

VERIZON IoT SERVICES EXHIBIT

(Exhibit VZW-1)

Carrier Specific Terms for Verizon Wireless IoT/M2M Connectivity Services

This Exhibit VZW-1 (this “Exhibit”) supplements and forms part of the SIMPL Wholesale Reseller Agreement (the “Reseller Agreement”) between SIMPL Wireless, LLC (“SIMPL”) and Customer, and applies only to Services that utilize the Verizon Wireless IoT and machine-to-machine (M2M) connectivity services (the “Verizon IoT Services”) provided by Cellco Partnership d/b/a Verizon Wireless (“Verizon”). This Exhibit is provided to Customer for presentation to and acceptance by Customer’s End Users.

This Exhibit provides Verizon IoT-specific “rules of the road” and does not replace or amend the Reseller Agreement. Capitalized terms not defined in this Exhibit have the meanings given in the Reseller Agreement.

By ordering, activating, accessing, or using Verizon IoT Services, Customer agrees to this Exhibit.

A. Verizon Policies and Acceptable Use

A.1 Carrier Policies: Customer will comply with all Verizon policies that apply to Verizon IoT Services, including Verizon’s acceptable use requirements, network management practices, and any plan- or program-specific restrictions communicated by SIMPL or Verizon (“Verizon Policies”). Verizon Policies may be updated from time to time; Customer is responsible for reviewing updates and ensuring ongoing compliance. SIMPL may, but has no obligation to, provide updates to Customer on the Verizon Policies applicable to Customer’s selection of Verizon IoT Services.

A.2 Enforcement: Customer acknowledges that Verizon may monitor for compliance and may restrict, suspend, or terminate Verizon IoT Services (in whole or in part) for suspected or actual violations of Verizon Policies, this Exhibit, or applicable law.

B. Permitted Use and Service Restrictions

B.1 Permitted Use: Verizon IoT Services are provided for use in Customer’s products, solutions, or service offerings. All devices must be Verizon-approved and used in accordance with this Exhibit.

B.2 Service Restrictions: Customer must not (a) resell, sublicense, or distribute the Services to other resellers or third parties for their own resale; or (b) use the Services in violation of the prohibited uses set forth in this Exhibit.

C. Prohibited and Restricted Uses

C.1 Voice and Messaging (Data-Only Plans): Verizon IoT Services are provisioned as data-only. Customer and End Users must not enable, provide, or use (or attempt any of the foregoing) Verizon-provisioned voice service or SMS/MMS messaging on IoT/M2M lines. Voice calls are limited to 611/911 only. Any attempt to use Verizon-provisioned voice on a data-only line may result in immediate suspension or termination.

C.2 Fraud, Abuse, and Unauthorized Use: Customer and End Users must not engage in fraud, abuse, excessive or anomalous automated usage, unauthorized access, account or device compromise, or any activity that facilitates theft of service. Customer will promptly notify SIMPL of suspected compromise, SIM theft, credential exposure, or other misuse. Customer shall be solely responsible for all risks, expenses, and liabilities arising from or relating to fraudulent usage by Customer, End Users, or any other person using the Verizon IoT Services.

C.3 Network Interference and Prohibited Equipment: Customer and End Users must not interfere with Verizon's network or other users' service, including by using repeaters, signal boosters, or other signal regeneration/amplification equipment unless Verizon has provided prior written approval and any required written agreement is in place.

C.4 Circumvention: Customer and End Users must not attempt to circumvent plan limitations, authentication, provisioning controls, traffic management, geographic restrictions, or other network protections.

C.5 No Critical/Life-Safety Reliance: Unless explicitly agreed in writing, Verizon IoT Services are not designed for, and must not be relied upon as, a sole means of support for emergency, life-safety, or other mission-critical applications where failure could result in death, serious bodily injury, or significant property damage. Customer acknowledges and agrees that plans which, in the event of network congestion, allow Verizon to lower stated maximum network speeds ("Traffic Management") or prioritize usage behind other customers ("Deprioritization") are not designed to be used with applications that have stringent requirements on availability, delay, or reliability ("Critical Applications"). Customer assumes all liability for any use of such plans for Critical Applications and shall indemnify SIMPL and Verizon from any claims arising from such use.

D. Device Eligibility and Network

D.1 Eligible Devices: Only Customer-provided, Verizon-approved 4G LTE CAT-1+, CAT-M1, and 5G Nationwide machine-to-machine devices may be activated on Verizon IoT Services. No other device types may be activated unless approved by Verizon in writing.

D.2 Network Coverage: Verizon IoT Services operate on the Verizon Wireless 5G Nationwide and 4G LTE network. For avoidance of doubt, the 5G Nationwide network is a separate network from the 5G Ultra Wideband network. IoT Services do not include coverage on the 5G Ultra Wideband network.

D.3 SIM/UICC Use in Authorized Equipment: SIMs/eSIM profiles (UICC) must be installed and used only within Verizon-approved equipment. Customer and End Users must not remove a SIM from authorized equipment and place it into other devices or otherwise misuse a SIM/UICC. Customer shall ensure that the UICC and/or SIM are used and physically located inside equipment which connects to the Verizon network.

E. Geographic Restrictions and Roaming

E.1 Activation: Equipment must be activated within Verizon's owned/operated U.S. network coverage areas.

E.2 US-Only Plans: Certain IoT plans are restricted to use within the United States only. Domestic and international roaming are not available on these plans. M2M Lines activated on such plans cannot be used outside the United States.

E.3 International-Capable Plans: Where a plan permits international usage, usage outside the United States will be billed at the applicable international travel feature rate or pay-as-you-go pricing. Equipment shall not be permanently located in a roaming area. Verizon reserves the right to terminate any Lines for Equipment that is permanently located in a roaming area.

E.4 Fixed-Location Equipment: Fixed-location IoT equipment must remain within Verizon's owned/operated U.S. network coverage areas unless the applicable plan explicitly permits otherwise.

F. Verizon IoT Billing Trigger

F.1 Initial Testing State Thresholds: For Verizon IoT Services under this Exhibit, the Initial Testing State (referred to by Verizon as the "Device Set-Up Feature") allows Customer to activate, test, configure, and warehouse/store devices until distribution. The feature automatically applies to new lines of service on eligible plans. When active, the monthly access fee (MRC) is suppressed until the earlier of the usage period threshold or the data threshold being exceeded, at which point MRC billing begins the following billing cycle. If Customer disconnects, suspends, upgrades a device, or changes the plan before the thresholds are met, the line will no longer qualify for MRC suppression. SIM-only activations are not eligible for this feature.

Initial Testing State Thresholds

Usage Period Threshold	One Hundred Fifty (150) Days
Data Threshold	60 KB

Note: Taxes, surcharges, and fees may apply during the Initial Testing State. Roaming may apply on a pay-as-you-go basis.

G. Minimum Security Requirements for Connected Devices

Customer will implement and maintain reasonable administrative, technical, and physical safeguards appropriate for connected devices and IoT deployments using Verizon IoT Services. At minimum, Customer will ensure the following baseline controls are implemented (as applicable to the device and deployment):

- change default usernames and passwords before deployment; use strong, unique credentials;
- disable unnecessary services, ports, protocols, and features; remove or disable unused accounts;
- keep device firmware, modem software, and security patches up to date;
- limit and harden remote management (disable if not needed; restrict by IP/VPN; use MFA where possible);
- use encryption for data in transit (e.g., TLS) and at rest where supported;

- segment IoT devices from general networks and apply least-privilege access controls;
- log and monitor access and security events appropriate to the deployment; investigate anomalies;
- protect physical access to devices and SIMs; maintain inventory and lifecycle controls;
- promptly remediate known vulnerabilities and rotate credentials if compromise is suspected;
- ensure third-party integrators and installers follow equivalent security practices.

H. Location-Based Services (Applies Only If Location Data Is Used)

H.1 Consent and Notice: If Customer uses Verizon IoT Services or any Verizon-provided interfaces to access, derive, or disclose location information associated with a device or End User (including for tracking, geofencing, or analytics), Customer must obtain affirmative opt-in consent from the relevant individual or authorized account holder before collecting, using, or disclosing location information. Customer must provide clear notice of what location data is collected, how it is used, with whom it is shared, and how consent may be revoked.

H.2 Use Limitations and Records: Location information may be used only for the disclosed purpose(s) and only to the extent permitted by applicable law and Verizon Policies. Customer must maintain comprehensive records of all consents obtained and notices provided under Section H.1 and promptly provide same to SIMPL or Verizon upon request. Notwithstanding any other provision, these records of consent and notice must be retained for a minimum period of five years from the date the consent was last active or the service was terminated.

I. Distributor Terms

I.1 Owned and Licensed Marks: Customer will ensure that its End Users (a) acknowledge that the Verizon-owned and/or licensed name(s), trademarks, and service marks (the “Verizon Marks”) are the sole property of Verizon and/or its parents or affiliates, and are good, valid, and enforceable in law and equity, (b) shall not challenge or assist in challenging the validity of registrations thereof, or engage in any activities or commit any acts, directly or indirectly, which may contest, dispute or otherwise impair the right, title, and interest of Verizon or its parents or affiliates therein, (c) neither have nor shall acquire, any right, title or interest in or to the Verizon Marks, and (d) shall not use any of the Verizon Marks, or any language from which the Verizon Marks may be inferred or implied, for any reason unless Verizon has expressly approved such usage in writing in advance. Any unauthorized direct or implied use of the Verizon Marks by distributors shall be a material breach of the Reseller Agreement and shall constitute an infringement of the Verizon Marks.

I.2 Distributor Security: Customer shall ensure that Customer’s distributors comply with the Verizon security requirements for any equipment that distributors connect to the Verizon network as outlined in Section G herein.

J. Remedies for Violations

J.1 Suspension/Termination: If Customer or any End User violates this Exhibit or Verizon Policies, Verizon or SIMPL may suspend, restrict, or terminate Verizon IoT Services

immediately (in whole or in part), in addition to any other rights and remedies under the Reseller Agreement. Verizon may also suspend, restrict, or terminate Verizon IoT Services if Verizon has a good-faith belief that termination is necessary to (a) prevent, mitigate, or eliminate fraud, (b) protect Verizon's personnel, network or property, or (c) comply with a law or regulation. Further, Verizon may deny any new line activations and/or suspend or terminate existing lines upon notice and opportunity to cure (if reasonable and practicable in Verizon's sole discretion), if (i) Customer fails to pay or dispute any charges when due, (ii) Customer uses the Verizon IoT Services or equipment in a manner prohibited by this Exhibit or the terms of the applicable plan, option, feature or application, (iii) Customer breaches the Reseller Agreement, (iv) Customer uses the Verizon IoT Services or lines for any illegal, improper or fraudulent purpose, (v) Customer uses, abuses or misuses Verizon's network in a manner that has an adverse impact on Verizon's network, operations, or customers, (vi) Customer or any user of Customer's equipment or any point of contact on its account provides false information relating to Customer's account, or (vii) Customer or any points of contact on Customer's account engages in fraudulent, threatening or harassing activities when using the Verizon IoT Services or interacting with Verizon representatives. Verizon may also temporarily limit Customer's Verizon IoT Services for any operational or governmental reason.

J.2 Cure: Customer must take immediate action to cure a default based on (a) violation of any FCC rule or regulation that could adversely affect any FCC spectrum license held by Verizon or any of its affiliates, (b) failure to certify or re-certify equipment as required by Verizon, or (c) Customer's failure to make payments when due.

J.3 Termination Consequences: Customer shall be responsible for notifying any impacted End Users and third parties of Verizon's termination of the Verizon IoT Services.

J.4 Continuing Charges; Transition: Suspension or termination may result in loss of connectivity and device functionality. Charges may continue to accrue as described in the Reseller Agreement and applicable Orders until deactivation is completed. Customer is responsible for implementing appropriate redundancy and transition planning.

K. Plan Amendments

Plan-specific pricing, data allowances, device eligibility requirements, and any additional plan-level restrictions applicable to Customer's use of Verizon IoT Services are set forth in one or more amendments to the Reseller Agreement executed between the Parties (each, a "**Plan Amendment**"). Each Plan Amendment is incorporated into the Reseller Agreement.