



## SPRINT BUSINESS MOBILITY FRAMEWORK SERVICES PRODUCT ANNEX

The following terms and conditions in this Sprint Business Mobility Framework Services Product Annex (“Annex”), together with the Sprint Master Services Agreement, Custom Service Agreement, Sprint Professional Developer Program Agreement, or Sprint Location Based Services Application Testing and Commercial Interface Agreement, as applicable, govern Sprint Spectrum L.P.’s provision of Sprint Business Mobility Framework (“SBMF”) Services to Customer.

1. **SBMF SERVICES.** Customer may only use SBMF Services in connection with a Sprint-certified Third Party Application (“TPA”). Customer may be a TPA provider that is also an end user of SBMF Services, or may be only an end user of SBMF Services that has a separate contractual relationship with a Sprint-certified TPA provider. Some SBMF Services may not work with all Products. SBMF may be used with one or more of the following services:

1.1 **Location Services.** Location services will only be supported for Wireless Devices (as defined in Section 2 below) shown on the official SBMF compatible device list. Some Wireless Devices may perform better than others. Location services are only available in Sprint coverage, not when roaming. Customer must obtain consent from the end users of the Wireless Devices for which Sprint will be providing location information to Customer.

A. **Precise Accuracy (“Precision Location”).** Precision Location queries must be ordered in conjunction with Cell Sector Location queries. The TPA must specify the Mobile Directory Number (“MDN”), requested accuracy in meters, and acceptable accuracy in meters. Requested accuracy must be 300 meters or less (or “High” for release 1 compatible interfaces). Acceptable accuracy must be at least 300 meters; the SBMF will reject requests with acceptable accuracy less than 300 meters. If the requested accuracy is less than 14,000 meters (“High” for release 1) then the request will be billed as a Precision Location transaction regardless of the received response accuracy.

Precision Location results vary greatly due to network conditions and the Wireless Device’s then-current environment. To get Precision Location, (A) the end user must be using a Wireless Device, (B) the Wireless Device must (i) be powered on, (ii) have a clear view of the sky, (iii) be enabled for GPS Location services, and (iv) be in a Sprint coverage area; and (C) the Sprint network must be available. Typical results show location within 150 meters, and such results are achieved for 50%-90% of Precision Location queries. When Precision Location is not attainable, SBMF will deliver the best location possible.

Other conditions will affect Precision Location results and may reduce the number of transactions that provide accuracy within 150 meters. Precision Location requests will fail when a Wireless Device is answering a call, placing a call, originating or terminating a data session, and during an EVDO data session. The ability to get a Precision Location fix on a Wireless Device in a data session is not as reliable as when the Wireless Device is idle or on a voice session. Environmental issues, such as weather, being inside or around buildings, and the position of the Wireless Device within vehicles can impact the ability to get Precision Location results. The ability to get a Precision Location fix on stationary Wireless Devices is greater than that on a Wireless Device that is moving.

B. **Cell Sector Accuracy (“Cell Sector Location”).** Cell Sector Location queries must be ordered in conjunction with Precision Location queries. The TPA must specify the MDN, requested accuracy in meters, and acceptable accuracy in meters. Requested accuracy must be 14,000 meters or greater (“Low” for phase 1 compatible interfaces). Acceptable accuracy must be greater than 300 meters; the SBMF will reject requests with acceptable accuracy less than 300 meters. If the requested accuracy is 14,000 meters or greater (“Low” for release 1) then the transaction will be billed as a Cell Sector Location transaction regardless of the received response accuracy. Cell Sector Location queries may fail if the device is in an EVDO data session.

C. **Notifications (“Location Notification”).** Customer may use the TPA with the Location Notification service in order to be notified when a Wireless Device has entered or exited an area. The area is



defined by a geo-fence consisting of a latitude/longitude point and a radius in meters. Location Notifications are based on Cell Sector Location accuracy rather than Precision Location accuracy. The TPA must specify the MDN, latitude/longitude, radius, and entry/exit parameters in the SBMF Services request. Sprint will provide a notification to the TPA upon detecting that the Wireless Device location matches Customer's request, or after 4 hours following the request if the Device does not enter or exit the applicable area, whichever comes first. Each Location Notification provides a snapshot of the Wireless Devices located within the applicable area at the time that Sprint gathers the information. Sprint may not provide Location Notifications for a particular Wireless Device if such device enters or exits and then exits or enters, as applicable, the same area within five minutes. The Location Notification service initiates 5 minute Cell Sector queries and therefore cannot return Precision Location.

- 1.2 **SMS (Mobile Terminated Text Messaging).** Customer may use the TPA to send SMS messages to any Sprint PCS Vision capable Product. The TPA must specify the MDN or an array of up to 20 MDNs or a group name as defined in the SBMF (as defined in Section 3 below) and the text message to send to the MDN(s). Sprint will attempt to deliver the message, but does not guarantee delivery. Customer may not use SMS in a manner that could result in the receipt of spam by other individuals.
  - 1.3 **Presence (User Status).** Customer may use the TPA with the Presence (User Status) service to determine if a Wireless Device located within the Sprint Nationwide PCS Network is powered on or off. Sprint does not guarantee the accuracy of the Presence (User Status) results for Wireless Devices that are roaming or otherwise off the Sprint Nationwide PCS Network.
  - 1.4 **Presence Notifications.** Customer may use the TPA with the Presence Notification service in order to be notified whenever a Sprint PCS Vision device has been powered on or off while within the Sprint Nationwide PCS Network. The TPA must specify the MDN and whether to be notified that the Wireless Device was powered on or off in the SBMF Service request. Sprint will provide a notification to the TPA upon detecting that the Wireless Device status matches Customer's request or after 4 hours if the Wireless Device did not change status as specified in the Customer's request, whichever comes first. Each notification provides a snapshot of the Wireless Device status at the time that Sprint gathers the information. Sprint may not provide notifications for a particular Wireless Device if such device is powered on or off and then is powered off or on, as applicable, within five minutes or if the device is not within the Sprint Nationwide PCS Network coverage area.
  - 1.5 **Voice Browsing.** Customer may use the TPA with the Voice Browsing service to initiate a Voice Browsing session with a telephone. The TPA must specify the telephone number and a URL where the SBMF can retrieve a voiceXML ("vXML") script. Customer must also provide a TPA Virtual Telephone Number ("TVTN") to be used as the caller ID of the SBMF-initiated voice call. When called, the TVTN must provide information about the TPA's use of the Voice Browsing service. Use of the SBMF with the Voice Browsing service is limited to use in the United States, Puerto Rico, and Canada. Use of transfer tags in vXML scripts is prohibited.
  - 1.6 **User Invitations.** User Invitations service is initiated by Customer or a TPA provider via the SBMF portal. User Invitations occur when an SBMF customer invites a Sprint PCS Vision device user to join the TPA's service. Customer may not use User Invitations service in a manner that could result in the receipt of spam by other individuals.
2. **DEVICE COMPATIBILITY.** Customer may only use devices that have been approved by Sprint to be used in connection with SBMF Services (the "Wireless Devices"), and will only allow individual liable users to participate in Customer's use of SBMF Services after Customer has confirmed that such individual liable users will use approved Wireless Devices. Sprint has implemented a mechanism to restrict the ability to send User Invitations to devices that are not compatible with SBMF Services.

The following Sprint devices are approved to be used in connection with SBMF Services:

RIM Blackberry 7250, RIM Blackberry 7130e, Sanyo VI-2300, Sanyo MM-8300, Sanyo RL-4930, Sanyo MM-9000, Sanyo MM-7500, Sanyo SCP-200, Sanyo SCP-3100, Sanyo SCP-2400, Sanyo "Katana" (SCP-6600), Sanyo 8400,



Sprint PPC-6600, Sprint PPC-6601, Sprint PPC-6700, Motorola c290, LG LX350, LG Fusic (LX 550), Samsung A580, Samsung A640, Samsung MM-A940, Samsung MM-A900, Samsung MM-A920, PalmOne Treo 650, PalmOne Treo 700p, Nokia 6165i, and Sendum VT-100.

Sprint may update the list of Wireless Devices that are compatible with SBMF Services by notifying Customer or by posting an updated version of this Annex.

**3. USE OF THE SPRINT BUSINESS MOBILITY FRAMEWORK MANAGER.** Sprint will provide Customer with an account for Customer's use of the Sprint Business Mobility Framework Manager ("SBMF") portal. Customer must designate an individual or individuals who will be "Domain Administrators" and who will have administrative authority over TPAs and/or Wireless Devices within the designated Domain. A "Domain" is defined by billing system account numbers and consists of all Wireless Devices and TPAs on Customer's specified account(s). The Domain Administrator will determine which billing account numbers should make up the Domain. Sprint will send SBMF access credentials via email to the Domain Administrator(s). Any additional administrators or managers created by a Domain Administrator will be the responsibility of the Domain Administrator, who will determine the privacy type for each TPA on the Domain. The privacy type for the application will determine which Wireless Device managers/end users can view the TPA from the SBMF portal and request Wireless Devices to be associated to the TPA. Privacy designations are defined as follows:

**3.1 Private.** Only Wireless Device managers assigned to the Domain can view the TPA and request Wireless Devices to be associated with the TPA.

**3.2 Corporate.** Only Wireless Device managers on Domains within the same corporate root account can view the TPA and request Wireless Devices to be associated with the TPA.

**3.3 Public.** Any Wireless Device manager/end user (including individual liable users) can view the TPA and request to be associated with the TPA.

Customer's use of the SBMF in conjunction with corporate-liable Wireless Devices that are not on the same Domain as the TPA will require Customer to have an SBMF account to provide permission for the TPA to target the corporate-liable devices.

**4. PRIVATE INFORMATION MANAGEMENT.** All information collected or developed by Sprint regarding the end users of Wireless Devices that use SBMF Services or derived from the TPA's interrelation with SBMF Services – including, but not limited to, the Mobile Identification Number or MDN issued by Sprint to an end user, the Electronic Serial Number associated with a Wireless Device, the Network Access Identifier, Location Information, Presence Information, and any customer information described in the FCC definition of "Customer Proprietary Network Information" as set forth in 47 USC 222(h)(1) ("Sprint Data") – is exclusively owned by Sprint. Nothing in this Agreement confers in Customer any right of ownership in the foregoing Sprint Data, except as the owner of the Wireless Device to which such Sprint Data relates. All Sprint Data is Confidential Information. Customer will not, except as otherwise stated in the Agreement or as the owner of the Wireless Device to which applicable Sprint Data relates, store, copy, analyze, monitor, or otherwise use any Sprint Data. The TPA provider will be responsible for the management and distribution of customer proprietary network information ("CPNI") such as location and presence. Sprint will not be responsible for the distribution of CPNI to additional parties, such as the end users of the TPA. The TPA provider must have consent from the Wireless Device owner in order to distribute CPNI to additional parties.

**5. END USER SUPPORT.** If Customer is not the end user of the SBMF Service, then Customer must be responsible for all TPA end user application support and must make all end users aware that application support should be received from the TPA administrator (not Sprint). This includes end users of Sprint Wireless Devices. The end user of the SBMF Service must contact the TPA provider for support issues related to the TPA.

**6. DIGITAL CERTIFICATES.** If Customer pays a per transaction fee for SBMF Services, Sprint will provide a digital certificate for the TPA to use with the SBMF Service. Customer may only use this certificate in connection with its use of SBMF Services under the Agreement. Sprint will use the certificate in connection with its billing for SBMF Services, and the certificate assigned to the TPA may only be used for that TPA. Customer must secure its digital certificates in a manner that may reasonably be expected to avoid fraudulent use or theft. Customer may not



duplicate its certificate or use its certificate on multiple machines without Sprint's written permission. This provision is not applicable if Customer pays an MRC per Wireless Device for SBMF Services.

7. **SUSTAINED MAXIMUM TRANSACTION RATE.** The SBMF will enforce a sustained maximum transaction rate for the TPA. Sprint will determine Customer's transaction rate and such rate will be based on the number of Wireless Devices in use with the TPA. To determine Customer's transaction rate, Sprint will average Customer's usage over a 60 second window as determined by Sprint. If Customer pays a per transaction fee for SBMF Services, the setting will be 20% of the number of Wireless Devices to be used with SBMF per 60 seconds. This allows each Wireless Device to be queried up to a maximum of 12 times per hour. If Customer pays an MRC per Wireless Device for SBMF Services, the setting will be 10% of the number of Wireless Devices. This allows each Wireless Device to be queried a maximum of 6 times per hour. Sprint will deny any request for SBMF Service above Customer's transaction rate threshold. The TPA shall make a reasonable attempt to evenly distribute requests throughout the 5 or 10 minutes, whichever is applicable. The maximum transaction rate is the same for each service type (location, SMS, etc.), but is calculated individually for each service type. The transaction rate will automatically increase as additional Wireless Devices opt-in for SBMF Services. Customer may not intentionally exceed its sustained maximum transaction rate. Sprint may suspend or terminate Customer's use of SBMF Service if Customer makes excessive attempts to exceed the sustained maximum transaction rate. Sprint will calculate Customer's transaction rate based on when the SBMF gateway receives the transaction request. The difference in transmission delay (i.e., "jitter") associated with Internet traffic is beyond Sprint's control and therefore the rate at which requests are sent may not be exactly the same as when requests are received.
8. **PROVISIONING.** Customer must provide all necessary information required by Sprint to provide SBMF Service, as set forth on a SBMF TPA Production Form. Customer may update the parameters of the SBMF Service once per month on the date of the month determined by Sprint. Such parameters are set forth on the SBMF TPA Production Form, and include without limitation: the number of Wireless Devices used with the SBMF application; Distinguished Name of the TPA as defined in the Digital Certificate; and Source IP address of the TPA (used in Sprint firewall configuration).
9. **MODIFICATIONS TO THE SBMF SERVICES.** Sprint makes no representation or warranty that future modifications to the SBMF Services or Sprint's wireless network will be backwards compatible with any TPA. At Sprint's sole discretion, Sprint may make commercially reasonable efforts to support backwards compatibility of SBMF Services for one prior release. If the TPA does not maintain compatibility with the SBMF Services, then Sprint may deactivate SBMF Service.
10. **GROUP SIZE.** Group size for groups used in an SBMF web service request may not exceed 20 Wireless Devices. The SBMF web services gateway will not accept transactions for groups larger than 20.
11. **SPAM CONSIDERATIONS.** Customer may not use SBMF Services in a manner that could result in the receipt of spam by other individuals.
12. **HOSTED APPLICATIONS.**
  - 12.1 If Customer intends to have its SBMF application hosted by another party and Customer will pay per transaction fees then Customer must provide the digital certificate information to the hosting party at Customer's own risk. Sprint is not responsible for any liability associated with Customer's provision of the digital certificate information to another party.
  - 12.2 Customer will be given an SBMF Manager account to manage permissions associated with SBMF Services. Customer may create a manager profile for the hosting party in order to delegate SBMF Manager activities to the hosting party. Sprint is not responsible for any liability associated with providing a manager profile to another party.
  - 12.3 Customer must specify to Sprint the party that is hosting the application on Customer's behalf, and must provide the hosting party's company name, address, contact name, contact phone, and contact email at the time of implementation of SBMF Services.



- 13. ADDITIONAL USAGE GUIDELINES.** This Section 13 is applicable if Customer pays an MRC per device for SBMF Services. The TPA provider, (either Customer or a third party, as applicable) will abide by these guidelines with respect to the TPA.
- 13.1** Location: Customer may not locate a Wireless Device more frequently than once every 10 minutes. The total queries should be evenly distributed over the 10 minutes. Customer may locate 10% of its Wireless Devices within a one minute period, thereby locating all of its Wireless Devices within a 10 minute period. Additional details are given in Section 7 ("Sustained Maximum Transaction Rate") of this Annex.
- 13.2** Presence: Customer must use the presence service after a location error is received. If the result shows "on," then the location service may be re-tried. If the presence returns "off," then a presence notification request should be made. When the presence notification is returned as "on," then location queries may again be attempted.
- 13.3** SMS: Customer may send SMS only to other Wireless Devices that are billed an MRC for SBMF Services. If Customer intends to send SMS to other Sprint PCS phones, the TPA must be set up so that Customer pays a per transaction fee for SBMF Services.
- 13.4** Voice Browsing: Customer may initiate a voice browsing session only with those Wireless Devices that are billed an MRC for SBMF Services. If Customer intends to initiate a voice browsing session with other Sprint PCS phones or landline phones, the TPA must be set up so that Customer pays a per transaction fee for SBMF Services.
- 13.5** Maximum usage per SBMF Service: Customer is expected to stay within the following usage guidelines:
- A. High precision location (and/or low precision location): 1 query every 10 minutes per Wireless Device.
  - B. SMS: 200 per month per Wireless Device.
  - C. Presence: 50 per month per Wireless Device.
  - D. Presence Notifications: 50 per month per Wireless Device.
  - E. Location Notifications: 25 per month per Wireless Device.
  - F. Voice Alerts: 200 per month per Wireless Device.