CODE OF CONDUCT FOR THE AT&T SHORT CODE AND 10-DIGIT A2P SMS MESSAGES

AT&T CODE OF CONDUCT

Code of Conduct

for the

AT&T Short Code and 10-Digit A2P SMS Messages

06/01/2020

Foreward

This Code of Conduct governs the existing Short Code Application-to-Person (A2P) messaging system and the AT&T 10-digit long code (10DLC) A2P Messages. The 10DLC A2P Messages allows A2P SMS traffic originating from 10DLCs outside of AT&T's network to be delivered to AT&T mobile customers.

This code of conduct is subject to change at AT&T's discretion.

Objectives of the AT&T 10DLC A2P SMS Messages

This Code of Conduct:

Produces meaningful and clearly-defined conduct and messaging **policies** to supplement existing compliance-related **guidelines** to:

- Provide additional clarity and a more granular understanding of enforceable behavior,
- Strive for consistency with the industry published best practices,
- Support transparency and communication with Messaging Partners, and
- Encourage AT&T and Messaging Partners to adhere to laws, regulations and industry guidelines (e.g., TCPA; CTIA Industry Best Practices).

Note that this document only provides a set of conduct and acceptable use requirements. It does not address and should not be interpreted as addressing the permissibility of

messaging under applicable laws and regulations; Messaging Partners are encouraged to consult their own legal counsel.

Definitions and Parties

A2P Message – Any SMS message to or from a mobile subscriber account for which the content is generated in whole or in part by an automated process or for which a single manual send command results in multiple messages being sent. A group message where all recipients of a small social group receive the same message and the content is personal and non-commercial is excluded from the definition of an A2P Message.

Service Provider – A party that offers end users and/or Message Senders a messaging service connected to mobile messaging, including but not limited to mobile-phone-based SMS/MMS/RCS messaging and their messaging APIs.

Mobile Network Operator – A special type of Service Provider that holds a license to use RF specturm for mobile messaging.

Inter-Carrier Vendor (ICV) – A party that provides network connectivity to, from, and/or between Mobile Network Operators, Aggregators and messaging Service Providers.

Aggregator – A party that offers Service Providers and/or other Aggregators a messaging service connected to mobile messaging, including but not limited to mobile phone based SMS/MMS/RCS messaging and messaging APIs; and is sending or receiving messages via a direct connection to either a Service Provider, Mobile Network Operator or Inter-Carrier Vendor.

Message Sender – means a high profile individual (Influencer) and/or a third-party who uses Service Provider's and/or other Aggregator's services for the purpose of enabling such Influencer and/or third-party to provide content to, or communicate with AT&T mobile customers through A2P Messages or 10DLC A2P Messages.

Messaging Partner – An Inter-Carrier Vendor, Aggregator or Service Provider with a direct or indirect contractual relationship with AT&T.

Note that a single party may be any combination of an ICV, Service Provider, and/or Message Sender in the context of a particular messaging stream. Figure 1 below illustrates many of the possible interconnections.

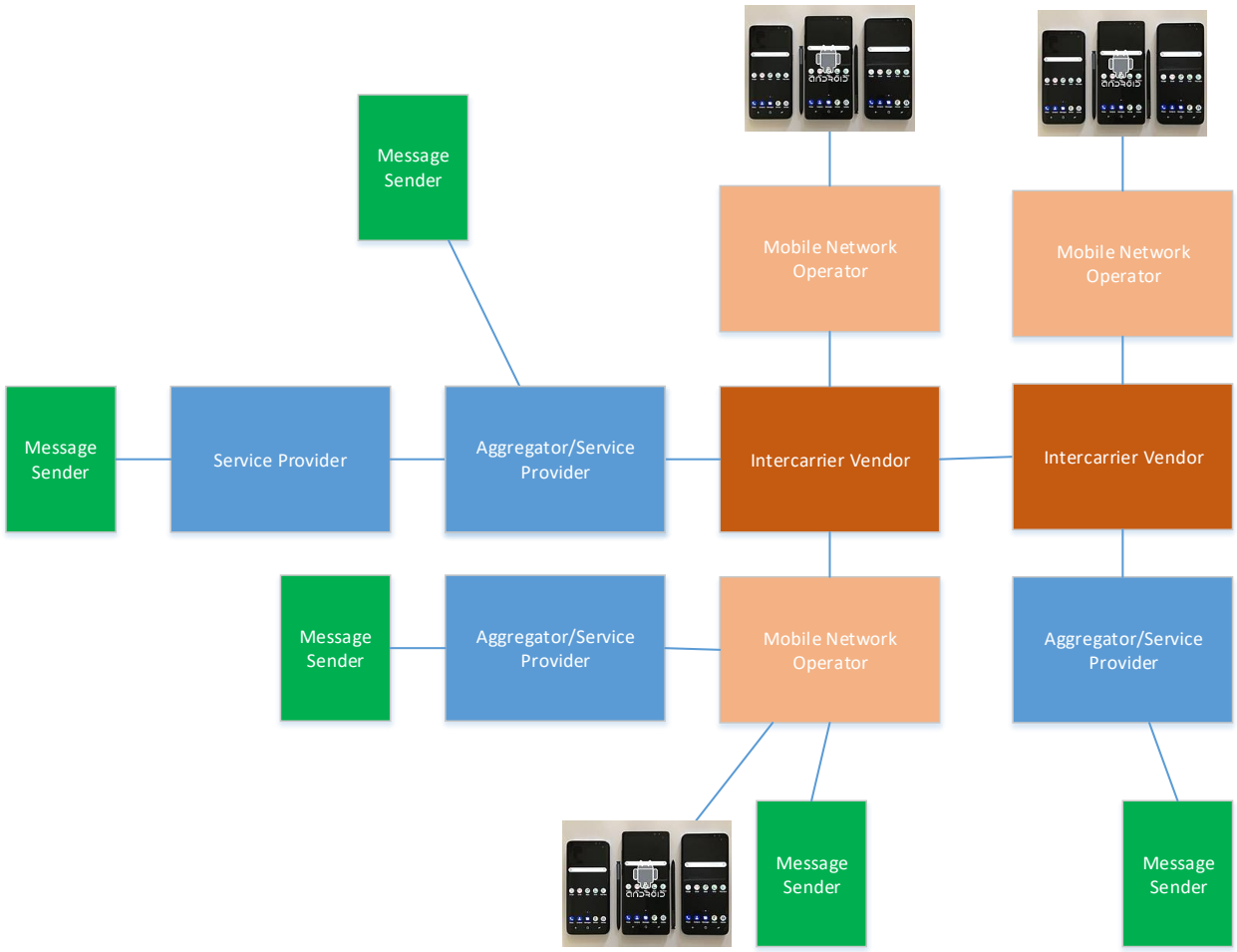

Figure 1. Connectivity Illustration

Enforcement – During Trial and Post Commercial Launch

Failure to comply with this Code of Conduct may, at AT&T's sole discretion, result in any of the following without prior notice:

- Downgrade in message service classes
- Suspension of specific messaging campaign, number, or Message Sender and/or Service Provider
- Termination of specific messaging campaign, number or Message Sender

Chronic non-compliance may result in suspension or termination of the Messaging Partner's messaging privileges.

Policies

Content Provider Vetting and Message Class

- Message Senders (or other Messaging Partners on their behalf) must apply for AT&T authority to use one or more Message Classes (defined below) across one or more specified phone numbers.

- AT&T assigns and authorizes the Message Sender to use one or more message classes, initially based on vetting of the applicant and provided information (Message Classes(es)).

- Unidentified or unknown Message Senders may be authorized to use a class of service having anti-spam policies similar to those of 10DLC P2P (e.g., with only low message rates permitted).

Message Classes and policies may be adjusted by AT&T with notice to the Aggregator and/or, if identified, the Service Provider and Message Sender, based on observed messaging campaign characteristics, such as Subscriber complaints and unsubscribe requests. Message Senders and Aggregators may also request changes to message class authorizations.

Class-Based Messaging

- Unless explicitly authorized in writing by AT&T, A2P Messages shall not exceed AT&T's maximum P2P message sending rate, which is currently 15 SMS messages or segments thereof, per sending number per minute. [Note: AT&T may in the future require all A2P messaging to be authorized.]

- For cases explicitly authorized by AT&T, 10DLC A2P Messages SHALL contain Message Class tags that conform to AT&T's "Messaging Tagging Requirements and Specifications, Version 1.2" on ingress to AT&T's network. Note that class tags may be supplied by the Message Sender, or by a Service Provider and/or Aggregator as a service to the Message Sender. Only authorized Message Class tags appropriate for the type of message SHALL be used.

- Each Message Class has a default AT&T anti-spam policy assigned to it. This policy includes a maximum authorized per-line message rate (typically far above current P2P message rates), and policies for traffic pattern and content-based message blocking.

- AT&T anti-spam policies are applied to a particular message based on the default policy for its Message Class and a risk assessment (aka reputation) of the particular Message Sender and to a more limited extent, the reputations of the Service Provider and/or Aggregator. AT&T may change its anti-spam policies as needed to mitigate abusive traffic. Such changes may be made by AT&T without notice.

Consumer Consent

The Message Sender must obtain proper consumer consent for each message sent. The type of consent that is required depends on the type of message content sent to the consumer. The table below includes the types of messaging content and the associated consent that is required by AT&T. Other legal obligations and requirements may apply, and by providing the table below, AT&T does

not purport to state that messages sent that comply with consent requirements outlined below are consistent with applicable law. For each message sent to a consumer, it is the obligation of the Message Sender to determine and comply with the legal obligations and requirements that apply to the message.

Consumers can revoke consent at any time and in any way. Consumer opt-out requests must be honored, whether they are made by phone call, email, or text of the word "Stop" (case insensitive), unless legal authority or obligation to provide the message dictates otherwise.

The consumer must give the appropriate consent for the given message type.

Where consent is required, the proposed entities authorized to send must be conspicuously communicated prior to obtaining consent, and Consumer's consent must explicitly name the entities authorized to send. Such consent may not be obtained using deceptive methods.

Consumer consent may not be bought, sold, rented, or shared.

Types of Messaging Content & Required Consent		
Consumer-Initiated Conversational	**Informational**	**Promotional**
Conversational messaging is a back-and-forth conversation that takes place via text. If a Consumer texts a business first and the business responds quickly with a single message, then it is likely conversational. If the Consumer initiates the conversation and the business simply responds, then no additional permission is expected	Informational messaging is when a Consumer gives their phone number to a business and agrees to be contacted in the future for a non-promotional purpose. Appointment reminders, welcome texts, and other non-promotional alerts fall into this category because the first text sent by the business fulfills the Consumer's request. A Consumer needs to agree to receive texts for a specific informational purpose when they give the business their mobile number.	Promotional messaging is a message sent that contains a sales or marketing promotion. Adding a call-to-action (e.g., a coupon code to an informational text) may place the message in the promotional category. Before a business sends promotional messages, the Consumer should agree in writing to receive promotional texts. Businesses that already ask Consumers to sign forms or submit contact information can add a field to capture the Consumer's consent.
First message is always sent by the consumer	First message is sent by the consumer or business	First message is sent by the business

Two-way conversation Message responds to a specific request	One-way or two-way conversation Message contains information	One-way alert Message promotes a brand, product, or service Prompts Consumer to buy something, go somewhere, or otherwise take action
IMPLIED CONSENT If the Consumer initiates the text message exchange and the business only responds to each Consumer with relevant information, then no verbal or written permission is expected.	EXPRESS CONSENT Unless an exemption applies, the Consumer should give express permission before a business sends them a text message. Consumers may give permission over text, on a form, on a website, or verbally. Consumers may also give written permission.	EXPRESS WRITTEN CONSENT The Consumer should give express written permission before a business sends them a text message. Consumers may sign a form, check a box online, or otherwise provide consent to receive promotional text messages.

Opt-out

Consent must be revocable without penalty to message recipient beyond the termination of any ongoing benefit that the message recipient would receive without the revocation.

Unless otherwise permitted or required by law, application-originated Informational and Promotional messaging must contain a notice that a consumer may opt-out of future communications by replying with the word “stop” in any combination of lower and upper case.

AT&T deactivation files must be processed daily and those CTN’s removed from the messaging provider / Message Sender’s data base for future messaging.

A “high” volume or percentage of opt-out messages may result in suspension or termination of a specific messaging campaign and/or blocking of sending numbers.

Consumer opt-in and opt-out must work correctly

Opt-in lists, systems and processes may only contain or add Consumers who have properly opted in. Unless otherwise permitted or required by law, all Opt-out requests must be promptly honored.

Opt-out notices must explicitly notify recipients that the word “Stop” may be used for opt-outs.

Consumer-originated messages indicating a desire to opt-out through the use of the “stop” keyword must result in a cessation of the indicated messaging.

Providing help such as in response to the word “help” is encouraged.

Prohibited Campaign Types

SMS A2P SMS Messaging may not be used for affiliate lead and/or commission generation. AT&T may block and/or terminate messaging campaigns and/or accounts which AT&T, at its sole discretion, determines to be affiliate-related. Additionally, the types of campaigns listed below are prohibited Effective immediately , no new campaigns of the nature below will be approved for provisioning. Existing campaigns of this nature on dedicated Short codes will be terminated in Early Q1 2019 with the exact date to be determined and communicated.

Any exceptions require written AT&T approval.

- Loan advertisements with the exception of messages from direct lenders for secured loans
- Credit repair
- Debt relief
- Work from home, ‘secret shopper,’ and similar advertising campaigns
- Lead generation campaigns that indicate the sharing of collected information with third parties
- Campaign types not in compliance with the recommendations of or prohibited by the CTIA Short Code Monitoring Handbook, Version 1.7 or later.

If a Message Sender is observed sending any of the above-listed disallowed content, then an account review may be performed by AT&T or its agents. This review can result in the suspension of sending rights for a provisioned phone number or short codes; restriction of high-throughput access; suspension of provisioning rights for new phone numbers or short codes; and/or suspension of all network services.

Service Providers, Aggregators and Inter-carrier Vendors are expected to enforce restrictions on their own networks to prevent these types of content at the intake source.

Abusive Messaging Prohibited

Message content that deceives or threatens consumers is not permitted.

Message streams that result in excessive complaints or STOP commands typically indicate an unwanted message campaign and will not be allowed to continue.

If a Message Sender is observed sending any of the content listed below, then an account review may be performed by AT&T or its agents. Based on this review, there may be a restriction, suspension or termination of sending rights, including changes of authorized Message Classes, throughput, termination of the messaging campaign; and/or termination of all messaging campaigns operated by a party suspected of negligence or complicity, including the Message Sender, Service Provider or Aggregator.

AT&T Messaging Partners are expected to place and enforce restrictions on their own networks to prevent these types of content:

- Phishing
- Fraud or scams
- Deceptive marketing
- Distribution or malware or app downloads from non-secure locations
- Loan, debt consolidation, debt relief and student loan programs from any enterprise that is not able to grant loans itself; affiliate lead generation for these financial programs is prohibited
- Affiliate marketing programs that seek to obtain opt-in subscriber lists

Prohibited Messaging Techniques

Snowshoe Sending Prohibited

Snowshoe sending is a technique used to send messages from more source phone numbers than are needed to support an application's function. This technique is often used to evade per-sender rate limits and other spam filters.

Messaging use cases that require the use of multiple numbers to distribute "similar" or "like" content must be declared in the campaign submission as requiring number pools for appropriate class designation.

Filter Evasion Assistance Prohibited

Sending mechanisms designed to evade spam controls are prohibited. Service Providers are expected to work with AT&T to resolve spam and unwarranted blocking issues. The practice of automatically providing a sender with new phone numbers to replace phone numbers blocked by a receiving network is specifically prohibited.

Dynamic Routing Prohibited

Each 10DLC or short code must have a single route (i.e., ordered sequence of Service Providers, Aggregators and Inter-Carrier Vendors) in the delivery path to a given destination phone number. Routing is expected to change infrequently, typically as a result of changing contractual relationships, rather than dynamically. The delivery path must include the assigned Service Provider as the originating service provider. This does NOT prohibit re-routing traffic as needed to maintain service in the event of major network outages, but MUST not be performed to circumvent accidental or intentional spam blocking.

Shared Codes Prohibited

Shared 10DLC or short codes are prohibited. There may be specific enterprise based use cases where exceptions may be granted.

Effective immediately no new shared short codes should be onboarded. All existing shared short codes will be terminated banned at a future date to be determined and consistent with the commercial availability of 10DLC A2P Messaging. This will formally be communicated with appropriate advance notice.

The use of a single 10DLC or short code to be "sub–aggregated" in a manner that allows multiple parties control of content and/or receiving phone numbers is prohibited. Exceptions may be considered when appropriately requested via campaign submission as requiring third-party content control. If approved, such campaigns will be assigned an appropriate Message Class designation to help prevent blocking of wanted messages (interactive messaging, Bots, RCS).

URL cycling / Public URL shorteners

The practice of using multiple FQDNs (i.e., host.domain) in bulk messaging with similar message content (e.g., for the specific purpose of evading filters and/or diluting reputation metrics) by a single party is prohibited. Exceptions may be considered when appropriately requested. If approved, they will be assigned an appropriate Message Class designation to help prevent blocking of wanted messages (interactive messaging, Bots, RCS).

The practice of using public URL shorteners in bulk messaging is highly discouraged, and messages containing them may be subject to blocking. The practice of using multiple public URL shorteners (i.e., host.domain/path) in bulk messaging with similar message content (e.g., for the specific purpose of evading filters and/or diluting reputation metrics) is prohibited.

References to Anonymous and Opaque Web Sites and Phone Numbers Prohibited in Bulk Messaging

Bulk messages must not contain URLs of or that redirect to websites that do not unambiguously identify the website owner (i.e., a person or legally registered business entity) and include contact

information including a postal mailing address. Landing websites that collect personal information must have a published, conspicuously-accessible privacy policy.

Similarly, bulk messages must not contain phone numbers that are assigned to or forward to unpublished phone numbers unless the owner (i.e., a person or legally registered business entity) of such phone numbers is unambiguously indicated in the text message.

Deactivation Files

Aggregators and Service Providers assume responsibility for managing information about deactivated and recycled mobile phone numbers. They must either enforce deactivations themselves or ensure that deactivation information is made available to Message Senders with a requirement for the Message Sender to manage opt-out of deactivated numbers.