Inteliquent Messaging Policies and Best Practice Guidelines

Contents

1.0 Introduction

The Inteliquent messaging solution supports high-quality, high-integrity communications. Spam or unwanted messaging is forbidden. To protect consumers and the ecosystem from abuse, Inteliquent enforces guidelines designed to promote best practices for exchange of messages.

The viability of the messaging ecosystem is dependent on Consumer perception of messaging as a trusted and convenient communication environment. These Policies and Best Practices are intended to preserve the credibility and utility of the ecosystem.

The objective of these policies is to enable wanted messages and prevent unwanted or deceptive messages. While these Policies and Best Practices are intended to encourage correct behaviors, the spirit behind them is equally important. Message senders acting in bad faith to thwart or undermine the spirit of these policies should expect to experience penalties.

2.0 Enforcement

Policy enforcement is performed at several points during message delivery.

1. Inteliquent Policy Management systems
2. Aggregator Policy Management systems (e.g., Sybase, Syniverse, Zipwhip)
3. Carrier Policy Management systems (e.g., T-Mobile, Verizon Wireless, Sprint, AT&T Wireless)

3.0 Violations

Violations of guidelines may result in on or more of the following resolutions taken by Inteliquent, aggregator's or carrier's:

1. Blocking of individual messages
2. Blocking of Telephone Numbers
3. Repeated violation may result in termination of all network services.

4. Definitions

Non-Consumer Application to Person (A2P): *A Non-Consumer is a business, organization, or entity that uses messaging to communicate with Consumers. Examples may include, but are not limited to, large-to-small businesses, financial institutions, schools, medical practices, customer service entities, non-profit organizations, and political campaigns.* Messages sent from an application, typically web based, to a mobile subscriber. Some common use cases include two factor authentication (2FA), travel notifications, banking alerts, or marketing messages. A2P delivery methods are either via 8xx (Toll Free) messaging service or soon to be implemented 10DLC (10 digit long code).

Consumer Person to Person (P2P): A Consumer is an individual person who subscribes to specific wireless messaging services or messaging applications. *Consumers do not include agents of businesses, organizations, or entities that send messages to Consumers*. *Consumer (P2P) messaging is sent by a Consumer to one or more Consumers and is consistent with typical Consumer operation (i.e., message exchanges are consistent with conversational messaging among Consumers).* Consumers are natural persons with uniquely assigned telephone numbers (long codes i.e. local telephone numbers) that can be dialed. Some Consumers utilize automation to assist in responding to communications. For example, a Consumer may direct their messaging service to auto-reply to a phone call in order to inform the caller about the Consumer's status (e.g., "I'm **busy**" or "Driving now, can't talk"). Such use of automation to assist Consumers in their composition and sending of messages falls within the attributes of typical Consumer operation. In contrast, automation in whole or in part used by Non-Consumers to facilitate messaging is not typical Consumer operation.

Short Message Service (SMS): Commonly known as "text messaging," this is a service for sending and receiving messages of up to 160 characters to mobile devices. Longer messages will be fragmented into smaller message fragments. Maximum character length per message fragment varies depending on the character set used in the body of the message, whether GSM default alphabet or Unicode.

Multimedia Message Service (MMS): Facilitates group messaging and allows for the exchange of multimedia content between mobile devices including, video, pictures and audio.

Short Message Peer-to-Peer (SMPP): SMPP is an open, industry standard Internet protocol designed to provide a flexible data communication interface for the transfer of SMS messages between External Short Messaging Entities (ESME), Routing Entities (RE) and Short Message Service Centers (SMSC).

MM4: MM4 is a 3GPP protocol for MMS service that covers the routing of an MMS from an originator MMS Relay/Server to a recipient MMS Relay/Server. MM4 is based on SMTP (email) protocol. MM4 is an extension of Internet Simple Mail Transport Protocol (SMTP) according to STD 10 (RFC 2821).

REST API: Application Programing Interface used to establish Messaging connectivity for sending and receiving messages and other service related access.

Unwanted Messages: May include, but are not limited to, unsolicited bulk commercial messages (i.e., Spam); "phishing" messages intended to access private or confidential information through deception; other forms of abusive, harmful, malicious, unlawful, or otherwise inappropriate messages; and messages that require an opt-in but did not obtain such opt-in (or such opt-in was revoked).

Fingerprinting: The process of extracting data points from identified SPAM content is known as "fingerprinting". Once message content has been fingerprinted as SPAM, all content found to be correlated to that fingerprint will be blocked in the future. Fingerprints do not expire or age out of existence.

Blacklisting: Numbers that have sent repeated known SPAM/unwanted content are subject to automatic blacklisting without notification for up to 30 days. Multiple or repeat offenses may result in permanent blacklisting. Additionally, numbers that have been reported by industry partners for SPAM/unwanted content may also be subject to permanent blacklisting.

5.0 Volumetric Limitations

5.1 Global Settings

These limitations apply at the customer level

5.1.1 SMPP

- 100 messages per second (6,000 messages per minute) per bind

5.1.2 REST

- Global account level throttles are not enforced currently. REST based messages are managed at the originating number level and are limited currently to 1 message per 200ms per single originating telephone number (5 messages per second per single originating telephone number).

5.2 Source Number Settings (applicable to both SMS and MMS)

5.2.1 Peer-to-Peer (P2P)

- 60 messages per minute from a single originating telephone number
- 100 distinct recipients/terminating telephone numbers per messages
- 1,000 messages per 24 hours from a single originating telephone number
- 1:1 ratio of outgoing to incoming messages per telephone number with some latitude in either direction 25 repetitive messages
- 1 telephone number assigned to or utilized by a single Consumer

5.2.2 Toll Free Numbers (8XX/10DLC)

- A2P enabled destinations (AT&T, Verizon, T-Mobile, Sprint, etc.): no additional defined per single originating toll free number velocity cap, see global thresholds listed above.
- P2P only destinations (Rogers, Bell Canada, etc.): defaults to lower velocity thresholds like policies applied to Local Telephone Numbers, see Local Telephone Number thresholds listed above.

6.0 Global Policies

6.1 General Rules of Content

Message senders should take affirmative steps and employ tools that monitor and prevent Unwanted Message content, including:

1. Unlawful, harmful, abusive malicious, misleading, harassing, excessively violent, obscene/illicit, or defamatory
2. Deceptive (e.g., phishing messages intended to access private or confidential information), including deceptive links
3. Invades privacy
4. Causes safety concerns
5. Incites harm, discrimination, or violence
6. Intended to intimidate

7. Includes malware
8. Threatens Consumers
9. Does not meet age-gating requirements

6.2 Inappropriate Use Cases

Due to high volumes of consumer complaints, messages containing the following content are not appropriate and may be blocked by carriers if sent over either P2P or A2P (Tollfree/10DLC) messaging, **regardless of opt-in status**.

If messaging traffic is identified by a provider as associated with one of the following use cases, there will be little that Inteliquent can do to assist in the removal of blocking.

1. Social marketing
2. Collections
3. Financial services, whether account notifications, marketing, collections or billing for:
    - High-risk/subprime lending/credit card companies
    - Auto loans
    - Mortgages
    - Payday loans
    - Short-term loans
    - Student loans
    - Debt consolidation/reduction/forgiveness
4. Insurance
    - Car Insurance
    - Health Insurance
5. Gambling, Casino, and Bingo
6. Gift cards
7. Sweepstakes
8. Free prizes
9. Investment opportunities
10. Lead generation
11. Recruiting
12. Commission programs
13. Credit repair
14. Tax relief
15. Illicit or illegal substances (including Cannabis)
16. Work from home
17. Get rich quick
18. UGGS and Rayban campaigns
19. Phishing
20. Fraud or scams
21. Cannabis
22. Deceptive marketing
23. SHAFT: Sex, Hate, Alcohol, Firearms or Tobacco

6.3 Additional Prohibited Practices

6.3.1 Snowshoe Messaging

Message Senders should not engage in Snowshoe Messaging, which is a technique used to spread messages across many sending phone numbers or short codes. Service Providers should also take measures to prevent Snowshoe Messaging.

6.3.2 Proxy Numbers

Message Senders might utilize a telephone number as a proxy number that functions as a relay point between possibly large sets of phone numbers and/or frequently changing phone numbers in certain wireless messaging use cases. For example, a driver for a ride-sharing service may need to communicate with a prospective passenger to confirm a pick-up location. The proxy telephone number functions as a conference call bridge telephone number, allowing the driver and passenger to communicate without either party having to reveal their personal telephone number. A 10-digit NANP telephone number used as a proxy is typically a means to connect two individuals, but proxy numbers are commonly reused in a way that may create volumes of messaging traffic that exceed typical Consumer operation. Given the use of proxy numbers to facilitate bulk messaging traffic among multiple 10-digit NANP telephone numbers, the proxy number qualifies as Non-Consumer (A2P) messaging traffic and may be subject to additional validation, vetting, and monitoring

6.3.3 Spoofing Telephone Numbers

Message number spoofing includes the ability of a Message Sender to cause a message to display an originating number for the message that is not assigned to the Message Sender, or when a Message Sender originates a message through a Service Provider other than the Service Provider to which reply messages will be delivered or received. Message number spoofing should be avoided and should comply with all applicable laws.

7.0 Consumer (P2P) Best Practices

Consumer (P2P) messaging is sent by a Consumer to one or more Consumers and is consistent with typical Consumer operation (i.e., message exchanges are consistent with conversational messaging among Consumers). Consumers do not include agents of businesses, organizations, or entities that send messages to Consumers.

8.0 Non-Consumer (A2P) Best Practices

8.1 Consumer Consent

The messaging ecosystem should operate consistent with relevant laws and regulations, such as the TCPA and associated FCC regulations regarding Consumer consent for communications. Regardless of whether these rules apply and to maintain Consumer confidence in messaging services, Non- Consumer (A2P) Message Senders should:

- Obtain a Consumer's consent to receive messages generally;
- Obtain a Consumer's express written consent to specifically receive marketing messages; and
- Ensure that Consumers have the ability to revoke consent.

Consent may vary upon on the type of message content exchanged with a Consumer. The following table provides examples of the types of messaging content and the associated consent that should be expected. The examples below do not constitute or convey legal advice and should not be used as a substitute for obtaining legal advice from qualified counsel. Reference to "business" below is used as an example of a Non-Consumer (A2P) Message Sender. Individual Service Providers may adopt additional Consumer protection measures for Non-Consumer (A2P) Message Senders, which may include, for example, campaign pre-approval, Service Provider vetting, in-market audits, or Unwanted Message filtering practices that are tailored to facilitate the exchange of wanted messaging traffic.

Exhibit II: Types of Messaging Content & Associated Consent Principles		
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 asks to be contacted in the future. Appointment reminders, welcome texts, and 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 only sent by a Consumer Two-way conversation	First message is sent by the Consumer or business One-way alert or two-way conversation	First message is sent by the business One-way alert
Message responds to a specific request	Message contains information	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 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.

8.2 Clear and Conspicuous Calls-to-Action

A "Call-to-Action" is an invitation to a Consumer to opt-in to a messaging campaign. The Call-to-Action for a single-message program can be simple. The primary purpose of disclosures is to ensure that a Consumer consents to receive a message and understands the nature of the program.

Message Senders should display a clear and conspicuous Call-to-Action with appropriate disclosures to Consumers about the type and purpose of the messaging that Consumers will receive.

A Call-to-Action should ensure that Consumers are aware of: (1) the program or product description; (2) the telephone number(s) or short code(s) from which messaging will originate; (3) the specific identity of the organization or individual being represented in the initial message; (4) clear and conspicuous language about opt-in and any associated fees or charges; and (5) other applicable terms and conditions (e.g., how to opt-out, customer care contact information, and any applicable privacy policy).

Calls-to-Action and subsequent messaging should not contain any deceptive language, and opt-in details should not be obscured in terms and conditions (especially terms related to other services).

8.3 Consumer Opt-In

Message Senders should support opt-in mechanisms, and messages should be sent only after the Consumer has opted-in to receive them. Opt-in procedures reduce the likelihood that a Consumer will receive an Unwanted Message. It can also help prevent messages from being sent to a phone number that does not belong to the Consumer who provided that phone number (e.g., a Consumer purposefully or mistakenly provides an incorrect phone number to the Message Sender).

Depending upon the circumstances, a Consumer might demonstrate opt-in consent to receive messaging traffic through several mechanisms, including but not limited to:

- Entering a telephone number through a website;
- Clicking a button on a mobile webpage;
- Sending a message from the Consumer's mobile device that contains an advertising keyword;
- Initiating the text message exchange in which the Message Sender replies to the Consumer only with responsive information;
- Signing up at a point-of-sale (POS) or other Message Sender on-site location; or
- Opting-in over the phone using interactive voice response (IVR) technology.

While the Common Short Code Handbook is a separate document specific to the Common Short Code program, the Common Short Code Handbook has additional examples of opt-in consent that may be helpful to Message Senders.

Message Senders should also document opt-in consent by retaining the following data where

applicable:

- Timestamp of consent acquisition;
- Consent acquisition medium (e.g., cell-submit form, physical sign-up form, SMS keyword, etc.);
- Capture of experience (e.g., language and action) used to secure consent;
- Specific campaign for which the opt-in was provided;
- IP address used to grant consent;
- Consumer phone number for which consent to receive messaging was granted; and
- Identity of the individual who consented (name of the individual or other identifier (e.g., online user name, session ID, etc.)).
-

8.4 Confirm Opt-In Confirmation for Recurring Messages

Message Senders of recurring messaging campaigns should provide Consumers with a confirmation message that clearly informs the Consumer they are enrolled in the recurring message campaign and provides a clear and conspicuous description of how to opt-out.

After the Message Sender has confirmed that a Consumer has opted-in, the Message Sender should send the Consumer an opt-in confirmation message before any additional messaging is sent.

The confirmation message should include: (1) the program name or product description; (2) customer care contact information (e.g., a toll-free number, 10-digit telephone number, or HELP command instructions); (3) how to opt-out; (4) a disclosure that the messages are recurring and the frequency of the messaging; and (5) clear and conspicuous language about any associated fees or charges and how those charges will be billed.

8.5 Single Opt-In per Campaign

A Consumer opt-in to receive messages should not be transferable or assignable. A Consumer opt-in should apply only to the campaign(s) and specific Message Sender for which it was intended or obtained.

8.6 Consumer Opt-Out

Opt-out mechanisms facilitate Consumer choice to terminate messaging communications, regardless of whether Consumers have consented to receive the message. Message Senders should acknowledge and respect Consumers' opt-out requests consistent with the following guidelines:

- Message Senders should ensure that Consumers have the ability to opt-out of receiving Messages at any time;
- Message Senders should support multiple mechanisms of opt-out, including phone call, email, or text; and
- Message Senders should acknowledge and honor all Consumer opt-out requests by sending one final opt-out confirmation message per campaign to notify the Consumer that they have opted-out successfully. No further messages should be sent following the confirmation message.

Message Senders should state in the message how and what words effect an opt-out. Standardized "STOP" wording should be used for opt-out instructions, however opt-out requests with normal language (i.e., stop, end, unsubscribe, cancel, quit, "please opt me out") should also be read and

acted upon by a Message Sender except where a specific word can result in unintentional opt-out. The validity of a Consumer opt-out should not be impacted by any de minimis variances in the Consumer opt-out response, such as capitalization, punctuation, or any letter-case sensitivities.

8.7 Renting, Selling, or Sharing Opt-In Lists

Message Senders should not use opt-in lists that have been rented, sold, or shared to send messages. Message Senders should create and vet their own opt-in lists.

8.8 Maintaining and Updating Consumer Information

Message Senders should retain and maintain all opt-in and opt-out requests in their records to ensure that future messages are not attempted (in the case of an opt-out request) and Consumer consent is honored to minimize Unwanted Messages. Message Senders should process telephone deactivation files regularly (e.g., daily) and remove any deactivated telephone numbers from any opt-in lists.

8.9 Privacy and Security

Message Senders should address both privacy and security comprehensively in the design and operation of messaging campaigns.

8.9.1 Maintain and Conspicuously Display a Clear, Easy-to-Understand Privacy Policy

Message Senders should maintain and conspicuously display a privacy policy that is easily accessed by the Consumer (e.g., through clearly labeled links) and that clearly describes how the Message Sender may collect, use, and share information from Consumers. All applicable privacy policies should be referenced in and accessible from the initial call-to-action. Message Senders also should ensure that their privacy policy is consistent with applicable privacy law and that their treatment of information is consistent with their privacy policy.

8.9.2 Implement Reasonable Physical, Administrative, and Technical Security Controls to Protect and Secure Consumer Information

Message Senders should implement reasonable security measures for messaging campaigns that include technical, physical, and administrative safeguards. Such safeguards should protect Consumer information from unauthorized access, use, and disclosure. Message Senders should conduct regular testing and monitoring to ensure such controls are functioning as intended.

8.9.3 Conduct Regular Security Audits

Message Senders should conduct either a comprehensive self-assessment or third-party risk assessment of privacy and security procedures for messaging campaigns on a regular basis and take appropriate action to address any reasonably foreseeable vulnerabilities or risks.

8.10 Content

8.10.1 Prevention of Unlawful Activities or Deceptive, Fraudulent, Unwanted, or Illicit Content

Message Senders should use reasonable efforts to prevent and combat unwanted or unlawful messaging traffic, including spam and unlawful spoofing. Specifically, Message Senders should take affirmative steps and employ tools that can monitor and prevent Unwanted Messages and content, including for example content that: (1) is unlawful, harmful, abusive, malicious, misleading, harassing, excessively violent, obscene/illicit, or defamatory; (2) deceives or intends to deceive (e.g., phishing messages intended to access private or confidential information); (3) invades privacy; (4) causes safety concerns; (5) incites harm, discrimination, or violence; (6) is intended to intimidate; (7) includes malware; (8) threatens Consumers; or (9) does not meet age-gating requirements. Message Senders can also review the Common Short Code Handbook for further examples of Unwanted Message content.

Further, Message Senders should take steps to ensure that marketing content is not misleading and complies with the Federal Trade Commission's (FTC) Truth-In-Advertising rules.

8.10.2 Embedded Website Links

Message Senders should ensure that links to websites embedded within a message do not conceal or obscure the Message Sender's identity and are not intended to cause harm or deceive Consumers.
Where a web address (i.e., Uniform Resource Locator (URL)) shortener is used, Message Senders should use a shortener with a web address and IP address(es) dedicated to the exclusive use of the Message Sender. Web addresses contained in messages as well as any websites to which they redirect should unambiguously identify the website owner (i.e., a person or legally registered business entity) and include contact information, such as a postal mailing address.

8.10.3 Embedded Phone Numbers

Messages should 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.

8.11 Text-Enabling a Telephone Number for Non-Consumer (A2P) Messaging

An authentication and validation process should be used to verify the Message Senders' authority to enable Non-Consumer (A2P) messaging for a specific telephone number. Message Senders should only enable Non-Consumer (A2P) messaging with a telephone number that the Message Sender has been assigned by a provider of telecommunications or interconnected Voice over Internet Protocol (VoIP) services.

9.0 Technical Message Specifications

9.1 Message Content Length

- UCS-2 (16 bit) = 70 character maximum. For longer multipart messages, a User Data Header (UDH) is added to the message to instruct the receiving device on how to reassemble the message, resulting in a maximum of 67 characters for the body of the message.
- Latin1 (8 bit) = 140 character maximum. For longer multipart messages, a User Data Header (UDH) is added to the message to instruct the receiving device on how to reassemble the message, resulting in a maximum of 134 characters for the body of the message.
- GSM7 (7 bit) = 160 character maximum. For longer multipart messages, a User Data Header (UDH) is added to the message to instruct the receiving device on how to reassemble the message, resulting in a maximum of 153 characters for the body of the message.
- Any message segment which has been broken up from a single message due to length will be treated as a single message as will messages to multiple recipients.

9.2 MMS Specific Policies

- **Maximum file size:** operators support different maximum file attachment sizes. Files of 2Mb or less will be resized to the appropriate destination operator defined limit. Files over 2Mb are not supported and will be rejected.
- **File types:** below is a list of currently supported file types. File types outside of this list are not supported and will be rejected.

File Type	Extension
audio/3gpp	.3gp
audio/amr	.amr
audio/amr	.3ga
audio/mp4	.m4a
audio/mp4	.m4p
audio/mp4	.m4b
audio/mp4	.m4r
audio/mpeg	.mp3
audio/wav	.wav
image/bmp	.bmp
image/bmp	.dib
image/gif	.gif
image/jpeg	.jpg
image/jpeg	.jpeg
image/png	.png
video/3gpp	.3gp
video/h263	.h263
video/h264	.h264
video/mp4	.mp4
video/mp4	.m4v

10.0 Resources

This section includes links to industry resources that may be helpful as a message sender starts to craft messaging content. Messages should follow guidance from these resources, otherwise messages may be blocked.

CTIA Messaging Principles and Best Practices
https://api.ctia.org/wp-content/uploads/2019/07/190719-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf

MMA Best Practices
http://www.mmaglobal.com/taxonomy/term/2820

M3AAWG Best Practices
https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015- 08.pdf

Telephone Consumer Protection Act (TCPA) Omnibus Declaratory Ruling (FCC 15-72)
https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.pdf

FTC Truth in Advertising
https://www.ftc.gov/news-events/media-resources/truth-advertising