further requires that, "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to customer proprietary network information ['CPNI'] in its provision of (A) telecommunications services from which such information is derived, or (B) services necessary to or used in the provision of such telecommunication services . . . ."

119. The information disclosed to hackers by T-MOBILE in the May 23, 2018 and June 1, 2018 SIM swap frauds transferring Claimant's telephone number, was CPI and CPNI under Section 222 of the FCA.

120. T-MOBILE failed to protect the confidentiality of Claimant's CPI and CPNI, including his wireless telephone number, account information, and his private communications, by divulging that information to hackers in the May 23, 2018 and June 1, 2018 SIM swap frauds.

121. Through its negligence, gross negligence and deliberate acts, including inexplicable failures to follow its own security procedures, supervise its employees, the CPNI Regulations, the warnings of the Pretexting Order, its Privacy Policy, COBC, and CPNI Policy, and by allowing its employees to bypass such procedures, T-MOBILE permitted hackers to access Claimant's telephone number, telephone calls, text messages and account information to steal more than $400,000.00 worth of his cryptocurrency.

122. As a direct consequence of T-MOBILE's violations of the FCA, Claimant has been damaged by loss of more than $400,000.00 worth in cryptocurrency which T-MOBILE allowed to fall into the hands of thieves, and for other damages in an amount to be proven at trial.

123. Claimant is also entitled to his attorney's fees under the FCA in bringing this action against T-MOBILE for its gross negligence and fraudulent misrepresentation as to the security that it provides for customer accounts as required by the FCA and the CPNI Regulation.

WHEREFORE, Claimant [redacted] [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation; for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Panel deems just and proper.

COUNT III – BREACH OF IMPLEMENTING REGULATIONS OF FEDERAL COMMUNICATIONS ACT [47 C.F.R. § 64.2001 *et seq.*] (UNAUTHORIZED DISCLOSURE OF CUSTOMER CONFIDENTIAL PROPRIETARY INFORMATION AND PROPRIETARY NETWORK INFORMATION)

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

124. 47 C.F.R. § 64.2010(b) provides: "The purpose of the rules in this subpart is to implement section 222 of the Communications Act . . . ."

125. 47 C.F.R. § 64.2010(a) provides:

> Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. **Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI** based on customer-initiated telephone contact, online account access, or an in-store visit.

126. In addition, subpart 64.2010(b), (d), and (e) further provide:

> Telephone access to CPNI. Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, **if the customer first provides the carrier with a password**, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. **If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record**. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.
>
> * * *
>
> In-store access to CPNI. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.
>
> * * *
>
> To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information.

127. Telecommunication carriers who rely on oral directions from customers "shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part." 47 C.F.R. § 64.2007(1).

128. The information disclosed to hackers by T-MOBILE in the May 23, 2018 and June 1, 2018 SIM swap frauds transferring Claimant's telephone number was CPI and CPNI under Section 222 of the FCA.

129. T-MOBILE failed to protect the confidentiality of Claimant's CPI and CPNI, including his wireless telephone number, account information, and his private communications, by divulging that information to hackers in the May 23, 2018 and June 1, 2018 SIM swap frauds.

130. Through its negligence, gross negligence, and deliberate acts -- including inexplicable failures to follow its own security procedures, supervise its employees, the CPNI Regulations, the warnings of the Pretexting Order, its Privacy Policy, COBC, and CPNI Policy; and by allowing its employees to bypass such procedures -- T-MOBILE permitted hackers to access Claimant's telephone number, telephone calls, text messages, and account information to steal more than $400,000.00 worth of his cryptocurrency.

131. As a direct consequence of T-MOBILE's violations of the FCA, Claimant has been damaged by his loss of more than $400,000.00 worth in cryptocurrency which T-MOBILE allowed to be taken from him, and for other damages in an amount to be proven at trial.

132. Claimant is also entitled to an award reimbursing him his attorney's fees under the FCA in bringing this action against T-MOBILE for T-MOBILE's gross negligence and fraudulent misrepresentation as to the security that it provides for customer accounts as required by the FCA and the CPNI Regulation.

WHEREFORE, Claimant [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation; for damages, including

compensatory damages, punitive damages, interest, expenses, and any other relief the Panel deems just and proper.

COUNT IV – NEGLIGENCE

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

133. T-MOBILE owed a duty to Claimant to exercise reasonable care in safeguarding and protecting his Personal Information, including CPI and CPNI, and keeping it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

134. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Claimant's Personal Information, including CPI and CPNI, was adequately secured and protected.

135. T-MOBILE had a further duty to implement and adhere to the "high security" protocol that it had promised Claimant that it would place on his account to protect his Personal Information and had a duty to adhere to the FCA and the CPNI Rules.

136. T-MOBILE knew that Claimant's Personal Information, including CPI and CPNI, was confidential and sensitive.

137. Indeed, T-MOBILE acknowledged this in its Privacy Policy, COBC, and CPNI Policy and in agreeing, at Claimant's request, to place additional "high security" measures on Claimant's account to prevent hackers from committing SIM swap fraud on Claimant. T-MOBILE further promoted its "extra security" on its website.

138. T-MOBILE likewise knew that Claimant's Personal Information was vulnerable to hacks by thieves and other criminals both because it acknowledged such in its Privacy Policy, COBC, and CPNI Policy and because it had been informed by Claimant of the May 23, 2018 hack into his T-MOBILE account.

139. T-MOBILE thus knew of the substantial harms that could occur to Claimant if it did not place adequate security on his Personal Information and did not follow its own "high security" measures for the account.

140. By being entrusted by Claimant to safeguard his Personal Information, including CPI and CPNI, T-MOBILE had a special relationship with Claimant.

141. Claimant signed up for T-MOBILE's wireless services and agreed to provide his Personal Information to T-MOBILE with the understanding that T-MOBILE would take appropriate measures to protect it. But T-MOBILE did not protect Claimant's Personal Information and violated his trust.

142. T-MOBILE knew its security was inadequate.

143. T-MOBILE is morally culpable, given prior security breaches involving its own employees.

144. T-MOBILE breached its duty to exercise reasonable care in safeguarding and protecting Claimant's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain adequate security measures to safeguard that information, including its duty under the FCA, the CPNI Rules, and its own Privacy Policy, COBC, and CPNI Policy.

145. T-MOBILE's failure to comply with federal and state requirements for security further evidences T-MOBILE's negligence in failing to exercise reasonable care in safeguarding and protecting Claimant's Personal Information, including CPI and CPNI.

146. But for T-MOBILE's wrongful and negligent breach of its duties owed to Claimant, his Personal Information, including his CPI and CPNI, would not have been compromised, stolen, viewed, and used by unauthorized persons.

147. T-MOBILE's negligence was a direct and legal cause of the theft of Claimant's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of more than $400,000.00 worth of cryptocurrency.

148. The injury and harm suffered by Claimant was the reasonably foreseeable result of T-MOBILE's failure to exercise reasonable care in safeguarding and protecting Claimant's Personal Information, including his CPI and CPNI.

149. T-MOBILE's misconduct as alleged herein is malice, fraud, or oppression in that it was despicable conduct carried on by T-MOBILE with a willful and conscious disregard of the rights or safety of Claimant and despicable conduct that has subjected Claimant to cruel and unjust hardship in conscious disregard of his rights.

150. As a result, Claimant is entitled to punitive damages against T-MOBILE.

WHEREFORE, Claimant [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation; for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Panel deems just and proper.

COUNT V – NEGLIGENT MISREPRESENTATION

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

151. T-MOBILE made numerous representations and false promises in its Privacy Policy, COBC, and CPNI Policy as well as in its advertising regarding the supposed security of consumers' Personal Information, including Claimant's Personal Information

152. Moreover, T-MOBILE made numerous false representations directly to Claimant when an T-MOBILE employee induced Claimant not to cancel his service after the May 23, 2018 hack with promises of heightened security on his T-MOBILE account.

153. Such representations and promises were false because T-MOBILE was using outdated security procedures and failed to disclose that it did not adhere to its own standards, including the heightened security standards that it implemented for Claimant after the May 23, 2018 hack or the CPNI Rules.

154. T-MOBILE's misrepresentations and false promises, including those made after the May 23, 2018 hack, were material to Claimant, who reasonably relied upon those representations and promises.

155. Claimant would not have agreed to continue to use and pay for T-MOBILE's services if he had known that they were not as secure as represented by T-MOBILE and would not have lost more than $400,000.00.

156. T-MOBILE intended that Claimant rely on its representations and promises, including those made after the May 23, 2018 hack, as it knew that Claimant would not entrust his Personal Information to unreasonable security risks, particularly because Claimant had been subject to the May 23, 2018 hack.

157. In reliance upon T-MOBILE's representations and promises, Claimant continued to maintain a wireless account with T-MOBILE and to use his T-MOBILE phone number for verification and other purposes.

158. As a direct and proximate result of T-MOBILE's wrongful actions, Claimant has been damaged by paying monthly fees to T-MOBILE and having thieves steal more than $400,000.00 worth of cryptocurrency through the May 23, 2018 SIM swap fraud.

WHEREFORE, Claimant [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation; for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Panel deems just and proper.

COUNT VI – NEGLIGENT TRAINING AND SUPERVISION

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

159. T-MOBILE owed Claimant a duty to exercise reasonable care in supervising and training its T-MOBILE employees to safeguard and protect Claimant's Personal Information, including CPI and CPNI, and to keep it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

160. T-MOBILE was aware of the ability of its employees to bypass its security measures and the fact that its employees actively participated in fraud involving its customers, including pretexting and SIM card swap fraud, by bypassing such security measures.

161. T-MOBILE knew that Claimant's Personal Information, including CPI and CPNI, was confidential and sensitive.

162. By being entrusted by Claimant to safeguard his Personal Information, including CPI and CPNI, T-MOBILE had a special relationship with Claimant.

163. Claimant signed up for T-MOBILE's wireless services and agreed to provide his Personal Information to T-MOBILE with the understanding that T-MOBILE's employees would take appropriate measures to protect it.

164. T-MOBILE also made promises in the Privacy Policy, COBC, and CPNI Policy that its employees would respect its customers' privacy and that T-MOBILE would supervise and train its employees to adhere to its legal obligations to protect their Personal Information.

165. T-MOBILE breached its duty to supervise and train its employees to safeguard and protect Claimant's Personal Information, including CPI and CPNI, by not requiring them to adhere to its obligations under the CPNI Rules and other legal provisions.

166. On or about May 23, 2018 and again on or about June 1, 2018, T-MOBILE's employees facilitated SIM swap frauds on Claimant by not requiring individuals requesting Claimant's telephone number to present valid identification.

167. T-MOBILE knew its supervision and monitoring of its employees was inadequate through its knowledge from prior incidents that its employees cooperated with hackers in SIM swap fraud.

168. T-MOBILE is morally culpable, given prior security breaches involving its own employees.

169. T-MOBILE breached its duty to exercise reasonable care in supervising and monitoring its employees to protect Claimant's Personal Information, including CPI and CPNI.

170. T-MOBILE's failure to comply with the requirements of the FCA and CPNI Rules further evidence T-MOBILE's negligence in adequately supervising and monitoring its employees so that they would safeguard and protect Claimant's Personal Information, including CPI and CPNI.

171. But for T-MOBILE's wrongful and negligent breach of its duties to supervise and monitor its employees, Claimant's CPI and CPNI would not have been disclosed to unauthorized individuals through SIM swap fraud.

172. T-MOBILE's negligence was a direct and legal cause of the theft of Claimant's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of more than $400,000.00 worth of cryptocurrency.

173. The injury and harm suffered by Claimant was the reasonably foreseeable result of T-MOBILE's failure to supervise and monitor its employees in safeguarding and protecting Claimant's Personal Information, including his CPI and CPNI.

174. T-MOBILE's misconduct as alleged here is done with malice, fraud and oppression in that it was despicable conduct carried on by T-MOBILE with a willful and conscious disregard of the

rights or safety of Claimant and despicable conduct that has subjected Claimant to cruel and unjust hardship in conscious disregard of his rights. As a result, Claimant is entitled to punitive damages against T-MOBILE.

WHEREFORE, Claimant [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation; for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Panel deems just and proper.

COUNT VII – BREACH OF CONTRACT
(PRIVACY POLICY, COBC, and CPNI POLICY)

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

175. The Privacy Policy, COBC, and CPNI Policy coalesce to form a binding contract between T-MOBILE and Claimant.

176. T-MOBILE breached the contract with respect to at least the following provisions of the Privacy Policy, COBC, and CPNI Policy:

(a) T-MOBILE's promise that it will not sell or disclose users' "Personal Information" to anyone not authorized to receive that information;

(b) T-MOBILE "use[s] a variety of physical, electronic, and procedural safeguards to protect Personal Information from unauthorized access, use, or disclosure while it is under our control";

(c) T-MOBILE "is committed to protecting the privacy and security of our customers' personal information and, as set forth in our Privacy Statement, we strive to be a leader in protecting all such personal information";

(d) T-MOBILE "has implemented polices and safeguard procedures to help ensure compliance" with FCC requirements involving the activities of "data brokers" and "pretexters" who attempt to obtain unauthorized access to such information;

(e) T-MOBILE assures its accountholders: "We protect the confidentiality of our customers' information"; and

(f) T-MOBILE assures its accountholders: "We share customer information only if the customer says we can or we're allowed to by the law, our Terms & Conditions, or Privacy policies."

177. T-MOBILE also breached its Privacy Policy, COBC, and CPNI Policy by failing to follow not only the letter of the law, but the spirit of the law by failing to protect Claimant's privacy.

178. T-MOBILE breached these provisions of its Privacy Policy, COBC, and CPNI Policy by not having proper safeguards in accordance with law, including the FCA and the CPNI Rules, to protect Claimant's "Personal Information," including CPI and CPNI.

179. T-MOBILE further breached its promises by not limiting access to Claimant's Personal Information to authorized or properly-trained individuals.

180. T-MOBILE likewise violated its commitments to maintain the confidentiality and security of Claimant's Personal Information by failing to comply with its own policies and applicable law, rules, regulations, court and/or administrative orders that apply to T-MOBILE's business -- including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of T-MOBILE customer records.

181. T-MOBILE thus breached its obligations under the FCA and the CPNI Rules.

182. The May 23, 2018 SIM swap fraud was a direct and legal cause of the injuries and damages suffered by Claimant, including loss of more than $400,000.00 of crypto currency.

183. To the extent that T-MOBILE maintains that the Exculpatory Provision, Damages Restriction, and the Indemnity in the Agreement apply to the promises made by T-MOBILE in the Privacy Policy, COBC, and CPNI Policy, such provisions, as well as the Agreement in its entirety, are unenforceable and do not apply to the Privacy Policy, COBC, and CPNI Policy.

184. Moreover, such provisions are unconscionable because an entity cannot exculpate itself from its obligations to maintain the privacy and security of personal information under federal and state law.

185. Claimant was harmed due to T-MOBILE's breach of the terms of the Privacy Policy, COBC, and CPNI Policy, because his "Personal Information," including CPI and CPNI, was breached

in the May 23, 2018 (and again in the June 1, 2018) SIM swap fraud, which led to monetary losses of more than $400,000.00.

WHEREFORE, Claimant [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation; for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Panel deems just and proper.

COUNT VIII – BREACH OF IMPLIED CONTRACT

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

186. To the extent that T-MOBILE's Privacy Policy, COBC, and CPNI Policy did not form express contracts, the opening of an T-MOBILE wireless account by Claimant created implied contracts between T-MOBILE and Claimant as to the protection of his Personal Information, the terms of which were set forth by the relevant Privacy Policy, COBC, and CPNI Policy.

187. T-MOBILE breached such implied contracts by failing to adhere to the terms of the applicable Privacy Policy, COBC, and CPNI Policy.

188. Specifically, T-MOBILE violated its commitment to maintain the confidentiality and security of the Personal Information of Claimant, including CPI and CPNI, and failed to comply with its own policies and applicable law, rules, regulations, court and/or administrative orders that apply to T-MOBILE's business -- including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of T-MOBILE customer records.

189. Claimant was harmed because of T-MOBILE's breach of the terms of the Privacy Policy, COBC, and CPNI Policy, because his "Personal Information," including CPI and CPNI, were breached in the May 23, 2018 (and again in the June 1, 2018) SIM swap fraud, which led to monetary losses of more than $400,000.00.

WHEREFORE, Claimant [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation; for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Panel deems just and proper.

COUNT IX – BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING

Claimant re-alleges, and adopts by reference herein, Paragraphs 1-83 above, and further alleges:

190. There is an implied covenant of good faith and fair dealing in every contract that neither party will do anything which will injure the right of the other to receive the benefits of the agreement.

191. Under the express and implied terms of the relationship between Claimant and T-MOBILE, including through the Privacy Policy, COBC, and CPNI Policy, Claimant and T-MOBILE were to benefit using T-MOBILE's services, while T-MOBILE was supposed to benefit through money received for Claimant subscribing to T-MOBILE's wireless services.

192. T-MOBILE exhibited bad faith through its conscious awareness of and deliberate indifference to the risk to Claimant's Personal Information, including CPI and CPNI, by: (a) not implementing security measures adequate to protect his Personal Information; (b) improperly hiring, training, and supervising its employees; (c) not adhering to its own security standards, including the "high security" standards for previously-compromised accountholders like Claimant; and (d) failing to invest in adequate security protections.

193. T-MOBILE, by exposing Claimant to vastly greater security risks, breached its implied covenant of good faith and fair dealing with respect to the terms of its Privacy Policy, COBC, and CPNI Policy and the implied warranties of its contractual relationship with its users.

194. Claimant was harmed because of T-MOBILE's breach of the implied covenant of good faith and fair dealing because his Personal Information was compromised by the hackers in the

May 23, 2018 and June 1, 2018 SIM swap frauds which led to monetary damages of more than $400,000.00.

195. T-MOBILE's misconduct as alleged herein is fraud in that it was deceit or concealment of a material fact known to T-MOBILE conducted with an intent on the part of T-MOBILE of depriving Claimant of legal rights or otherwise concerning injury.

196. In addition, T-MOBILE's misconduct, as alleged herein, is malice, fraud or oppression in that it was despicable conduct carried on by T-MOBILE with a willful and conscious disregard of the rights or safety of Claimant and has subjected Claimant to cruel and unjust hardship in conscious disregard of his rights. As a result, Claimant is entitled to punitive damages against T-MOBILE.

WHEREFORE, Claimant [redacted] an individual, demands entry of a judgment against Respondent T-MOBILE USA, INC., a Delaware corporation; for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Panel deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Claimant [redacted] an individual, respectfully prays for relief as follows:

(a) A declaration that Respondent T-MOBILE's Agreement in its entirety is unenforceable as unconscionable and against public; or, in the alternative that: (a) the Exculpatory Provision is unenforceable as against Claimant; (b) the Indemnification is unenforceable as against Claimant; and (c) the Arbitration Provision is unenforceable as against Claimant;

(b) A judgment awarding Claimant equitable restitution, including, without limitation, restoration of the *status quo ante*, and return to Claimant all cryptocurrency or fiat currency taken from him in connection with the SIM card swap negligently-allowed by Respondent T-MOBILE;

(c) An award of any and all additional damages recoverable under law including but not limited to compensatory damages, punitive damages, incidental damages, and consequential damages;

(d) Pre- and post-judgment interest;

(e) Attorneys' fees, expenses, and the costs of this action; and

(f) All other and further relief as this Panel deems necessary, just, and proper.

Respectfully submitted,

SILVER MILLER
11780 W. Sample Road
Coral Springs, Florida 33065
Telephone: (954) 516-6000

By: _____
DAVID C. SILVER
Florida Bar No. 572764
E-mail: DSilver@SilverMillerLaw.com
JASON S. MILLER
Florida Bar No. 072206
E-mail: JMiller@SilverMillerLaw.com
TODD R. FRIEDMAN
Florida Bar No. 097919
E-mail: TFriedman@SilverMillerLaw.com

Counsel for Claimant, [redacted]

Dated: October 11, 2018

Did you activate (or renew) service prior to August 22, 2018? If yes, please click the date for the applicable version of the Terms and Conditions: August 10, 2018 | September 20, 2017 | September 1, 2016 | March 17, 2016 | February 17, 2016 | January 25, 2016 | November 14, 2015 | June12, 2015 | March 18, 2015 |November 10, 2014 |March 27, 2014 |October 20, 2013 |December 30, 2011 |July 24, 2011 |July 18, 2010 |June 28, 2008 | December 2004

T-Mobile Terms & Conditions

Effective as of August 22, 2018

Thanks for choosing T-Mobile. Please read these Terms & Conditions ("T&Cs"), which contain important information about your relationship with T-Mobile, including mandatory arbitration of disputes between us, instead of class actions or jury trials. You will become bound by these provisions once you accept these T&Cs.

WHO IS THIS AGREEMENT WITH?

These T&Cs are an agreement between you and us, T-Mobile USA, Inc., and our controlled subsidiaries, assignees, and agents.

HOW DO I ACCEPT THESE T&Cs?

You accept these T&Cs by doing any of the following things:

- giving us a written or electronic signature or confirmation, or telling us orally that you accept;
- activating, using or paying for the Service or a Device; or
- opening the Device box.

If you don't want to accept these T&Cs, don't do any of these things.

When you accept, you're telling us that you are of legal age (which means you are either legally emancipated, or have reached the age of majority as defined in your jurisdiction) and that you are able to enter into a contract. If you accept for an organization, you're telling us that you are authorized to bind that organization, and references to "you" in these T&Cs may mean the organization.

WHAT IS INCLUDED IN THESE TERMS AND CONDITIONS?

In these T&Cs, you'll find important information about:

- T-Mobile services provided to you ("Services");
- Any equipment for which we provide Service, such as a phone, handset, tablet, or SIM card (collectively, a "Device");
- Any charges, taxes, fees, and other amounts we bill you or that were accepted or processed through your Device ("Charges");
- Privacy information;
- Network management practices;
- Limitations of liability; and
- Resolution of disputes by arbitration and class action and jury trial waivers (full terms available here).

ARE THERE ANY OTHER TERMS THAT APPLY TO ME?

Yes. Your "Agreement" includes these T&Cs, the additional terms found in your Rate Plan, your Data Plan, your Service Agreement, and provisions linked to from these T&Cs. Sections marked "*" continue after termination of our Agreement with you.

EXHIBIT "A"

You should also be aware that our Privacy Policy and Open Internet Policy apply to the use of our products and services.

You might also have other agreements with us, such as an equipment installment plan or JUMP! On Demand Lease Agreement.

***HOW DO I RESOLVE DISPUTES WITH T-MOBILE?**

By accepting these T&Cs, you are agreeing to resolve any dispute with us through binding arbitration or small claims dispute procedures (unless you opt out), and to waive your rights to a jury trial and to participate in any class action suit. Your complete arbitration agreement, including opt-out instructions, is available here, and the opt-out website is available here. For additional terms and conditions governing a dispute between us, including how to dispute Charges assessed to you on your bill, choice of law, disclaimers of certain warranties, limitations of liabilities, and your indemnification obligations, click here.

WHAT IS A RATE PLAN?

Your “Rate Plan” includes your Service allotments, for example, for minutes, messages or data, rates, coverage and other terms. T-Mobile may introduce access to new technologies, features, or services that you can add for an additional charge. You can check your current usage by visiting my.T-mobile.com, or by using a short code from your Device (you can find more information about the short code at www.t-mobile.com). If any term in your Rate Plan conflicts with these T&Cs, the term in your Rate Plan governs.

HOW WILL I BE CHARGED FOR DATA USAGE?

Data service may be included in your Rate Plan or data pass or you may be charged for data usage on a pay per use basis (“Data Plan”). Your Rate Plan and/or Data Plan will contain more information about how we calculate data usage. You can check your current usage by visiting my.T-mobile.com or by using a short code from your device (you can find more information about the short code at www.t-mobile.com). If you do not have a Data Plan, your Device may not be able to access data services.

ARE THERE SEPARATE TERMS FOR PREPAID CUSTOMERS?

The terms of these T&Cs apply to prepaid customers, and additional terms specific to prepaid customers may be found here.

HOW DO I GIVE OTHER PEOPLE ACCESS TO MY ACCOUNT?

If you want someone else to be able to access and manage your account, you can establish them as an “Authorized User,” so they can:

- Make changes to your account;
- Add or remove services or features to your account;
- Receive notices and disclosures on your behalf;
- Purchase Devices for use with our Service, including under an installment plan; and
- Incur Charges on your account.

The easiest way to designate an Authorized User is online through your my.T-mobile.com account. Keep in mind that you should not share your account validation information, which includes the last four digits of your social security number or your passcode. An Authorized User will need to verify identity before we provide access to account information. When calling us, this requires presentation of the last four digits of the primary account holder’s social security number or the account PIN/passcode. This information is sensitive so take steps to protect it. We will treat presentation of the proper account validation information as authorized access to an account.

WHERE, HOW, AND WHEN DOES MY SERVICE WORK?

These T&Cs describe the experience you can expect on our network, including information about our reasonable network management practices, and the experience on our roaming partners' networks:

- Please check our coverage maps, which approximate our anticipated coverage area outdoors. Your experience on our network may vary and change without notice depending on a variety of factors. For more information, click here. You agree that we are not liable for problems relating to Service availability or quality.
- For more information about roaming, click here.
- To provide the best possible experience for the most possible customers on T-Mobile branded plans, we prioritize the data usage of a small percentage of our heavy data users, specifically those using more than 50GB of data in a billing cycle below that of other customers. This threshold number applies to all rate plans, is periodically evaluated, and may change over time. We also prioritize the data of customers who choose certain rate plans after the data for other T-Mobile branded rate plans, but before customers using more than 50GB of data in a billing cycle. Customers whose data is prioritized lower may notice speeds lower than customers with higher priority in times and locations where there are competing customer demands for network resources. See your selected service or visit our Open Internet page at the link below for details. We prioritize smartphone and mobile internet (tablet) over Smartphone Mobile HotSpot (tethering) traffic on our network. Click here for more information.
- We utilize streaming video optimization technology in our network on qualifying Rate Plans to help minimize data consumption while also improving the service experience for all customers. Some Rate Plans have video optimization via the Binge On feature. Some qualifying video providers may choose to opt-out of the Binge On program. For a list of opt-out providers visit http://www.t-mobile.com/offer/binge-on-streaming-video.html#. The Binge On optimization technology is not applied to the video services of these providers; video from these services will stream at native resolution, and high-speed data consumption will continue as if Binge On were not enabled.
- Additionally, we may implement other network practices, such as caching less data.
- Our Open Internet Policy includes important information on these topics as well as information on commercial terms, performance characteristics (such as expected speed, latency and network practices).

***WHAT ARE THE PERMITTED AND PROHIBITED USES FOR MY DEVICE AND THE SERVICES?**

Our wireless network is a shared resource, which we manage for the benefit of all of our customers. Your Data Plan is intended for Web browsing, messaging, and similar activities. Certain activities and uses of our Services and your Device are permitted and others are not. For examples of permitted and prohibited uses, click here. If you buy, lease, or finance a Device manufactured for use on our network, you agree, and we rely on your agreement, that you intend it to be activated on our Service and will not resell or modify the Device, or assist anyone doing so.

***WHAT HAPPENS IF MY DEVICE IS LOST OR STOLEN?**

You agree to notify us if your Device is lost or stolen. Once you notify us, we will suspend your Service. Click here to learn more about how we handle Charges that are incurred after you report that your Device is lost or stolen.

***HOW WILL I BE BILLED FOR USE OF THE SERVICES?**

You agree to pay all Charges we assess and bill you or that were accepted or processed through all Devices on your account. **Off-Rate Plan Charges.** You may have to pay extra for calls to some numbers (e.g., conference & chat lines, broadcast, calling card, international, 900 or 976 calls, etc.). You agree to provide us with accurate and complete billing and tax related information and to report all changes within 30 days of the change. You will receive an electronic (paperless) bill unless you tell us you want a paper bill. You have the option of switching to a paper bill at no cost to you by changing your billing preferences at my t-mobile or by contacting Customer Care. For more information about paperless billing, please visit www.t-mobile.com/billterms.

Your Device can be used to purchase services and products from third parties, and Charges for these purchases may be included on your T-Mobile bill. For no additional cost you can block third party charges from being included on your T-Mobile bill by logging into your account at www.my.t-mobile.com or calling Customer Care. For more information about

billing, click here.

WHAT IF I DON'T PAY ON TIME?

We may charge a late fee of the greater of 1.5% per month (18% annually) or $5 per month and a returned payment fee up to $35, subject to the maximum allowed by law. We may use a collection agency to collect past due balances and you agree to pay collection agency fees. If we accept late or partial payments, you still must pay us the full amount you owe, including late fees. We will not honor limiting notations you make on or with your checks. Late payment, non-payment or collection agency fees are liquidated damages intended to be a reasonable advance estimate of our costs resulting from late payments and non-payments by our customers; these costs are not readily ascertainable and are difficult to predict or calculate at the time that these fees are set.

***DOES T-MOBILE CHECK MY CREDIT?**

Yes, for many of our products and services. We may get information about your credit history from credit-reporting agencies, which may affect your credit rating. We may also report your payment record to credit-reporting agencies.

AM I REQUIRED TO MAKE A DEPOSIT?

We may require you to make a deposit or prepayment for Services. We can apply deposits, payments, or prepayments in any order to any amounts you owe us on any account. This deposit is refundable, and will be applied as a credit to your account along with interest as may be required by law.

CAN T-MOBILE ACCESS MY DEVICE?

We may remotely change software, systems, applications, features or programming on your Device without notice. These changes will modify your Device and may affect or erase data you have stored on your Device, the way you have programmed your Device, or the way you use your Device. You will not be able to use your Device during the installation of the changes, even for emergencies.

CAN I DOWNLOAD AND USE THIRD PARTY CONTENT AND APPS ON MY DEVICE?

Yes. You are free to download and use content or applications ("Content & Apps") on your Device that are not provided by T-Mobile, at your own risk. Third party Content & Apps may require your agreement to a license or other terms with the third party. Some Devices or Content & Apps may contact our network without your knowledge, which may result in additional Charges (e.g., while roaming internationally).

***LICENSE**

Your Device's Software is licensed, not sold, to you by T-Mobile and/or other licensors for your personal, lawful, non-commercial use on your Device only. You may only use the Software as authorized by its license. Your Device's "Software" includes its software, interfaces, documentation, data, and Content & Apps, as each may be updated or replaced by feature enhancements or other updates. For additional information regarding these license terms, including restrictions on your use of the Software, please click here.

***WHAT IS THE TERM OF THESE T&Cs?**

As the Un-Carrier, we did away with annual service contracts. You are free to go, although we'd be sad to see you leave. You are responsible for all Charges incurred through the end of your Service term. If you port your number to another carrier, your Service will be deactivated. In addition, cancellation of Service may affect other agreements that you have with us, including equipment installment plans or lease agreements where some of your payments may be accelerated upon cancellation.

CAN T-MOBILE CHANGE OR TERMINATE MY SERVICES OR THIS AGREEMENT?

Yes. Except as described below for Rate Plans with the price-lock guarantee (including the "Un-Contract Promise"), we may change, limit, suspend or terminate your Service or this Agreement at any time, including if you engage in any of the prohibited uses described here or no longer reside in a T-Mobile-owned network coverage area. Under certain limited circumstances, we may also block your device from working on our network. If the change to your Service or Rate Plan will have a material adverse effect on you, we will provide 14 days' notice of the change. You'll agree to any change by using your Service after the effective date of the change. We may exclude certain types of calls, messages or sessions (e.g. conference and chat lines, broadcast, international, 900 or 976 calls, etc.), in our sole discretion, without further notice.

If you are on a price-lock guaranteed Rate Plan, we will not increase your monthly recurring Service charge ("Recurring Charge") for the period that applies to your Rate Plan, or, if no specific period applies, for as long as you continuously remain a customer in good standing on a qualifying Rate Plan. If you switch plans, the price-lock guarantee for your new Rate Plan will apply (if there is one). The price-lock guarantee is limited to your Recurring Charge and does not include, for example, add-on features, taxes, surcharges, fees, or charges for extra features or Devices. If your Service or account is limited, suspended or terminated and then reinstated, you may be charged a reactivation fee. For information about our unlocking policy, click here.

***YOUR CONSENT TO BE CONTACTED**

We may contact you without charge, on any wireless telephone number assigned to your account for any purpose, including marketing, and in any manner permitted by law. You also expressly consent to be contacted by us, and anyone contacting you on our behalf, for any purpose, including billing, collection, or other account or service related purpose, at any telephone number or physical or electronic address where you may be reached, including any wireless telephone number. You agree that T-Mobile, and anyone contacting you on our behalf, may communicate with you in any manner, including using a pre-recorded or artificial voice, using an automatic telephone dialing system to place calls or send messages, or alerts, or using an automatic e-mail system to deliver email messages. If a contact number you have provided to us is no longer your number, you agree to notify us promptly that you can no longer be reached at that number. You represent that you have received, and are authorized to convey to us, the consent of any authorized users on your account to be contacted by us as described in this Section. You agree that all consents provided in this Section will survive cancellation of your Service and account.

HOW DO WE NOTIFY EACH OTHER?

You may contact us at www.T-Mobile.com, by calling 1-800-937-8997 or 611 from your Device, or by writing to: T-Mobile Customer Relations, P.O. Box 37380, Albuquerque, NM 87176-7380. **Puerto Rico customers** you may contact us at www.t-mobile.com, by calling 1-800-937-8997 or 611 from your Device, or by writing to: T-Mobile Customer Relations, B7 Tabonuco Street, Suite 700, Guaynabo, Puerto Rico 00968-3349, Attn: Customer Care Manager. Electronic notices are considered delivered when sent. Mail notices are considered delivered 3 days after mailing. For multi-line accounts, we may assign a "Primary Telephone Number" to your account for the purpose of receiving notices, as well as for other purposes. If you would like to change it, contact us.

To begin arbitration or any other legal proceeding, you must serve our registered agent. Our registered agent is Corporation Service Company and can be contacted at 1-866-403-5272. For **Puerto Rico customers**, our registered agent is Fast Solutions, LLC and can be contacted at Citi Tower, 252 Ponce de Leon Avenue, Floor 20, San Juan, Puerto Rico, 00918, phone: 1-787-688-5881.

EMERGENCY ALERTS

T-Mobile has chosen to offer wireless emergency alerts, within portions of its coverage area. Wireless alert capable handsets with appropriate notification settings are required for the service. There is no additional charge for these wireless emergency alerts. For details visit www.t-mobile.com/responsibility/consumer-info/safety/wireless-emergency-alerts.

911 ACCESS

911 services are made possible by your state and local government. T-Mobile handsets are capable of making calls to 911 in the United States, and 911 access is available to customers regardless of your Rate Plan. The handset must have battery power and connectivity to complete a 911 call. When making 911 calls, you should be prepared to provide information about where you are located. In some cases, 911 communications center operators may not know your phone number or have information about your location. Other third-party entities are involved in connecting a 911 call and T-Mobile does not determine the public safety agency to which your 911 call is routed. If you are porting a phone number to or from us, we may not be able to provide you with some Services, such as 911 location services, while the port is in process. If you are outside the U.S., you may have to dial a different number than 911 to call emergency services.

Wi-Fi Calling. Wi-Fi Calling services use an internet connection to make calls, including 911 calls, and calls to 911 using Wi-Fi Calling operate differently than traditional 911. When enabling Wi-Fi Calling, you must provide us with the primary street address at which the Wi-Fi Calling service will be used ("Registered Location"). If you call 911 over Wi-Fi, we will provide your Registered Location to the public service entity that answers the call, and it may be used to help emergency responders locate you. You agree to update your Registered Location if you use Wi-Fi service at a different location. You can update your Registered Location by accessing your MyT-Mobile.com account or by contacting T-Mobile Customer Care. **Text-to-911.** Text to 911 may be available in some locations where T-Mobile service is provided, and is dependent on the public safety agency's ability to receive text messages.

Calls to 911 from a TTY will not work when using Wi-Fi Calling or Voice over LTE ("VoLTE"). If you cannot make a voice call to 911, T-Mobile recommend that you use an internet-based Telecommunications Relay Service such as Video Relay Service, IP Relay Service, or IP Captioned Telephone Service. T-Mobile Real-Time Text ("RTT") technology is available on T-Mobile's network and can be used on select devices to contact 911. For more information, see www.t-mobile.com/accessibilitypolicy.

PARENTAL CONTROLS

We offer services that help you to monitor and filter, or restrict, internet access to minors. See T-Mobile.com for details.

***WHAT ELSE DO I NEED TO KNOW?**

Click here for additional terms that apply to you.

Dispute Resolution

***HOW DO I RESOLVE DISPUTES WITH T-MOBILE?**

Dispute Resolution and Arbitration. YOU AND WE EACH AGREE THAT, EXCEPT AS PROVIDED BELOW, ANY AND ALL CLAIMS OR DISPUTES IN ANY WAY RELATED TO OR CONCERNING THE AGREEMENT, OUR PRIVACY POLICY, OUR SERVICES, DEVICES OR PRODUCTS, INCLUDING ANY BILLING DISPUTES, WILL BE RESOLVED BY BINDING ARBITRATION OR IN SMALL CLAIMS COURT. This includes any claims against other parties relating to Services or Devices provided or billed to you (such as our suppliers, dealers, authorized retailers, or third party vendors) whenever you also assert claims against us in the same proceeding. You and we each also agree that the Agreement affects interstate commerce so that the Federal Arbitration Act and federal arbitration law, not state law, apply and govern the enforceability of this dispute resolution provision (despite the general choice of law provision set forth below). THERE

IS NO JUDGE OR JURY IN ARBITRATION, AND COURT REVIEW OF AN ARBITRATION AWARD IS LIMITED. THE ARBITRATOR MUST FOLLOW THIS AGREEMENT AND CAN AWARD THE SAME DAMAGES AND RELIEF AS A COURT (INCLUDING ATTORNEYS' FEES).

For Puerto Rico customers, references to "small claims court" should be understood to mean the Puerto Rico Telecommunications Regulatory Board ("**TRB**") for matters within the jurisdiction of said agency. See **OTHER TERMS REGARDING DISPUTE RESOLUTION** for details on the billing dispute process in Puerto Rico.

Notwithstanding the above, **YOU MAY CHOOSE TO PURSUE YOUR CLAIM IN COURT AND NOT BY ARBITRATION IF YOU OPT OUT OF THESE ARBITRATION PROCEDURES WITHIN 30 DAYS FROM THE EARLIER OF THE DATE YOU PURCHASED A DEVICE FROM US OR THE DATE YOU ACTIVATED A NEW LINE OF SERVICE (the "Opt Out Deadline")**. You must opt out by the Opt Out Deadline for each line of Service. You may opt out of these arbitration procedures by calling 1-866-323-4405 or online at www.T-Mobiledisputeresolution.com. **Any opt-out received after the Opt Out Deadline will not be valid and you will be required to pursue your claim in arbitration or small claims court.**

For all disputes, you must first give us an opportunity to resolve your claim by sending a written description of your claim to the address provided in the "How Do We Notify to Each Other" Section below. You and we each agree to negotiate your claim in good faith, and you agree that you may not commence any arbitration or court proceeding unless you and we are unable to resolve the claim within 60 days after we receive your claim description. You and we each agree that if you fail to timely pay amounts due, we may assign your account for collection, and the collection agency may pursue, in small claims court, claims limited strictly to the collection of the past due amounts and any interest or cost of collection permitted by law or this Agreement.

If the arbitration provision applies or you choose arbitration to resolve your disputes, then either you or we may start arbitration proceedings. You must send a letter requesting arbitration and describing your claim to our registered agent (see the "How Do We Notify to Each Other" section below) to begin arbitration. The arbitration of all disputes will be administered by the American Arbitration Association ("AAA") under its Consumer Arbitration Rules in effect at the time the arbitration is commenced. The AAA rules are available at www.adr.org or by calling 1-800-778-7879. The arbitration of all disputes will be conducted by a single arbitrator, who shall be selected using the following procedure: (a) the AAA will send the parties a list of five candidates; (b) if the parties cannot agree on an arbitrator from that list, each party shall return its list to the AAA within 10 days, striking up to two candidates, and ranking the remaining candidates in order of preference; (c) the AAA shall appoint as arbitrator the candidate with the highest aggregate ranking; and (d) if for any reason the appointment cannot be made according to this procedure, the AAA may exercise its discretion in appointing the arbitrator. Upon filing of the arbitration demand, we will pay or reimburse all filing, administration and arbitrator fees. An arbitrator may award on an individual basis any relief that would be available in a court, including injunctive or declaratory relief and attorneys' fees. In addition, for claims under $75,000 as to which you provided notice and negotiated in good faith as required above before initiating arbitration, if the arbitrator finds that you are the prevailing party in the arbitration, you will be entitled to recover reasonable attorneys' fees and costs. Except for claims determined to be frivolous, we agree not to seek attorneys' fees in arbitration even if permitted under applicable law.

CLASS ACTION WAIVER. **YOU AND WE EACH AGREE THAT ANY PROCEEDINGS, WHETHER IN ARBITRATION OR COURT, WILL BE CONDUCTED ONLY ON AN INDIVIDUAL BASIS AND NOT AS A CLASS, REPRESENTATIVE, OR CONSOLIDATED ACTION**. If a court or arbitrator determines in an action between you and us that any part of this Class Action Waiver is unenforceable with respect to any claim, the arbitration agreement and Class Action Waiver will not apply to that claim, but they will still apply to any and all other claims that you or we may assert in that or any other action. **If you opt out of the arbitration provision as specified above, this Class Action Waiver provision will not**

apply to you. Neither you, nor any other customer, can be a class representative, class member, or otherwise participate in a class, consolidated, or representative proceeding without having complied with the opt out requirements above.

JURY TRIAL WAIVER. If a claim proceeds in court rather than through arbitration, **YOU AND WE EACH WAIVE ANY RIGHT TO A JURY TRIAL**.

Other Terms Regarding Dispute Resolution

*HOW CAN I DISPUTE MY CHARGES?

If you have any questions about your bill or want to dispute any Charges, please contact us by visiting www.T-Mobile.com, by calling 800-937-8997 or 611 from your Device, or by writing to T-Mobile Customer Relations, P.O. Box 37380, Albuquerque, NM 87176-7380. **Puerto Rico customers:** You may contact us at www.T-Mobile.com, by calling 1-800-937-8997 or 611 from your Device, or by writing to us at: T-Mobile Customer Relations, B7 Tabonuco Street, Suite 700, Guaynabo, Puerto Rico 00968-3349, Attn.: Customer Care Manager. If this does not fix things, please notify us in writing. Unless otherwise provided by law, you must notify us in writing of any dispute regarding your bill or Charges to your account within 60 days after the date you first receive the disputed bill or Charge. If you don't, you may not pursue a claim in arbitration or in court. If you accept a credit, refund or other compensation or benefit to resolve a disputed bill or Charge, you agree that the issue is fully and finally resolved and T-Mobile shall be released from any and all liability regarding said dispute. Unless otherwise provided by law, you must pay disputed Charges until the dispute is resolved.

Puerto Rico customers: Unless otherwise provided by law or these T&Cs, for billing disputes, you must notify us not later than 20 days from the date the disputed bill was sent to you. If you don't, you may not pursue a claim in arbitration or with the TRB. We will provide you with a determination regarding the billing dispute you present to us within 20 days after we receive it. You will have 20 days from the mailing date of the notification to request a reconsideration of our determination. You may appeal our determination to the TRB by filing a petition for review up to 30 days after the date of our determination. Your petition for review shall be made through the filing of a document containing the following information: (a) your name and address; (b) our company name; (c) the pertinent facts; (d) any applicable legal provisions that you are aware of; and (e) the remedy you are requesting. The document may be filed handwritten or typewritten and must be signed by you. You must send us a copy of your document to the following address: B-7 Calle Tabonuco Suite 7000, Guaynabo, Puerto Rico 00969, Attn: Customer Care Manager. You must send your petition for review to the Puerto Rico Telecommunications Regulatory Board at the following address: 500 Ave. Roberto H. Todd (Pda. 18 - Santurce), San Juan, Puerto Rico 00907-3941. The TRB will review our determination only on appeal. You are advised of the provisions regarding suspension of Service that appear in Law 33 of July 7, 1985, Law 213 of September 12, 1996 and Regulations 8065 promulgated on August 31, 2011 by the TRB regarding the procedures for customer's dispute resolution and suspension of Services.

*CHOICE OF LAW

This Agreement is governed by the Federal Arbitration Act, applicable federal law, and the laws of the state or jurisdiction in which your billing address in our records is located, without regard to the conflicts of laws rules of that state or jurisdiction. Foreign laws do not apply. Arbitration or court proceedings must be in the county and state or jurisdiction in which your billing address in our records is located, but not outside the U.S.; or Puerto Rico.

*DISCLAIMER OF WARRANTIES

Except for any written warranty that may be provided with a T-Mobile Device you purchase from us, and to the extent permitted by law, the Services and Devices are provided on an "as is" and "with all faults" basis and without warranties of any kind. We make no representations or warranties, express or implied, including any

implied warranty of merchantability or fitness for a particular purpose concerning your Service or your Device. We can't and don't promise uninterrupted or error-free service and don't authorize anyone to make any warranties on our behalf. This doesn't deprive you of any warranty rights you may have against anyone else. We do not guarantee that your communications will be private or secure; it is illegal for unauthorized people to intercept your communications, but such interceptions can occur.

Services or Software provided by third parties (including voice applications), 911 or E911, text to 911, or other calling or messaging functionality, may work differently than services offered by us, or may not work at all. Please review all terms and conditions of such third party products. When using these products, we are not responsible for the availability or reliability of 911 calls or text to 911 messages, or if inaccurate location information is provided to the 911 Communications Center. We cannot assure you that if you place a 911 call or text you will be found.

We are not responsible for any download, installation, use, transmission failure, interruption, or delay related to Content & Apps, or any third party content, services, advertisements, or websites you may be able to access by using your Device or the Services, even if charges for Content & Apps appear on your T-Mobile bill. You are responsible for maintaining virus and other Internet security protections when accessing third party Content & Apps or other services.

***LIMITATION OF LIABILITY**

To the extent permitted by law, you and we each agree to limit claims for damages or other monetary relief against each other to direct and actual damages regardless of the theory of liability. This means that neither of us will seek any indirect, special, consequential, treble, or punitive damages from the other. This limitation and waiver also applies to any claims you may bring against any other party to the extent that we would be required to indemnify that party for such claim. You agree we are not liable for problems caused by you or a third party, or by any act of nature. You also agree we aren't liable for missed or deleted voice mails or other messages, for any information (like pictures) that gets lost or deleted if we work on your Device, or for failure or delay in connecting a call or text to 911 or any other emergency service. To the extent permitted by law, you and we each also agree that all claims must be brought within 2 years of the date the claim arises.

***INDEMNIFICATION**

You agree to defend, indemnify, and hold us and our directors, officers, and employees harmless from any claims arising out of use of the Service or Devices, breach of the Agreement, or violation of any laws or regulations or the rights of any third party by you, any person on your account, or any person you allow to use the Services or your Device.

Additional Terms for Prepaid Customers

Your T-Mobile prepaid Service account balance, if sufficient, or your active prepaid plan, gives you access to our prepaid Service for a limited amount of time; you must use your prepaid Service during the designated period of availability. To use our prepaid Service you must have a T-Mobile prepaid Service account balance for pay as you go service or be on an active prepaid plan. Service will be suspended when your account balance reaches zero and/or you are at the end of the time period associated with your prepaid plan. Monthly plan features are available for 30 days, however, depending on the time of day that you activate your Service or that your Service expires, your service cycle may not equal 30 full 24-hour days. Your monthly plan will automatically renew at the end of 30 days if you have a sufficient T-Mobile prepaid Service account balance to cover your prepaid Service plan before the first day after your service cycle. If you do not have a sufficient T-Mobile prepaid Service account balance, your prepaid Service will be suspended unless you move to a pay as you go plan. If you do not reinstate prepaid Service within the required period based upon your service plan,

your phone number will be reallocated. The Charges for Service and the amount of time that Service is available following activation of your prepaid Service account balance may vary; see your Rate Plan for more information. Prepaid Service is non-refundable (even if returned during the Cancellation Period), and no refunds or other compensation will be given for unused airtime balances, lost or stolen prepaid cards, or coupons. You will not have access to detailed usage records or receive monthly bills. Coverage specific to our prepaid Service may be found at https://prepaid.t-mobile.com/prepaid/coverage-map and differs from coverage related to our postpaid Service.

Using Our Network

WILL MY SERVICE VARY? WHAT FACTORS MAY AFFECT MY SERVICE?

As our customer, your actual Service area, network availability, coverage and quality may vary based on a number of factors, including network capacity, terrain, weather, if you are on a private or public Wi-Fi network, using a non-T-Mobile device, or if your Device no longer supports network technologies compatible with or available on T-Mobile's network. Outages and interruptions in Service may occur, and speed of Service varies. Devices also have varying speed capabilities and may connect to different networks depending on technology. Even within coverage areas and with broadband-capable devices, network changes, traffic volume, outages, technical limitations, signal strength, obstructions, weather, and other conditions may impact speeds and service availability.

We engineer our network to provide consistent high-speed data service, but at times and at locations where the number of customers using the network exceeds available network resources, customers will experience reduced data speeds. In those cases, customers who choose certain rate plans may notice speeds lower than customers on other T-Mobile branded rate plans, which are prioritized higher on our network. Further, to provide the best possible on-device experience for the most possible customers on T-Mobile branded plans and minimize capacity issues and degradation in network performance, we may, without advance notice, take any actions necessary to manage our network on a content-agnostic basis, including prioritizing all on-device data over Smartphone Mobile HotSpot (tethering) data and further prioritizing the data usage of a small percentage of heavy data users, specifically those using more than 50GB of data in a billing cycle, below that of all other customers in times and locations where there are competing customer demands for network resources, for the remainder of the billing cycle. This threshold number is periodically evaluated and may change over time.

Where the network is lightly loaded in relation to available capacity, a customer whose data is prioritized below other data traffic will notice little, if any, effect from having lower priority. This will be the case in the vast majority of times and locations. At times and locations where the network is heavily loaded in relation to available capacity, however, these customers will likely see significant reductions in data speeds, especially if they are engaged in data-intensive activities. Customers should be aware that these practices may occasionally result in speeds below those typically experienced on our LTE networks. We constantly work to improve network performance and capacity, but there are physical and technical limits on how much capacity is available, and in constrained locations the frequency of heavy loading in relation to available capacity may be greater than in other locations. When network loading goes down or the customer moves to a location that is less heavily loaded in relation to available capacity, the customer's speeds will likely improve. See www.T-Mobile.com/OpenInternet for details.

Roaming

***CAN I ROAM ON MY DEVICE?**

Domestic Roaming: Your Device may connect to another provider's network ("Off-Net"). This may happen even when you are within the T-Mobile coverage area. Check your Device to determine if you are Off-Net. Please do not abuse this; we may limit or terminate your Service if you do. Your device may also connect to another provider's secured Wi-Fi network. See **WHAT ARE THE PERMITTED AND PROHIBITED USES FOR MY DEVICE AND THE SERVICE?** section for additional info.

International Roaming & Dialing: Availability and features offered for international roaming and dialing vary depending on your Rate Plan and Device. All countries may not be available for roaming and available countries may change from time to time; click here for more information about which countries are currently available for roaming. Whether roaming internationally or making and sending international calls and messages while in the U.S. (or Puerto Rico), you may be charged international rates (including for voicemails left for you and for data usage). This includes per-minute rates for calls and per-minute rates for calls transferred to your voicemail and the relevant data rates for data usage. You may be charged for more than one call for unanswered calls that are forwarded to voicemail regardless of whether the calls result in actual voicemail messages being left for you and regardless of whether your Device is on or off. Different rates and rounding increments apply in different countries. Click here for information on international access, rates, Services and coverage. While roaming internationally, your data throughput may be reduced and your Service may be otherwise limited or terminated at any time without notice. You are responsible for complying with U.S. Export Control laws and regulations, and the import laws and regulations of foreign countries when traveling internationally with your Device. The availability of, and access to, emergency calling services (e.g., 911 in the U.S.), may vary by country. You should familiarize yourself with how to access these services before using your handset for international roaming. See **WHAT ARE THE PERMITTED AND PROHIBITED USES FOR MY DEVICE AND THE SERVICE?** section for additional information about international roaming.

Streaming Video

We deploy streaming video optimization technology in our network as a feature on qualifying Rate Plans, which also helps to ensure that available network capacity can be utilized to provide a good service experience for the maximum number of customers. The optimization technology is intended to manage data usage on the network, reduce the risk of streaming video stalling and buffering on mobile devices, and reduce the amount of data consumed for streaming video, making room for other users to enjoy higher speeds and a better network experience overall. Video optimization occurs only to data streams that are identified by our packet-core network as video or where the video provider has chosen to establish protocols to self-optimize their video. While many changes to streaming video files are likely to be indiscernible, the optimization process may impact the appearance of the streaming video as displayed on a user's Device. Customers may have Rate Plans where this feature is always enabled (e.g., "T-Mobile ONE"), with the ability to add a feature disabling optimization to foster native-resolution video capability. Alternatively, customers may choose Rate Plans that offer video optimization as a customer-controlled feature (e.g., "Binge On"). When this feature is enabled, on-device video is typically delivered at DVD quality (up to 1.5 Mbps speeds, generally 480p).

Some qualifying video providers may choose to opt-out of the Binge On program, see listing at http://www.t-mobile.com/offer/binge-on-streaming-video.html#. The Binge On optimization technology is not applied to the video services of these providers; video from these services will stream at native resolution, and high-speed data consumption will continue as if Binge On were not enabled. Rate Plans that feature this technology allow customers to choose to enable (and disable) video streaming optimization when connected to the cellular network, unless a provider has chosen to opt-out, see listing at http://www.t-mobile.com/offer/binge-on-streaming-video.html#.

For more information about video optimization, click here.

Examples of Permitted and Prohibited Uses of the Services and Your Device

Permitted uses include:

- Voice calls;
- Web browsing;
- Messaging;
- Email;
- Streaming music;
- Uploading and downloading applications and content to and from the Internet or third party stores;
- Using applications and content without excessively contributing to network congestion; and
  Tethering your Device to other non-harmful devices pursuant to the terms and conditions and allotments of your Data Plan.

Unless explicitly permitted by your Rate Plan or Data Plan, you are not permitted to use your Device or the Services in a way that we determine:

- Uses a repeater or signal booster other than one we provide to you;
- Compromises network security or capacity, degrades network performance, uses malicious software or “malware”, hinders other customers’ access to the network, or otherwise adversely impacts network service levels or legitimate data flows;
- Uses applications which automatically consume unreasonable amounts of available network capacity;
- Uses applications which are designed for unattended use, automatic data feeds, automated machine-to-machine connections, or applications that are used in a way that degrades network capacity or functionality;
- Misuses the Service, including "spamming" or sending abusive, unsolicited, or other mass automated communications;
- Accesses the accounts of others without authority;
- Results in more than 50% of your voice and/or data usage being Off-Net (i.e., connected to another provider’s network) for any 2 billing cycles within any 12-month period;
- Results in unusually high usage (specifically, more 50GB (updated periodically) in a month) and the majority of your data usage being Smartphone Mobile HotSpot (tethering) usage for any 3 billing cycles within any 6-month period;
- Resells the Service, either alone or as part of any other good or service;
- Tampers with, reprograms, alters, or otherwise modifies your Device to circumvent any of our policies or violate anyone’s intellectual property rights;
- Causes harm or adversely affects us, the network, our customers, employees, business, or any other person;
- Conflicts with applicable law;
- Is not in accordance with these T&Cs; or
- Attempts or assists or facilitates anyone else in any of the above activities.

Information about What Happens if Your Device is Lost or Stolen

Once you notify us that your Device has been lost or stolen, we will suspend your Service and you will not be responsible for additional usage charges incurred in excess of your Rate Plan Charges, applicable taxes, fees, and surcharges. If Charges are incurred before you notify us, you are not liable for Charges you did not authorize. However, the fact that your Device or account was used is some evidence of authorization. You may ask us to investigate Charges you believe were unauthorized. We may ask you to provide information and you may submit information to support your request. If we determine the Charges were unauthorized, we will credit your account. If we determine the Charges were authorized, we will inform you within 30 days and you will remain responsible for the Charges. If you request that we not suspend your Service, you will remain responsible for all Charges incurred. We may prevent a lost or stolen Device from registering on our and other networks.

You can click here to learn about additional anti-theft measures that may apply to you.

Billing Information

Please read the following for more information about how we bill for calls, data usage and messaging, Wi-Fi usage, third party charges, taxes, and surcharges.

Usage: Airtime usage is measured from the time the network begins to process a call (before the phone rings or the call is answered) through its termination of the call (after you hang up). For voice calls, we round up any fraction of a minute to the next full minute. Depending upon your Rate Plan, data usage may be rounded at the end of each data session, at the end of your billing cycle, and/or at the time you switch data plans. You may be charged for more than one call/message when you use certain features resulting in multiple inbound or outbound calls/messages (such as call forwarding, call waiting, voicemail, conference calling, and multi-party messaging). You will be charged for text, instant or picture messages, and email whether read or unread, sent or received, solicited or unsolicited. We use filters to block spam messages, but we do not guarantee that you will not receive spam or other unsolicited messages. Additional blocking options are available at www.my.T-Mobile.com. Most usage and Charges incurred during a billing cycle will be included in your bill for that cycle. Some usage and Charges may be delayed to a later billing cycle, which may cause you to exceed Rate Plan allotments in a later billing cycle. Unused Rate Plan allotments expire at the end of your billing cycle. You may be billed additional Charges for certain features and services. Charges for Wi-Fi usage may vary; see your Rate Plan for more details.

Taxes: You agree to pay all taxes and fees imposed by governments or governmental entities. We may not give advance notice of changes to these charges. To determine taxes & fees, we use the street address you identified as your Place of Primary Use (“PPU”). The PPU for **Puerto Rico customers** must be in Puerto Rico. If you did not identify the correct PPU, or if you provided an address, such as a PO Box, that is not a recognized street address, does not allow us to identify the applicable taxing jurisdiction(s) or does not reflect the Service area associated with your telephone number, you may be assigned a default location for tax purposes. Except as may be otherwise required by law, in the event you dispute your PPU or the location we assigned you and the resulting taxes or fees applied on your bill, you must request a refund of the disputed tax or fee within 60 days of the date of our bill containing such tax or fee. Regardless of any Rate Plan guarantee, taxes and fees may change from time to time without notice.

Surcharges: You agree to pay all surcharges applicable to your Rate Plan. Surcharges are not mandated or imposed on you by law, they are T-Mobile Charges that are determined, collected and retained by us. The components and amounts of the Surcharges are subject to change without notice. Surcharges include charges, costs, fees and certain taxes that we incur to provide Services (and are not government taxes or fees imposed directly on our customers). Examples include general and administrative fees (such as certain costs we incur to provide Service) as well as governmental-related assessments (such as Federal or State Universal Service fees, regulatory or public safety charges, environmental fees, and gross receipts taxes). Surcharges assessed to you will vary depending on the type of Service and the Rate Plan you have. Surcharges will apply whether or not you benefit from the programs, activities or services included in the Surcharge. When Surcharges are assessed in connection with your Service, you can find the Surcharges detailed in either the “Taxes, Fees & Surcharges”, “T-Mobile Fees and Charges” or the “Other Charges” sections of your bill or at www.my.T-Mobile.com. Regardless of any Rate Plan guarantee, Surcharges may change from time to time without notice.

Additional Software License Terms

Except as permitted by applicable law, you may not assign, transfer, sublicense, copy, reproduce, redistribute, resell, modify, decompile, attempt to derive the source code of, or reverse engineer all or any part of the Software, or alter, disable or circumvent any digital rights management security features embedded in the Software. The Software may not

be transferable from one Device to another Device. You may not create derivative works of all or any part of the Software. You agree the Software contains proprietary content and information owned by T-Mobile, its licensors, and/or other third parties. T-Mobile, its licensors, and such other third parties reserve the right to change, suspend, terminate, remove, impose limits on the use or access to, or disable access to, the Software at any time without notice and will have no liability for doing so. You agree that your violation of the Software license harms T-Mobile, its licensors, and/or other third parties, that this harm cannot be fully redressed by money damages, and that T-Mobile, its licensors, and such other third parties shall be entitled to immediate injunctive relief in addition to all other remedies available.

Additional Terms

If we don't enforce our rights under this Agreement in one instance, that doesn't mean we won't or can't enforce those rights in any other instance. If any part of the Agreement is held invalid that part may be severed from the Agreement.

You can't assign or transfer the Agreement or any of your rights or duties under it without our written consent. We may assign or transfer all or part of the Agreement, or your debts to us, without notice. You understand that the assignment or transfer of all or any part of this Agreement or your debt will not change or relieve your obligations under this Agreement.

The Agreement is the entire agreement between you and us regarding the rights you have with respect to your Service, except as provided by law, and you cannot rely on any other documents or statements by any sales or service representatives or other agents.

The original version of the Agreement is in English. To the extent there are conflicts between the English version and any other language version, the English version will control.

If you believe that any material residing on our system or network infringes your copyright, notify our Designated Agent by using the Digital Millennium Copyright Act (DMCA) notice procedure described at www.t-mobile.com/responsibility/legal/copyright (http://es.t-mobile.com/responsibility/legal/copyright for our Spanish website). Our Designated Agent is Copyright Agent, 12920 S.E. 38th Street, Bellevue, WA 98006; copyrightagent@t-mobile.com; phone: 425-383-4000. There are substantial penalties for sending false notices. It is our policy, in appropriate circumstances and in our sole judgment, to suspend or terminate the Service of any subscriber, account holder, or user who is deemed to be a repeat or blatant infringer of copyrights.

T-Mobile Privacy Statement Highlights

Revised December 31, 2016

Read our full Privacy Statement
See also our Financial Privacy Statement

Print-Friendly version

This Privacy Statement describes how we collect, use, disclose, and store your personal information. As we may periodically update this Privacy Statement, you should review this Privacy Statement often for changes. Expand All Text

What Types of Information We Collect About You

We collect information from you in order to provide our products and services. Examples of the types of information we collect include:

- **Personal Information.** Personal information means information we directly associate with a specific person, for example your name, address or email address.
- **Contact Information.** We collect information about you for contact and billing purposes, including your name, address, phone number and email address.
- **Credit and Financial Information:** We collect information about your credit card or banking information, Social Security Number, and credit history so we can verify, process and bill for our products and services.
- **Network and Device Information.** We may collect information about your use of your device and our network, WiFi usage, and performance information, as well as data relating to your use of our website, applications and other products and services.

  Learn more about the information we collect

- **Children.** We do not knowingly solicit children to purchase our products and services to children or knowingly collect information from children under 13 years of age. If you allow a child to use your device or our services, you should be aware that their personal information could be collected as described in this statement.

  Learn more about our statement for Children

How Information About You Is Collected

EXHIBIT "B"

We collect information about you in three primary ways:

- **Information You Provide.** We collect information that you provide when you apply for, purchase, or use our services or products, such as your personal contact and billing information, credit information, or other information you may provide to us.

  Learn more about how we collect information

- **Information We Collect Automatically.** We automatically collect a variety of information associated with your use of your device and our products and services, some of which may be associated with you or another user on your account.

  Learn more about automatically-collected data

- **Information From Other Sources.** We may obtain or purchase information about you from other sources, such as credit information before starting service, or updated address information from shippers.

How We Use Information We Collect About You

- We use your information to provide and bill for services and products, to verify your identity, and to send you offers for T-Mobile products and services. We also use information we collect to answer your questions about your account or assist you with troubleshooting.
- We may also use your information for internal purposes, such as auditing, data analysis, and research to improve our products, services, customer communications, content.
- We may use your information to personalize services and offers we provide to you.

  Learn more about how we use information we collect

- **Location Data.** We may use information about your location to provide our services or to customize data presented to you.

  Learn more about location information

- **Advertising.** You may see advertisements when you visit our websites, mobile websites, in applications, or on your device. We may help advertisers better reach our customers by providing certain customer information, including device type, geographic information, language preferences or demographic information obtained from other companies.

  Learn more about third-party advertising

When We Share Information Collected About You

- We do not sell your name, address or phone number to others outside the T-Mobile corporate family to market those companies' products or services.
- **Account Holder.** If your use of our products and services is in conjunction with an employer discount or multi-line account, your employer or the primary account holder may have access to your information.
- **Transactions.** We may provide your information to third-party service providers to process transactions or otherwise provide you service, such as billing companies or shipping services, or when roaming on another carrier's network.
- **Acquisitions.** We may also transfer your information in a corporate business transaction, such as a merger or acquisition.

- **For Legal Process and Protection.** We will provide customer information where necessary to comply with the law, such as disclosure of your information to a law enforcement agency for your safety or the safety of others, or when compelled by subpoena or other legal process.
- **De-Identified Data.** We may provide your de-identified information to third parties for marketing, advertising, or other purposes.

Learn more about how we share information with third parties

- **Third Party Applications.** When you install third party applications on your device, you may consent to third-party access to information from your device or on our network, such as your contact list or location. Third-party application information collection is not covered under our Privacy Statement.

Learn more about third-party applications

How We Store and Protect the Information Collected About You

- **Protecting Your Information.** We use a variety of safeguards to protect the information we collect about you.
- **Retaining Your Information.** We retain information collected about you for only as long as we need such information for business, legal, or tax purposes.

Learn more about how we safeguard customer data

How You Can Update Your Information and Choose How We Contact You

- **Access.** You can help ensure that information we have about you is accurate, complete, and up-to-date by accessing your account at my.t-mobile.com, at a T-Mobile store, or by calling Customer Service.

Learn more about how you can correct your information

- **Marketing Communications.** You may manage your marketing communications preferences through my.t-mobile.com. Noncustomers and customers may manage their marketing preferences by completing T-Mobile's Marketing Communications Preferences form.

Learn more about your choices

Your Role in Protecting Your Privacy

You play an important role in protecting your information. For more information please see Protecting Your Privacy

Privacy Statement Updates and Contact Information

Statement Changes. We may change this Statement at any time.

Notice. If we propose to use Personal Information in a materially different way, we will provide you with notice by posting notice of the changes on our website for at least 30 days before we implement those changes, and obtain your consent as specified above for any material change regarding disclosure of Personal Information.

Check Back Often. You should review this Privacy Statement often for changes.

Contact Us. If you have any questions or comments about this statement or about T-Mobile's privacy practices, please send an e-mail message to privacy@t-mobile.com or call Customer Service at 611 (from a T-Mobile phone) or 1-800-937-8997 (from any phone). You may also direct your privacy-related comments or questions to the address below:

T-Mobile USA, Inc.
Attn: Chief Privacy Officer
12920 SE 38th Street
Bellevue, Washington 98006

T-Mobile Privacy Statement

December 31, 2016
Please click here for Spanish version of the T-Mobile Privacy Statement
Please click here for the T-Mobile Privacy Statement Highlights

This Privacy Statement ("Statement") describes how information about you is collected, used, and disclosed by T-Mobile USA, Inc. ("T-Mobile") and provides other important privacy information, describes when and how we may change this Statement, and tells you how to contact us with any questions or comments.

WHAT TYPES OF INFORMATION WE COLLECT ABOUT YOU

top

We collect information about you and your associated device(s) when you use our products or services or otherwise interact with us or with third-party services through our products and services. Examples of the types of information we collect include:

Personal Information

"Personal Information" means information that we directly associate with a specific person or entity (for example, name; addresses; telephone numbers; email address; Social Security Number; call records; wireless device location). Personal information does not include "de-identified," "anonymous," or "aggregate" information – which are not associated with a specific person or entity.

Customer Proprietary Network Information (CPNI)

Customer Proprietary Network Information, or "CPNI", is a subset of Personal Information that is generated in connection with the telecommunications services we provide to you. CPNI includes, for example, call details, call location information, and certain information about your rate plans and features. CPNI does not include your name, address, and phone number.

For more information see CPNI

Credit and Financial Information

We collect information about your credit card or banking information, Social Security Number, and credit history for account opening, management and billing and collection purposes. Financial information we collect is governed by T-Mobile's Financial Privacy Statement

Network and Device Information

We may collect information about your use of our network (or other carriers' networks when roaming domestically and internationally) and the device(s) associated with your account, network data related to WiFi usage and device, and performance information, as well as data relating to your use of our website, applications and other

products and services.

Location Data
We may collect your device's location whenever it is turned on (subject to coverage limitations).

Performance and Diagnostic Data
We may collect performance and diagnostic data about your use of our network, networks you roam on, WiFi services or your device. For example, we may collect information about the performance of the device, signal strength, dropped calls, data failures, battery strength and other device or network performance issues. We may also collect information about applications on your device, the fact that an application has been added, when an application is launched or fails to launch, and length of time an application has been running.

Telematics
If you are a customer of the T-Mobile SyncUp connected car service, we, and our application provider, collect data from the SyncUp device in your car. This data includes driver behavior information such as acceleration and braking, speed, and RPM. The device also reports vehicle location via GPS and can report on common vehicle issues called Diagnostic Trouble Codes (DTC).

Video Data
When you use a T-Mobile video application, for example T-Mobile TV, on your device, we may collect information about the programs you watch to determine customer viewing habits so that we can tailor video selections to you or our customers.

Back Up and Cloud Services
Some devices may automatically upload to T-Mobile network servers information you have stored on the device and/or SIM card in order to facilitate specific functions. For instance, some devices may back-up your address book, photo album, or diagnostic data. You may choose to disable such uploads, but this may affect functionality of the device or your services. We may also provide you the ability to upload other information from your device to T-Mobile or third-party network servers. For instance, you may have the option to upload pictures, text messages, recordings, calendars, tasks, or notes.

Collection of Information About Children
We do not knowingly solicit children to purchase our services or products. If, however, you authorize a child to use our services or products by providing them a device associated with your account, any information associated with such use will be treated as your information in accordance with this Statement. If you are the primary account holder, you will have the ability to set the marketing preferences for any other lines on your account, including those for any children to whom you provide a device.

Our websites are not designed to attract children under the age of 13 and we do not intentionally or knowingly collect Personal Information on our websites from anyone under the age of 13. We encourage parents to be involved in the online activities (including wireless Internet browsing) of their children to ensure that no information is collected from a child without parental permission.

HOW INFORMATION ABOUT YOU IS COLLECTED

top

T-Mobile collects information about you in three primary ways:

Information You Provide

We collect information that you provide to us when you apply for, purchase, or use our products or services, or otherwise communicate with us.

For example, some of the ways you may provide information to us include:

- When you sign up for our voice or data services or purchase other products or services, we may collect personal contact, billing, and credit information.
- When you establish or modify an online account, we may collect user identification information, passwords, and/or security question responses that you will use for future sign-on.
- When you interact with our customer service representatives, enter information on our websites, submit survey responses, or pay for services, we may also collect Personal Information and other information. We may monitor and record phone calls, e-mails, live chats, or other communications between you, your device, and our customer service representatives or other employees or representatives.
- When you use our services on a phone provided to you by an account holder.

Information We Collect Automatically

We automatically collect a variety of information associated with your use of your device (on our network, when roaming, or in WiFi mode) and our products and services, some of which may be associated with you or another user on your account.

For example some of the ways we may automatically collect information include:

- Our systems capture details about the type and location of wireless device(s) you use, when the device is turned on, calls and text messages you send and receive (but we do not retain the content of those calls or messages after delivery), and other data services you use.
- We may also gather information about the performance of your device and our network. Some examples of the types of data collected include: the applications on the device, signal strength, dropped calls, data failures, and other device or network performance issues.
- **Cookies, Web Beacons, and Similar Technologies**
  We may use, or we may engage third-parties to use on our behalf, cookies (small data text files placed on your computer or device) or similar technologies to identify your computer or device and record your preferences and other data so that our websites can personalize your visit(s), see which areas and features of our websites are popular, and improve our websites and your experience.

  We may also use web beacons (small graphic images on a web page or an HTML e-mail) to monitor interaction with our websites or e-mails. Web beacons are generally invisible because they are very small (only 1-by-1 pixel) and the same color as the background of the web page or e-mail message.

  The information we receive through cookies, web beacons and similar technologies may enable us to recognize users across devices, such as smartphones, computers, tablets or related browsers. Depending upon your device or computer, you may be able to set your browser(s) to reject cookies or delete cookies, but that may result in the loss of some functionality on our websites. If we combine or link cookie or web beacon information with Personal Information, we will treat the combined or linked information as Personal Information under this Statement.

- **Web Browsing Activity**
  Our Websites. When accessing our websites, mobile websites and related applications and widgets designed for your device or web-based experience, we automatically collect certain information about your device and your visit, such as your IP address, browser type, date and time, the web page you visited

before visiting our website, your activities and purchases on our websites, and other analytical information associated with the sites.

Other Websites. When your device's web browser utilizes our data services to access websites other than our own, we automatically capture information associated with your browsing activities, and measure and monitor network and Internet connection performance, throughput, latency, and similar network data.

Do Not Track Statement. Some browsers have incorporated "Do Not Track" features. Most of these features, when turned on, send a signal or preference to the websites you visit indicating that you do not wish to be tracked. Those sites (or the third party content on those sites) may continue to engage in activities you might view as tracking even though you have expressed this preference, depending on the sites' privacy practices. Because there is not yet a common understanding of how to interpret the DNT signal, we do not currently respond to the browser DNT signals when you use our services and products or interact with our websites or online services. We do allow you to exercise choice regarding the collection of information by third parties about your online activities over time and across third-party websites or online services for online interest based advertising purposes and to opt out of our interest-based advertising on your device, as described below.

- **Voice Controlled Applications**
  If you use a voice-controlled application, that application may collect and record your requests and other information from you and your phone.
- **Retail Beacons**
  We may use beacon devices in our retail locations that collect data about your device. These programs use signals from smart devices (like mobile phones and tablets) to track movement and wait times. Retail beacons collect a unique identifier that your device routinely transmits (e.g., a MAC address) and coverts it to an identifier unique to T-Mobile. In some cases, we will use identifiers that are already routinely collected by the T-Mobile network in order to provide you with wireless service. We use aggregated data in order to understand general traffic trends in our stores. This helps us to better service our customers.

Information From Other Sources

We may also obtain information about you from other sources. For example, we may receive credit information from third-party sources before initiating your service, or background information in connection with employment opportunities. We may also obtain updated address information from our shippers or other vendors. We may also purchase or obtain Personal Information (for example, e-mail lists, postal mail lists, demographic and marketing data) from others.

HOW WE USE INFORMATION WE COLLECT ABOUT YOU

top

We use the information we collect for a variety of business purposes, such as:

- To route your calls or message or otherwise provide you with service;
- To provide and bill for products and services you purchase and charge to your account;
- To deliver and confirm products and services you obtain from us;
- To verify your identity and maintain a record of your transactions and interactions with us;
- To provide customer and technical services to you;
- To create, modify, improve, enhance, remove or fix our network, products and services, and their performance;
- To identify and suggest products or services that might interest you;
- To make internal business decisions about current and future product and service offerings;
- To provide you customized user experiences, including personalized product and service offerings;

- To protect our rights, interests, safety and property and that of our customers, service providers and other third parties; and
- To comply with law or as required for legal purposes.

Fraud Prevention
We may use Personal Information, including voice print recordings, account information (such as purchase patterns) and device information for investigations or prevention of fraud or network abuse. We provide fraud prevention services to banks or other third parties. As part of this service, we may verify your phone number to help those third parties prevent your personal information from being used for fraudulent purposes. We also may provide the information you report as spam to 7726 to a third party to prevent fraud or network abuse, and we may share such information with government agencies and others that work to combat spam and prevent fraudulent, deceptive, and unfair practices.

Information Collected from Cookies
We may also use information collected from cookies or other similar technologies to improve our websites, make recommendations, and complete transactions you request.

Marketing
We may use information we collect to contact you about T-Mobile or third-party products, services, and offers that we believe you may find of interest. We may contact you by telephone, postal mail, e-mail, or other methods. You may opt-out of receiving marketing communications from us at any time as outlined below in Choices Regarding Use of Your Information.

Directories
We do not publish directories of our customers' wireless numbers; nor will we provide or make such numbers available to third-parties for listing in their public directories, without the customer's prior consent.

Performance, Diagnostics & Management
We collect information about devices, our network and WiFi usage to perform diagnostic analyses and understand how your device is performing overall. Diagnostic data helps us troubleshoot technical issues related to your device's performance such as battery life, dropped calls, processing speed, device memory, service coverage, and network and WiFi signal strength that you and other customers may experience. If you are using a device in WiFi mode, we may collect information about that usage, such as the routing address and IP address. We also may use diagnostic data to identify and recommend products and services.

Location-Based Services
We use location information to route wireless communications and to provide 911 service, which allows emergency services to locate your general location. We may disclose, without your consent, the approximate location of a wireless device to a governmental entity or law enforcement authority when we are served with lawful process or reasonably believe there is an emergency involving risk of death or serious physical harm.

Depending on your device, you may also be able to obtain a wide array of services based on the location of your device (for example, driving directions, enhanced 411 Directory Assistance, Find My Device, or search results, etc.). These data services, known as Location-Based Services ("LBS") are made available by us and others, usually via applications. These services use various location technologies and acquire location data from various sources.

These applications and services use various location technologies (including Global Positioning Satellite ("GPS"), Assisted GPS ("AGPS"), cell ID and enhanced cell ID technologies) to identify the approximate location of a device, which is then used in conjunction with the application to enhance the user's experience (for example, to

provide driving directions, to provide enhanced 411 Directory Assistance, or search results, etc.)

LBS may, or may not, involve any interaction with or dependency on our network, and location-based services may or may not look to our network to obtain location data. Where we allow third parties the capability of accessing data about your location that is derived from our network, we require those third parties to observe specific privacy and security protections consistent with this statement.

It is important that you understand the location capabilities and settings of your device, and that you carefully read and understand the terms under which these services are provided – whether by us or another entity.

You should carefully review the privacy statements and other terms of third-parties with whom you have authorized the sharing of your location information, and you should consider the risks involved in disclosing your location information to other people.

Where we provide a location-based service, you will receive notice of the location features of the service and collection of location data is with your consent. You will be provided options for managing when and how such information should be shared (except in the case of certain parental controls or similar services associated with enterprise or multi-line accounts – for example, T-Mobile's FamilyWhereTM services – which may be managed solely by the primary account holder or their designee, but always with notice to the end-user). T-Mobile follows the CTIA's Best Practices Guidelines for Location-Based Services, which are available here.

For more information on location services, see Location Services

Telematics
Data from our SyncUp connected car service is used to provide you with that vehicle monitoring service, to enable the functions of the SyncUp associated Motion app, and to enable WiFi connectivity in your car. In addition, your data may be shared with our application provider in order to enable third-party services that use your personal data, though in such cases no third-party will be granted access to data that identifies you without first obtaining your consent. We may also use such data for any of the other purposes listed in this statement, such as internal analysis, or to personalize offers we provide to you.

Advertising
You may see advertisements when you visit our websites, mobile websites, in mobile applications, or on your device. We may help advertisers better reach our customers by providing certain information, including device type, geographic information, language preferences or demographic information obtained from other companies to allow advertisers to determine which ads may be more relevant to you. However, we do not share Personal Information for advertising purposes outside of our corporate family without your consent.

Some examples of the types of advertising you might see include:

Our Ads on Our Websites. We may provide advertisements, such as banner ads, on our websites, mobile websites, and in mobile applications and widgets you may download, access or use on your device.

Other Company Ads on Our Websites. You may also see third-party advertisements on some T-Mobile websites, services, or in applications, or on devices. These third-party advertisers, or their ad networks, may place or access cookies, web beacons, or similar technologies on your device, or use your device identifier, and may collect certain anonymous or de-identified information about your visit on our websites. The third-party advertisers who provide these ads may use this information to provide you with advertising on our websites, as well as on other websites. We do not have control over or access to any information contained in the cookies that are set on your computer or device by ad servers, ad networks, or third-party advertisers.

Our Ads on Other Websites. We may ask third-parties to place advertisements about our products and services on other websites, mobile websites and in mobile applications and widgets. The use of cookies, web beacons, or similar technologies by such third-parties on other websites is subject to any applicable privacy statements that they may have, not this Statement.

Interest-Based Ads. You may receive ads from us and our ad providers that are tailored to your interests. These interest-based ads are selected based on your use of our services and products as well as other information obtained by us and our ad providers. None of this information is Personal Information.

- We do not provide your Personal Information to third-party advertisers without your consent.
- Advertising may be tailored to the interests that advertisers have inferred from your browsing of our websites or other websites or applications with which the third-party partners to provide advertising.
- We may provide third-party advertisers with aggregated or de-identified location, demographic or similar data (unrelated to your browsing activities) that does not personally identify you. This data may be used by advertisers to help tailor their ads on our websites, and on other sites and applications.
- We, and our providers, may use a de-identified profile of your web-browsing and application use activity and interests. This profile does not contain information that identifies you personally, but may include a unique or encrypted identifier that enables your device to be matched to a profile of your browsing activity and de-identified characteristics about your interests.
- When we use information associated with your web browsing activities on websites that are not our own to provide interest-based advertising or offers, we will provide you with notice and appropriate choice.

  For more information see T-Mobile Ad Options

Choices About Advertising.

T-Mobile adheres to the Digital Advertising Alliance's ("DAA") Self-Regulatory Principles for Online Behavioral Advertising.

- *On Your Mobile Device.* Where we offer interest-based ads, you can opt-out of certain interest-based advertising by clicking on the ad options link on or near the advertisement or by clicking here.
    - If you turn off interest-based ads, you will still see just as many ads, but the ads may not be based on your interests and may be less relevant to you.
    - Your choice only affects the ads you see on websites and applications you access on your device.
    - If your device's browser cookies are deleted, or your device is reset, you may need to reset the interest-based ads feature.
    - If you are using your device, but are not on our network (such as a WiFi network), we, and our ad providers, may not be able to identify your ad choices.
- *On Your Computer or Non-Mobile Device.* For information about targeted advertising, or to opt-out of use of your browser information for purposes of certain third-party advertising, please visit

www.aboutads.info/choices. Please note that if you opt out, you will continue to receive the same number of ads, but they may be less relevant because they will not be based on your interests. You may still see ads related to content on a web page or based on other nonpersonal information. Please note that this opt-out is cookie-based. If you change computers or devices, change web browsers, or delete cookies, you will need to visit the aboutads site and opt-out again.

WHEN WE SHARE INFORMATION COLLECTED ABOUT YOU

top

We do not sell, license, rent, or otherwise provide your Personal Information to unaffiliated third-parties (parties outside the T-Mobile corporate family) to market their services or products to you without your consent. We may, however, disclose your information to unaffiliated third-parties as follows:

With Your Consent

We may disclose Personal Information about you to third-parties with your consent. We may obtain your consent in writing; online, through "click-through" agreements; when you accept the terms of disclosures on your phone for certain applications or services; orally, in our stores or on the phone, including through interactive voice response, or implicitly, for example, when you purchase a product and ask that it be shipped to your home, consenting to our disclosure of your name and address to a third-party shipping company to complete delivery.

To the Primary Account Holder

We may disclose information about an account user to the primary account holder (the party financially responsible for the account). If a business, governmental agency, or other individual obtains service for you, that entity or individual is our customer, and we may provide information about you or your use of the service, products or devices to them or others at their direction.

When you are the primary account holder, but you receive special or discounted pricing, terms, or other benefits through another party’s agreement with us (for example, an employee discount), we may provide enough information to that party to verify your initial and continuing eligibility for benefits under their agreement with us and to calculate any associated discounts.

To Our Service Providers

We may disclose information to third-party vendors and partners who complete transactions or perform services on our behalf (for example, credit/debit card processing, billing, shipping, repair, customer service, auditing, and marketing).

Third-Party Carriers and Suppliers

If you are roaming on the network of another carrier or WiFi service provider, your wireless telephone number, your location, the numbers you dial, and other information about your usage will be available to that carrier to facilitate that service. Additionally, services and functionality offered through certain devices are sometimes provided in conjunction with entities other than T-Mobile. As a result, Personal Information from your devices may be uploaded and stored on their servers. For instance, BlackBerry® service is provided in conjunction with Research in Motion (RIM), and Personal Information from your device is stored on their BlackBerry Enterprise ServersTM. Their specific terms and conditions, terms of use, and privacy statements apply to those services.

In a Business Transfer

We may sell, disclose, or transfer information about you as part of a corporate business transaction, such as a merger or acquisition, joint venture, corporate reorganization, financing, or sale of company assets, or in the unlikely event of insolvency, bankruptcy, or receivership, in which such information could be transferred to third-

parties as a business asset in the transaction. We may also share information with banks for purposes of transferring loans in connection with your device financing.

For Legal Process & Protection

We may disclose Personal Information, and other information about you, or your communications, where we have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary:

- To satisfy any applicable law, regulation, legal process or enforceable governmental request;
- To enforce or apply agreements, or initiate, render, bill, and collect for services and products (including to collection agencies in order to obtain payment for our products and services);
- To protect our rights or interests, property or safety or that of others;
- In connection with claims, disputes, or litigation – in court or elsewhere;
- To protect users of our services and other carriers or providers from fraudulent, abusive, or unlawful use of, or subscription to, such services;
- When information is reported to the Spam Reporting Service, it may be shared with government agencies and others that work to combat spam and prevent fraudulent, deceptive, and unfair practices;
- To facilitate or verify the appropriate calculation of taxes, fees, or other obligations due to a local, state, or federal government; or
- In an emergency situation.

Co-Sponsored Websites and Partners

If you provide information to us in connection with a co-sponsored website, this Statement will apply to our use of the information and the co-sponsor's statement will apply to their use of the information. If you purchase equipment or activate service at one of our partner's locations (including websites of such dealer or retailer), they may request information from you that is passed to us as part of the activation process, but which may also be retained by the partner. This Statement will govern our use of such information, and the partner's privacy statement will govern its use of such information.

De-Identified Information

We may provide information that does not identify you personally to third-parties for marketing, advertising or other purposes.

For more information about our INSIGHTS Program see T-Mobile INSIGHTS

Third-Party Applications for Your Devices

We are not responsible for the third-party applications (for example, applications, programs, widgets, etc.) you select and install on your device. When you install third party applications, you may give your consent for the third party to access information stored on the device and on our network to facilitate the application's functions (for example, you may consent to third-party access to your location information – see Location Based Services). The manner in which such third-parties may use, share, or disclose such information is governed by the terms and conditions and privacy statement provided by that third party – not by this Statement. For more information, see Device Apps

HOW WE STORE AND PROTECT THE INFORMATION COLLECTED ABOUT YOU

↑ top

Protecting Your Information

We use a variety of physical, electronic, and procedural safeguards to protect Personal Information from unauthorized access, use, or disclosure while it is under our control.

We provide password protected online access to your account information through my.t-mobile.com. For multi-line accounts, the primary account holder is authorized to access online account information for all the devices and lines on the account. Other users may generally access online account information related only to their respective device and line (for example, if a parent provides a device to their child, the child may access online information about that device and line– including CPNI). The primary account holder, however, may designate additional or more limited access rights for other users on the account.

Under federal law, you have a right, and we have a duty, to protect the confidentiality of CPNI and we have adopted statements and procedures designed to ensure compliance with those rules. We will not intentionally disclose your CPNI to third-parties without your permission, except as allowed under FCC rules, applicable law, or explained in this Statement. However, if you are the primary account holder, you may designate other "authorized users" (for example, a spouse) to access and manage your account information, including CPNI. For more information see CPNI

Retention and Disposal
We retain information only for as long as we have a business or tax need or as applicable laws, regulations, or government orders require. When we dispose of Personal Information, we use reasonable procedures designed to erase or render it unreadable (for example, shredding documents and wiping electronic media).

HOW YOU CAN UPDATE YOUR INFORMATION AND CHOOSE HOW WE CONTACT YOU

top

Access to Your Information
You may access and modify your contact information by visiting my.t-mobile.com or a T-Mobile retail store, or by contacting Customer Service. You may also contact us using the information in the How to Contact Us section below.

Choices Regarding Use of Your Information
We may send you communications about services or products we, or our partners, sell. We want to provide you with meaningful choices regarding our marketing communications, and you may choose to limit or opt-out of some marketing communications from us at any time. Although you may elect not to receive marketing information from us, if you subscribe to our services or buy our products, you will continue to receive invoices, customer-service and transactional notices, and similar communications. The Primary Account Holder can configure options for marketing communications for all lines on the account.

If you are a T-Mobile customer and you manage your account online, you can manage your preferences regarding marketing communications by logging into your my.t-mobile.com profile. If you do not manage your account online, or you are not a current T-Mobile customer, you may manage your preferences regarding marketing communications here.

You may also manage your preferences regarding marketing communications by contacting Customer Service by dialing 611 from your T-Mobile phone or 1-800-937-8997 from any phone, or, with respect to marketing e-mails, by following the "unsubscribe" instructions on any marketing e-mail we send you.

See also Marketing Choice

Do Not Call Registry
The FTC maintains a National Do Not Call Registry at https://www.donotcall.gov/, and your state may maintain its own Do Not Call Registry. Putting your number on these Registries also may limit our telemarketing calls to that number.

YOUR ROLE IN PROTECTING YOUR PRIVACY

top

You play an important role in ensuring the security of Personal Information. We encourage you to use safeguards to protect your information and devices. For more information please see Protecting Your Privacy.

OTHER INFORMATION YOU SHOULD KNOW

top

Consumer Code for Wireless Service

We follow the Consumer Code for Wireless Service established by the Cellular Telecommunications & Internet Association ("CTIA"). In doing so, we want to help customers understand their bills, receive quality service, and make informed choices and conform our information practices under this Statement to meet the requirements of applicable federal and state laws and regulations.

Your California Privacy Rights

California Civil Code Section 1798 entitles California customers to request information concerning whether a business has disclosed Personal Information to any third parties for the third parties' direct marketing purposes. As stated in this Statement, we will not sell or share your Personal Information with non-affiliated companies for their direct marketing purposes without your consent. California customers who wish to request further information about our compliance with this law or have questions or concerns about our privacy practices and statements may contact us as specified in the How to Contact Us section below.

PRIVACY STATEMENT UPDATES AND CONTACT INFORMATION

top

How We Communicate Changes to This Statement

We may update this Statement at any time to provide updates to or clarification of our practices. If we make changes, we will revise the date at the top of the Statement. If we propose to use Personal Information in a materially different way, we will provide you with notice by posting notice of the changes on our website for at least 30 days before we implement those changes, and obtain your consent as specified above for any material change regarding disclosure of Personal Information. You should refer to this Statement often for the latest information and the effective date of any changes.

How to Contact Us

If you have any questions or comments about this Statement or about T-Mobile's privacy practices, please call Customer Service at 611 (from a T-Mobile phone) or 1-800-937-8997 (from any phone) or send an e-mail message to privacy@t-mobile.com. You may also direct your privacy-related comments or questions to the address below:

T-Mobile USA, Inc.
Attn: Chief Privacy Officer
12920 SE 38th Street
Bellevue, Washington 98006

T · ·Mobile·®

CODE OF BUSINESS CONDUCT

EXHIBIT "C"

TABLE OF CONTENTS

A Message From John:

We've spent the past several years forcing change on the wireless industry and our Un-carrier strategy continues to deliver fantastic results.

How we do things along the way is just as important as the results we deliver. We move fast, we turn on a dime, and we play hard - but we will never sacrifice our core values just to get ahead.

We all have a role to play. Our continued success relies on earning the trust of our customers, suppliers and business partners, and one another each and every day. We all have an obligation to conduct business with uncompromised ethics. Winning is important, but how we get there matters!

Our Code of Business Conduct provides clear expectations on how we "Do it the right way" at T-Mobile. Take a few minutes, read it, internalize it and use it to help guide decisions and choices we all make on a daily basis. Whatever your responsibilities at T-Mobile may be, you're responsible for conducting yourself according to these high standards.

It's important that we continue to make honest assessments about how we're doing things along the way. If you feel someone's falling short of our Code, I want you to speak up. It makes no difference who you are, or who they are—what's important is that we take action to get back on track. And know that we have your back—retaliation of any kind will not be tolerated. Period.

Let's keep working hard to disrupt the wireless industry—and let's keep doing things the Un-carrier way—the right way!

HOW WE PLAY

HOW WE PLAY

WE PLAY TO WIN AND HAVE FUN. AND WE DO IT THE RIGHT WAY.

HOW WE PLAY

We're changing the wireless industry! And we're doing it the RIGHT Way—by following high standards. You'll find those standards in this Code of Business Conduct.

The Code is a snapshot of the legal and policy requirements we follow here at T-Mobile as part of our commitment to ethical business practices. Keep in mind it's a guide, not the last word. If you need more detail, take a look at our company policies.

All of us at T-Mobile and its subsidiaries—employees, officers and board members—are expected to uphold this Code.

We take this expectation seriously.

- No one can ask you to break the Code.
- Waivers of any Code requirement for executive officers and members of the T-Mobile Board of Directors can be made only by the T-Mobile Board, and will be promptly disclosed to shareholders.
- Code violations can land you in a world of trouble. You could face discipline, and even get fired.

Ask Questions

Look, the Code can't cover everything. Life is complicated, and sometimes throws surprises at you.

When you're faced with a difficult decision, and the Code isn't helpful, do the smart thing: **Stop. Think. Ask.**

OK, let's break this down:

Stop: Don't make a snap decision. When in doubt, step back and think about things.

Think: Before you act, ask yourself these questions. Act only if the answer to ALL of them is "yes":

- Is my action legal?
- Is it consistent with our Code and T-Mobile policies?
- Is it the right thing to do for customers, co-workers, shareholders, suppliers, and business partners?
- Would I feel OK about my action if I read about it on someone's Facebook page? Or if my mom knew about it??

Ask: Not sure if the answer to each question is "yes"? Ask for help. And keep asking until you're satisfied that you'll do something that will make Team Magenta proud.

Got a question? We're here for you.

- Your manager or next-level manager
- Human Resources business partner or Legal Affairs partner
- T-Mobile Compliance & Ethics
- Our 24/7 Integrity Line at 1-866-577-0575 or www.T-MobileIntegrityLine.com (Anonymous questions are OK)
- Or, you can connect with "Additional Resources" that are available to help.

HOW WE PLAY

Speak Up

If you see something that violates the law or the Code, say something. Follow your gut. Something doesn't seem quite right to you? Then it probably isn't. Call it out so it can be dealt with and everyone can get back to doing things the right way.

What's the best way to report a concern? You can always start by talking with your manager, next-level manager or Human Resources business partner.

If you're not comfortable using these resources, or don't feel they resolved your concern, contact T-Mobile Compliance & Ethics. This team is available to all T-Mobile employees, customers, suppliers, shareholders, and business partners who want to raise concerns.

T-Mobile provides several other ways to report a concern:

- Our Integrity Line: This 24/7 resource is managed by a leading third-party reporting service. You have the option to remain anonymous.
  - By phone: 1-866-577-0575
  - By web: www.T-MobileIntegrityLine.com
- Our Chief Compliance Officer
- The Chair of the Audit Committee (Board of Directors)

Questions and concerns about accounting, internal accounting controls, or auditing issues (or other issues) can be submitted (including anonymously) to:

T-Mobile Audit Committee Chair
c/o Chief Compliance Officer
T-Mobile US, Inc. 12920 S.E. 38th St.
Bellevue, WA 98006

We hope you'll use these resources. But keep in mind, nothing in this Code or in any company policy or agreement prevents you from making a good faith report to outside governmental or regulatory authorities.

No matter how you choose to report, we'll review and investigate your report with care. And we'll let you know when we're done.

Because we're committed to doing things the right way, violations of the legal or policy requirements in this Code could result in discipline, including job termination.

Don't Retaliate

We don't tolerate retaliation—ever. Anyone who reports a possible violation of the law, this Code or any company policy in good faith is protected from retaliation. Any employee who is found to have retaliated may be disciplined and could lose their job.

Whistleblower Protection Policy

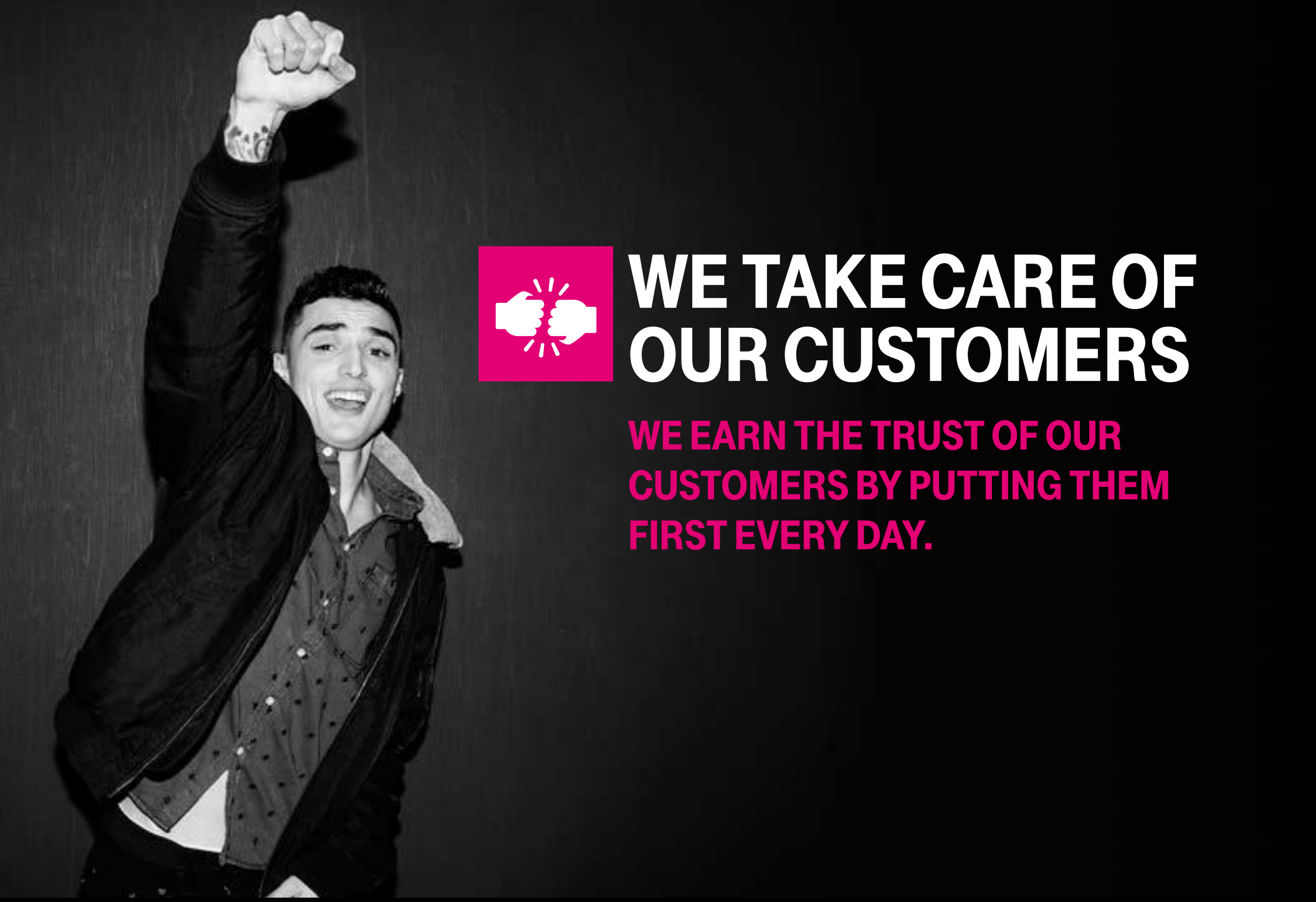
Leaders Set the Tone

We expect our managers to lead by example and encourage everyone to do things the right way.

What do we mean by that? We mean that T-Mobile leaders follow the Code every day and expect the people who work for them to do the same. We want our leaders to take it to the competition, but in a way that meets our high ethical standards. And no one should ever feel they're being asked to bend the rules to meet a company goal.

It also means that our leaders take care of problems before they become bigger problems. If an employee sees something that worries them, our leaders listen to that employee and let them know that speaking up is the right thing to do.

Finally, it means that our leaders forward reported legal or Code violations to T-Mobile Compliance & Ethics. And leaders demonstrate zero tolerance for retaliation. No one gets punished for raising a good faith ethical concern or possible legal or Code violation.



WE TAKE CARE OF OUR CUSTOMERS

WE EARN THE TRUST OF OUR CUSTOMERS BY PUTTING THEM FIRST EVERY DAY.

WE TAKE CARE OF OUR CUSTOMERS

Treat Customers Honestly and Fairly

Why do customers love T-Mobile? Because we listen to them, then go all out to meet their needs. That doesn't mean over-selling. It means giving customers honest and complete information about our great products and services. It means delivering what we promise. And we never charge customers for things they haven't authorized.

Guard Customers' Private Communications

Customers expect us to protect their private communications. And we do! We'll comply with government requests for customer communications, but only to the extent the law requires. Be sure to refer all government and law enforcement requests for customer communications to the Law Enforcement Relations Group.

Protect the Confidentiality of Customer Information

Customers entrust a lot of sensitive information to us—credit card numbers, Social Security numbers, addresses, all sorts of things. We hold other customer information as well, like call detail records and location data. Here's the thing: We protect the confidentiality of our customers' information. We collect, use, and store this sensitive information only so far as is permitted by law, T-Mobile Terms & Conditions, and company policies.

When it comes to customer information, we're also careful about access and disclosure: We access this information only when we need to when doing our job—and only to the extent our job duties allow. And we access customer information only for the legal and business reasons listed in our Terms & Conditions and Privacy policies, or when we have received advance authorization from the customer or our manager. We share customer information only if the customer says we can or we're allowed to by the law, our Terms & Conditions, or Privacy policies.

If the police, the government, or an attorney is asking for customer information, notify the Law Enforcement Relations Group.

- T-Mobile Privacy Policy
- MetroPCS Privacy Policy
- CPNI Policy
- Customer Location Information Policy
- Terms and Conditions

Honor Rules That Apply to Governmental Customers

Working with governmental customers takes particular care. They have special bidding, pricing, disclosure, contracting, and certification requirements for companies with which they do business, like us. They also have specific rules about gifts and entertainment, political donations, and who can contact government employees to market goods and services during active government procurement opportunities or under an existing government contract.

We completely get what it means to work with the government, and go to the extra lengths that government rules require.

- Political Activities & Lobbying Policy
- Anti-Corruption Policy

WE RESPECT EACH OTHER AND OUR ENVIRONMENT

WE SUCCEED BY DOING RIGHT BY EACH OTHER AND OUR ENVIRONMENT.

WE RESPECT EACH OTHER AND OUR ENVIRONMENT

Do Not Tolerate Discrimination or Harassment

We love our diverse workforce, and our culture of inclusion. All the great ideas and different viewpoints our co-workers bring to work are what make T-Mobile such a great place.

Help keep our awesome work environment awesome. Don't discriminate and don't engage in unlawful harassment (such as sexual harassment). We follow laws against discrimination everywhere we do business.

Protect Confidential Employee Information

Our customers expect their privacy, and so do our co-workers. So we respect it. We don't access or take employee information from company systems unless required for authorized legal or business reasons. And only people who need to know can access or take this information.

Acceptable Use Policy for Information and Communication Resources

Put Health and Safety First

We want everyone to be safe on the job. So we work hard to prevent accidents and injuries by reducing workplace hazards and complying with all safety laws and regulations.

What's more, we follow T-Mobile's health and safety program, complete required training, and follow the safe work practices that apply to our jobs. We also look out for each other by reporting and investigating workplace injuries and by being prepared to respond to potential emergencies.

If you see something that could pose a hazard, correct it. If you can't, tell your supervisor, site safety contact, or local facility manager immediately, so they can address it. If you have safety questions or concerns, e-mail Safety@T-Mobile.com, or call the Safety Hotline at 877-604-SAFE (7233).

Environmental, Health and Safety Policy

Environmental Health and Safety Standard

T-Mobile Employee Safety Site

Minimize our Impact on the Environment

We know our customers try to go green, and we do the same. We strive to make business decisions that preserve the environment. And we work to minimize waste and maximize natural resources through product reuse and recycling, cutting energy use, sustainable product packaging, waste reduction initiatives and ride sharing. Every sustainable contribution helps and we're committed to doing our part!

And that includes following laws protecting the environment everywhere we do business.

T-Mobile Sustainability Site

24/7 WE DEMONSTRATE INTEGRITY 24/7

WE'RE TRANSPARENT. WE DO THE RIGHT THING EVEN WHEN NOBODY IS WATCHING. OUR BUSINESS DECISIONS ARE BASED ON BUSINESS FACTORS. PERIOD.

WE DEMONSTRATE INTEGRITY 24/7

Don't Steal or Deceive

Theft and fraud hurt our reputation, our brands, and every one of us. So we don't embezzle, steal, or take money, property, or services that don't belong to us.

Maintain Accurate Records and Reports

Each of us must be sure that the records and reports we produce are accurate and complete. Our financial and accounting records must be correct and include all transactions and assets. And we don't mislead, record things that didn't happen, or leave out important information. That goes for financial reports, documents and communications as well, including those we file with the Securities and Exchange Commission and provide to investors.

In addition, we don't hide cash or company assets or use them for unauthorized purposes or to break the law. Lastly, any report or statement filed with or given to the government or the public must be accurate, complete, and timely.

Anti-Corruption Policy

Travel, Expense and Corporate Card Policy

Avoid Conflicts of Interest

Lots of us have outside interests. It's important that those activities are legal (of course!), and that they don't get in the way of doing what's best for T-Mobile when we're doing our jobs. If they do, that's called a conflict of interest.

Conflict of interest is hard to define because it can take many forms. Put simply, it's when your personal interest, relationship, or activity influences—or can be seen by others as influencing—your ability as a T-Mobile employee to do what's best for the company.

Here are some examples: You have a family member who needs a job, so you hire them to work for T-Mobile. Conflict! Or you start dating someone you supervise. REALLY a conflict. Let's say you take a job working part-time in a competitor's wireless store. Big conflict. Or you participate in the selection of a vendor that your spouse works for or a friend owns. Yep, conflict.

Sometimes conflicts seem innocent. After all, maybe you're just trying to help a friend or relative. Or you're confident the conflict won't affect your work for T-Mobile. But to make sure you're doing the right thing and not risking your own job, talk over the situation with your manager.

Be aware that the activities of OTHERS can create a potential conflict of interest for YOU. Like if your brother hires on with a T-Mobile supplier. Or your wife starts working for a competitor. You haven't done anything, but now you have a potential conflict.

The best way to prevent conflicts is to avoid those things that could be seen as influencing you on the job. But is this always reasonable or necessary? No! That's why you must tell your manager and Human Resources business partner about personal interests, relationships, and activities that could conflict with your job. They'll review the situation and advise you on what to do. You can also contact T-Mobile Compliance & Ethics.

Another kind of conflict is when you use your T-Mobile position to benefit yourself. Like scoring game tickets from a vendor by hinting you can give them some T-Mobile work. Or taking for yourself business opportunities you learn about at work that T-Mobile would be interested in pursuing. Always avoid these conflicts.

Lastly, NEVER compete with T-Mobile. But why would you want to?

Avoiding Conflicts of Interest Policy

Note: The provisions of our certificate of incorporation regarding the duties of non-employee members of the board of directors takes precedence over any provision in this section that is in conflict.

WE DEMONSTRATE INTEGRITY 24/7

Exchange Only Reasonable Business Gifts and Entertainment

It's a normal part of doing business—you want to take a potential business partner to dinner, or a vendor wants to show their gratitude to you with some kind of gift.

These things are generally OK, so long as these gift and entertainment conditions are met:

- They're legal and serve a legitimate business purpose.
- They're not an effort to influence a business decision or gain special treatment, and are not likely to be seen as one.
- Gifts from a single giver don't exceed $100 in value in a calendar year.
- The gift is not cash (or a cash equivalent).
- The entertainment is not frequent or routine.
- They would not embarrass T-Mobile if word got out.
- The gifts or entertainment you give are accurately reflected in accounting records and expense reports.
- A gift or entertainment (including meals) does not go to a government employee or the employee of a government-owned business, unless you have a written OK from T-Mobile Compliance & Ethics.

Sometimes vendors may give us products or services to evaluate. And sometimes T-Mobile may give phones or accessories to another company or an organization for business reasons. That's generally fine, as long everyone knows what's going on, it's legal, and it aligns with T-Mobile's business interests.

It's fine if you attend a social function hosted by a vendor or supplier. Just talk with your manager first and make sure the event meets the conditions we just mentioned.

Make sure that corporate charitable donations to a non-profit organization follow our Charitable Contributions Policy.

Finally, never ask our vendors, suppliers or other business partners for gifts or entertainment.

- Anti-Corruption Policy
- Charitable Contributions Policy
- Gifts and Business Entertainment Policy
- Political Activities & Lobbying Policy
- Travel, Expense and Corporate Card Policy

Don't Buy or Sell Stock When You Have Material Non-Public Information

As a T-Mobile employee, you probably know lots of stuff about the company that outsiders don't. That may include information that isn't yet public and could move our stock price. When that's the case, you cannot buy or sell T-Mobile stock. Same thing when you've become aware of information about a third party on the job, including a T-Mobile supplier or vendor, that isn't yet public and could affect its stock price; don't buy or sell the stock. It's also against our policy—and is likely illegal—to give friends and relatives tips on whether to buy or sell stock when you have material non-public information that could affect its price.

- Policy on Securities Trading

WE DO BUSINESS THE RIGHT WAY

WE PLAY HARD, AND WE PLAY FAIR. IT'S HOW WE ROLL.

WE DO BUSINESS THE RIGHT WAY

Uphold T-Mobile's Anti-Corruption Commitment

It goes without saying that corruption is bad for business and it's bad for society. We follow all U.S. and foreign laws barring corruption and bribery.

That means we don't offer or take bribes or kickbacks from anyone—whether a government official or private person. In other words, never offer or take anything of value to improperly influence a business or government decision, or to create a return obligation or expectation of favorable treatment.

Anti-Corruption Policy

Travel, Expense and Corporate Card Policy

Compete Fairly

We take care of our customers by fixing pain points. We've ignited a new level of competition in wireless and we're changing the industry for good! And we won't stop. When we amp up competition customers win, so we compete hard. That means we follow antitrust laws, compete fairly, and don't conspire with our competitors to rig prices, fix bids, divvy up sales territory, or boycott particular suppliers or customers. Because it's smart to avoid even the appearance of not following antitrust laws, we won't even TALK to our competitors about these things.

Antitrust Guidance

Meetings with Competitors Guidelines

Respect Others' Trade Secrets and Confidential Business Information

We have trade secrets; our competitors have trade secrets. Just like we wouldn't appreciate it if they tried to do something sneaky to learn what our next big move will be, we respect the fact that they too have confidential information. So we don't use illegal or unethical methods to gather confidential business information that belongs to other people or businesses. That includes any sensitive information—business plans, technical info, marketing strategies, and so on.

We also don't hire people to glean the business secrets of the company where they last worked. And if you DID work for one of our competitors, please keep confidential information about them to yourself.

Finally, if you somehow come across trade secrets or other confidential business information belonging to another person or business, don't take advantage of it. Immediately secure the information without using or sharing it and tell your manager. Your manager should contact your Legal partner or T-Mobile Compliance & Ethics right away for guidance.

Competitive Intelligence Policy

Deal in Good Faith

We achieve amazing results—the right way. We follow all laws and regulations that apply to our business, even those not specifically mentioned in this code. More than that, we're fair and honest in our business dealings. We don't try to gain unfair advantage over competitors, suppliers or customers by tricking anyone, taking advantage of confidential information, or fudging on the facts.

WE DO BUSINESS THE RIGHT WAY

Engage Ethical Suppliers

We look for suppliers who remind us of ourselves—ethical, hard-working, and customer-focused. And we want them to share our commitment to diversity, human rights, and business practices that are fair and considerate of their workers and the environment. Before selecting or retaining suppliers, we consider their business integrity and let them know about our ethical expectations.

In addition, we stand fully behind U.S. and international efforts to stop slavery and human trafficking. We have a zero-tolerance policy against trafficking and activities related to trafficking.

Anti-Corruption Policy

Follow Rules on Campaign Contributions, Lobbying and Gifts to Government Officials

T-Mobile wants to inform and guide government decisions that impact our business, customers, and employees, so we actively participate in the political process. We engage the right way—by following all campaign contribution and lobbying laws and the ethical standards that apply to dealing with public officials and government employees.

Don't use corporate money or other resources to support a political candidate or cause, except as permitted by law and specifically allowed in company policy. If you use your own resources to make a donation to a cause or candidate on T-Mobile's behalf, note that we can't reimburse you for that.

Keep in mind that only authorized employees of T-Mobile are allowed to lobby government officials and employees on behalf of T-Mobile.

Don't offer gifts, meals or anything else of value to government officials and employees without the approval of T-Mobile Compliance & Ethics.

Lastly, do your personal political work with your own resources and on your own time—not T-Mobile's.

Political Activities & Lobbying Policy

Travel, Expense and Corporate Card Policy

WE PROTECT T-MOBILE INFORMATION AND ASSETS

WE KEEP OUR COMPETITIVE ADVANTAGE AND PROTECT T-MOBILE BY USING COMPANY RESOURCES WISELY.

WE PROTECT T-MOBILE INFORMATION AND ASSETS

Safeguard T-Mobile Information

We're in a fiercely competitive industry. Our "secret sauce" to doing well is our ability to use our business information and technical know-how to introduce leading-edge products and services that our customers love.

We keep this valuable commercial information confidential. We don't disclose it to anyone outside the company unless we get advance approval from our manager. That goes for any confidential company information, trade secrets, inventions, details about our network—all that stuff. Releasing confidential information can hurt T-Mobile and lead to serious legal trouble. Sometimes we'll tell a vendor or partner some of this information, but only after they sign a non-disclosure agreement. Be careful with your co-workers too, and share certain information only if they really need to know.

If a government or law enforcement agency or an attorney asks for T-Mobile information, ask Legal Affairs for advice before you respond.

Acceptable Use Policy for Information and Communications Resources

Social Media Policy

Use Company Assets Responsibly

Let's all take care of T-Mobile. Use such things as company funds, property, vehicles, equipment, and office supplies first and foremost for company business. Try not to lose or waste them. And take common sense steps to protect them from theft.

During your daily work, use e-mail, web-browsing, social media and other digital resources provided by T-Mobile in a way that meets our business needs and our Acceptable Use Policy and Social Media Policy. When you use the company's digital resources, remember that we have no expectation of privacy. When necessary, T-Mobile can monitor and use any content that's shared or stored on them.

Acceptable Use Policy for Information and Communications Resources

Social Media Policy

ADDITIONAL RESOURCES

Sometimes the Code and the supporting policies don't have the answers to all your questions. Don't worry, we've got you covered! In almost all cases, you can start with our go-to resources.

- Your manager or next-level manager
- Human Resources business partner
- T-Mobile Compliance & Ethics
- Integrity Line: 1-866-577-0575 or www.T-MobileIntegrityLine.com (Remember, the Integrity Line can be anonymous)

If they can't answer your question or address your concern, contact the additional resources below.

- Antitrust or competition: Antitrust Compliance Officer
- Company information security: T-Mobile Privacy
- Customer information security: T-Mobile Privacy
- Government sales or contracts: Legal Affairs partner
- Political activities or lobbying: Government Affairs or Legal Compliance
- Requests for Customer Information: Law Enforcement Relations Group
- Requests for T-Mobile information: Legal Affairs
- Securities trading: Securities Compliance Officer
- Workplace safety: Safety@T-Mobile.com or 1-877-604-SAFE (7233)

Approved 6/15/2016
Tech. Rev 160708

T-Mobile is committed to protecting the privacy and sec rity of our customers' personal information and, as set forth in our Privacy Statement, we strive to be a leader in protecting all such personal information. In today's data-centric world, most consumers are familiar with the sensitivity and potential for misuse of information such as social security numbers, credit card numbers, and even demographic information.

As a telecommunications company, however, T-Mobile has access to a unique and highly-regulated form of personal information – known as **Customer Proprietary Network Information**, or "**CPNI.**" Despite its complex-sounding name, CPNI is simply the information generated in connection with the telecommunications services we provide to our customers. It includes, for example, call details (the phone numbers you call and the numbers calling you, the call times and dates, etc.) and certain information about customer rate plans and features. (CPNI does not include customers' names, addresses, or cell phone numbers – although we certainly treat that information with care under our general privacy and security promises.)

For most customers (as well as "authorized users" – which a customer may designate to access and manage the customer's account information), the most sensitive CPNI is the detailed records of whom they have called or from whom they have received calls. This "call detail" information may be of interest to people who know the customer or even to complete strangers.

EXHIBIT "D"

For example, a jealous boyfriend might be curious about who his girlfriend is talking to – and therefore might want to obtain the girlfriend's call details. Similarly, a person might wish to obtain call records related to a business competitor in order to know whether the competitor is nearing a deal with a specific supplier.

Although federal law has long-required telecommunications carriers to protect CPNI, in an Order released on April 2, 2007, the Federal Communications Commission ("FCC") issued revised and expanded CPNI rules in response to several high-profile incidents involving the activities of "data brokers" and "pretexters" who attempt to obtain unauthorized access to such information. These rules became effective December 8, 2007 and T-Mobile has implemented policies and safeguard procedures to help ensure compliance. T-Mobile continually reviews its compliance with such rules and annually certifies compliance to the FCC.

Highlights of FCC's rules and T-Mobile's policies

Carriers are prohibited from releasing call detail information to customers during customer-initiated telephone contacts, except when the customer has previously established a password for their account. Otherwise, carriers cannot release call detail information except by sending it to an address of record or by calling the customer at the telephone number of record.

- With the exception of T-Mobile Puerto Rico, T-Mobile does not disclose call details over the telephone in response to customer-initiated telephone contacts. (T-Mobile Puerto Rico may disclose call detail over the telephone in response to a customer-initiated telephone contact, but only after verifying the customer's account password and a one-time-use Personal Identification Number or "PIN" sent to the customer's handset via SMS text message during the call.) T-Mobile allows customers the option to establish account passwords for use in connection with calls to customer care, but first verifies the customer's (or authorized user's) identity through the use of a randomly-generated PIN delivered via SMS text message.

Carriers must provide mandatory password protection for online account access.

- T-Mobile provides online account access to CPNI only with a password that is initially established through use of a randomly-generated PIN delivered to the customer via SMS text message. For multi-line accounts, the customer may designate himself/herself as the primary account holder, which gives that person access to online account information for all the devices on the account. (This is the equivalent of the customer receiving the bill in the mail that contains the detailed usage information for all lines on the account.) Other users may access detailed online account information related

only to their respective device (for example, if a parent provides a device to their child, the child may access online information about that device – including CPNI). The primary account holder, however, may designate additional or more limited online access rights for other users.

Carriers may provide CPNI to customers in a retail location with a valid government issued photo ID.

- T-Mobile generally requires a valid government-issued photo ID matching the customer or authorized user's account information prior to disclosing CPNI during a visit to a retail store. T-Mobile utilizes a customer-established PIN for authentication of pre-paid accounts at retail locations.

Carriers must notify their customers when a password, address, and certain other account changes occur.

- T-Mobile's policy is to mail a notice to the customer's address of record or send an SMS message to the customer's number of record whenever, among other changes, a password, customer response to a back-up means of authentication for lost or forgotten password, online account, or address of record is created or changed. Any mailed notice is sent only to an address that has been associated with the customer's account for at least 30 days (except for accounts activated within the last 30 days, in which case the notice is sent to the address provided at

account activation). Any such notice does not include or reveal the changed information.

Carriers must establish a notification process for both law enforcement and customers in the event of a CPNI breach. Specifically, carriers must notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") after discovering a breach of CPNI.

- T-Mobile's policy is to notify law enforcement as soon as practicable, but in no event later than seven (7) business days, after a reasonable determination has been made that a breach of its customer's CPNI has occurred. Similarly, T-Mobile's policy is to notify customers of the breach no sooner than the eighth business day following completion of the notice to law enforcement unless directed by the U.S. Secret Service or the FBI not to so disclose or notify customers. T-Mobile may extend the period for customer notification pursuant to a written request of a relevant law enforcement agency.

T-Mobile is committed to the protection of its customers' CPNI and full compliance with the FCC's CPNI rules. Questions and/or concerns may be directed to privacy@t-mobile.com. A copy of the FCC's Final Order dated April 2, 2007, is available at:http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf.