sinch

E-BOOK

US SMS compliance guide

Summary

SMS is the most powerful communication channel for engaging your customers. In fact, people are 35x more likely to read a text message than an email.

But even armed with that knowledge, starting with SMS can be tough. Compliance rules, like the Telephone Consumer Protection Act (TCPA) or requirements from industry regulators and wireless carriers, can complicate things. Regardless, you need to take SMS compliance seriously. These rules protect customer data, privacy, and improve the overall customer experience. We get it – headaches aren't fun, and we're not fans either. At Sinch, simplicity is our thing. Our cloud communications platform, including SMS, makes reaching your audience easy. We're here to help you send SMS the compliant way.

Note that we can't give you legal advice. Talk to your legal team to see how these regulations apply to your specific business. But we can simplify the basics and give you an overview of the rules, what they mean, and how to handle them.

In this guide we'll cover:

- TCPA and CTIA guidelines on consent and best practices
- A2P vs P2P messaging
- Sender IDs and number types
- Consent management
- SHAFT content
- Carrier expectations - code of conduct, playbooks, and policies

We've also got a handy compliance self-checklist for you, and lots of additional resources. Let's get started!

Background

Okay, let’s get the lay of the land. In the United States, there are government rules and policies on how to send SMS.

Each carrier has its own set of guidelines, and there are also new codes of conduct which aren’t laws but must be followed. Ignore them, and your campaigns might never take off, or end up blocked in carrier or aggregator filters. And you don’t want that!

In the U.S., remember three main frameworks:
First, the regulations under the Telephone Consumer Protection Act (TCPA); second, the guidelines under the Cellular Telephone Industries Association (CTIA), which includes carrier playbooks, policies, and codes of conduct; and third, oversight by the Federal Communications Commission (FCC) which regulates safe and fair use of interstate and international communications. The Mobile Marketing Association's U.S. Consumer Best Practices for Messaging guide is also a helpful resource — more on that later.

Let’s start with the TCPA.

The Telephone Consumer Protection Act (TCPA)

Alright, this is an important one. U.S. Congress passed the TCPA in 1991 to curb unwanted telemarketing calls. It covers all telemarketing, text messages, and pre-recorded calls. The most important rule of the TCPA is that **companies can’t contact consumers without prior expressed written consent**. The needed consent type varies based on factors like the message’s content, device, and technology used to send the message.

A key fact to remember is that the TCPA applies even if you accidentally target the wrong number - perhaps due to a call being reassigned or ported. So, make sure to verify customers before reaching out. Do your homework!

TCPA violations are serious. Consumers can sue, and major companies have paid hefty fines of hundreds of millions of dollars. You definitely don’t want to join that club.

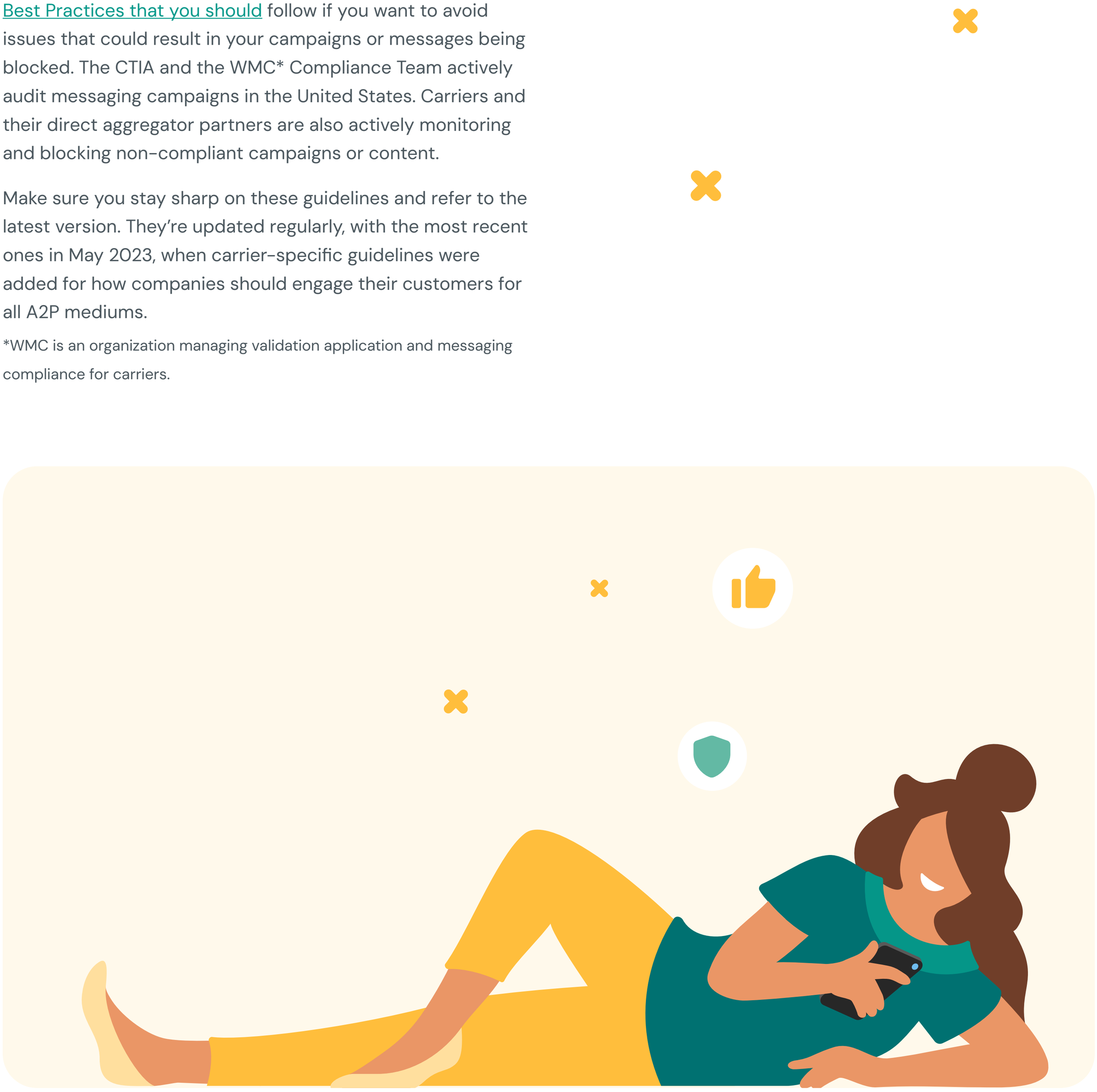
The Cellular Telecommunications and Internet Association (CTIA) guidelines

The CTIA is a trade association representing the U.S. wireless communications industry. It includes representatives from a wide range of companies like wireless carriers, CPaaS companies, VoIP operators, manufacturers, etc. Their goal is to maintain the most positive experience possible for end-users.

To that end, the CTIA publishes the Messaging Principles and Best Practices that you should follow if you want to avoid issues that could result in your campaigns or messages being blocked. The CTIA and the WMC* Compliance Team actively audit messaging campaigns in the United States. Carriers and their direct aggregator partners are also actively monitoring and blocking non-compliant campaigns or content.

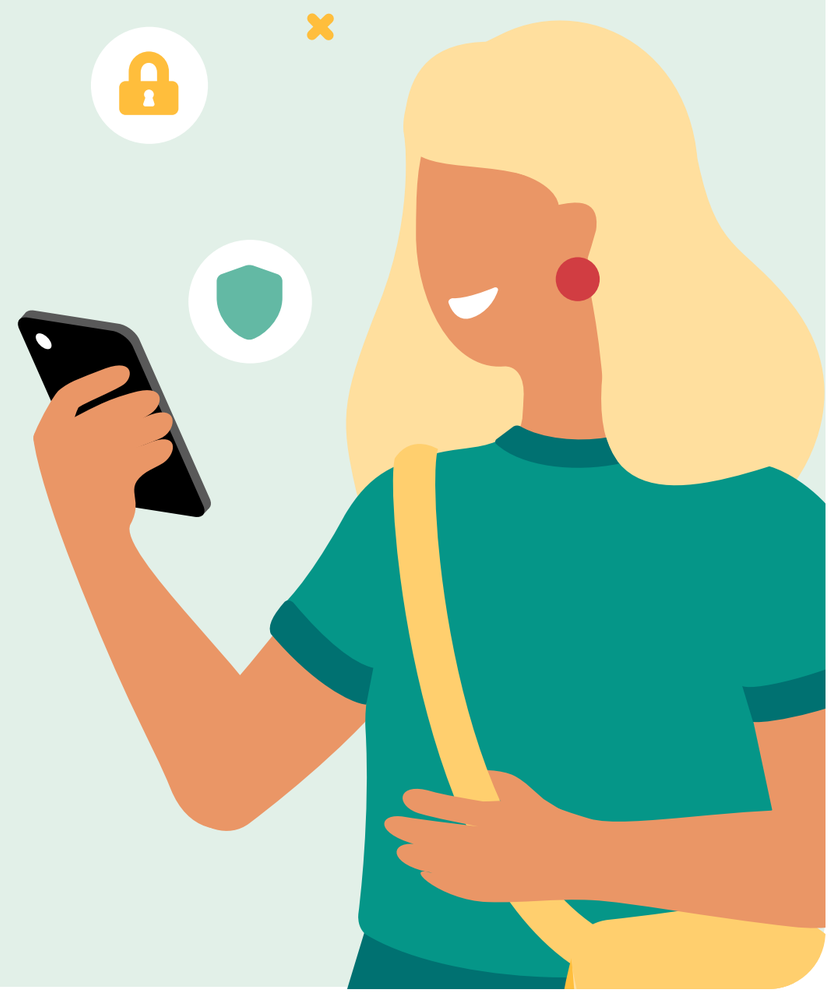
Make sure you stay sharp on these guidelines and refer to the latest version. They're updated regularly, with the most recent ones in May 2023, when carrier-specific guidelines were added for how companies should engage their customers for all A2P mediums.

*WMC is an organization managing validation application and messaging compliance for carriers.



Sinch Sender IDs and number types used in U.S. messaging

Let’s go through what number types Sinch offers for A2P traffic in the United States, the benefits of each, and how compliance affects them.

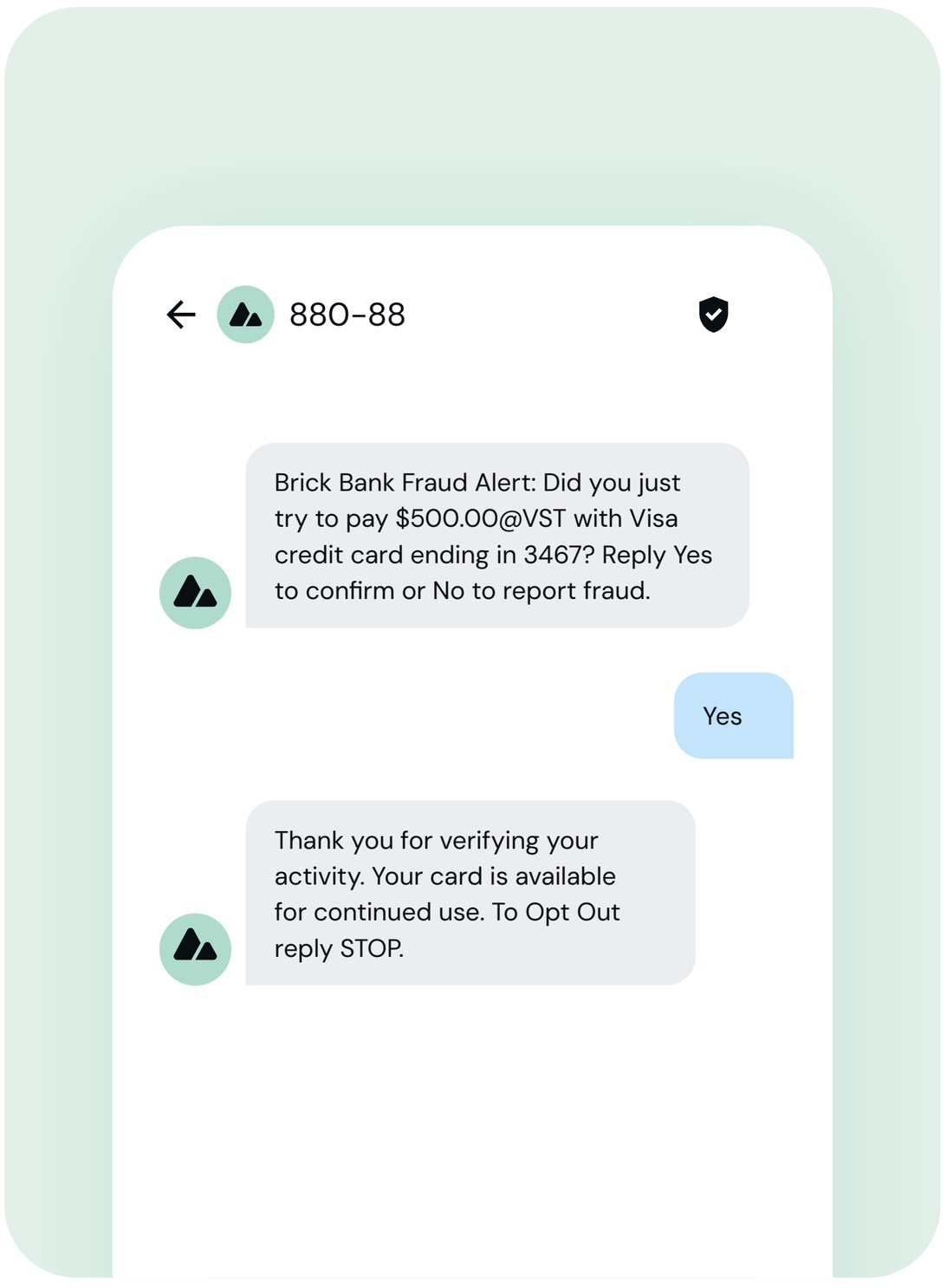


Short codes

Let’s talk short codes – they’re as straightforward as they sound, and are short numbers (four to six digits) that companies use to send messages to subscribers. Many companies choose a "vanity code," available at a premium that are a five- or six-digit phone numbers that you specifically select to represent your brand. You can also select random (leased) short codes for a discount. It’s up to you – select what suits your business best!

It’s important to keep in mind that U.S. short codes only work for U.S.- based carriers and their consumers in the United States and United States territories, not for people using providers from other countries. For example, a U.S. short code won’t be delivered to a German phone, but would work on a U.S. phone while its owner is travelling in Germany.

Keep this in mind: Short code numbers usually need approval and provisioning, and this process can take anywhere from two to eight weeks. They also undergo regular CTIA audits to ensure proper use. Short codes don’t support voice traffic today.



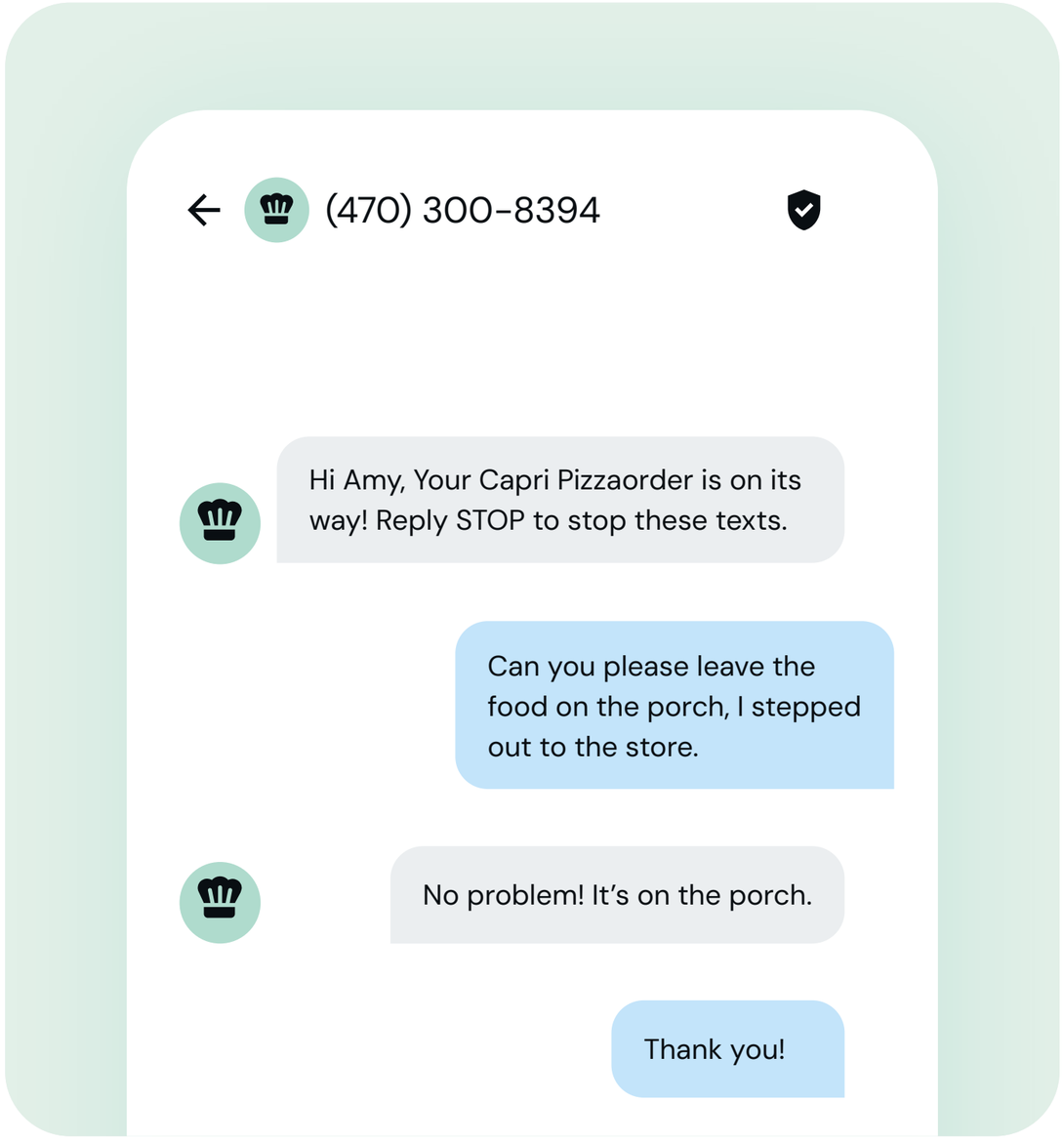
Long codes

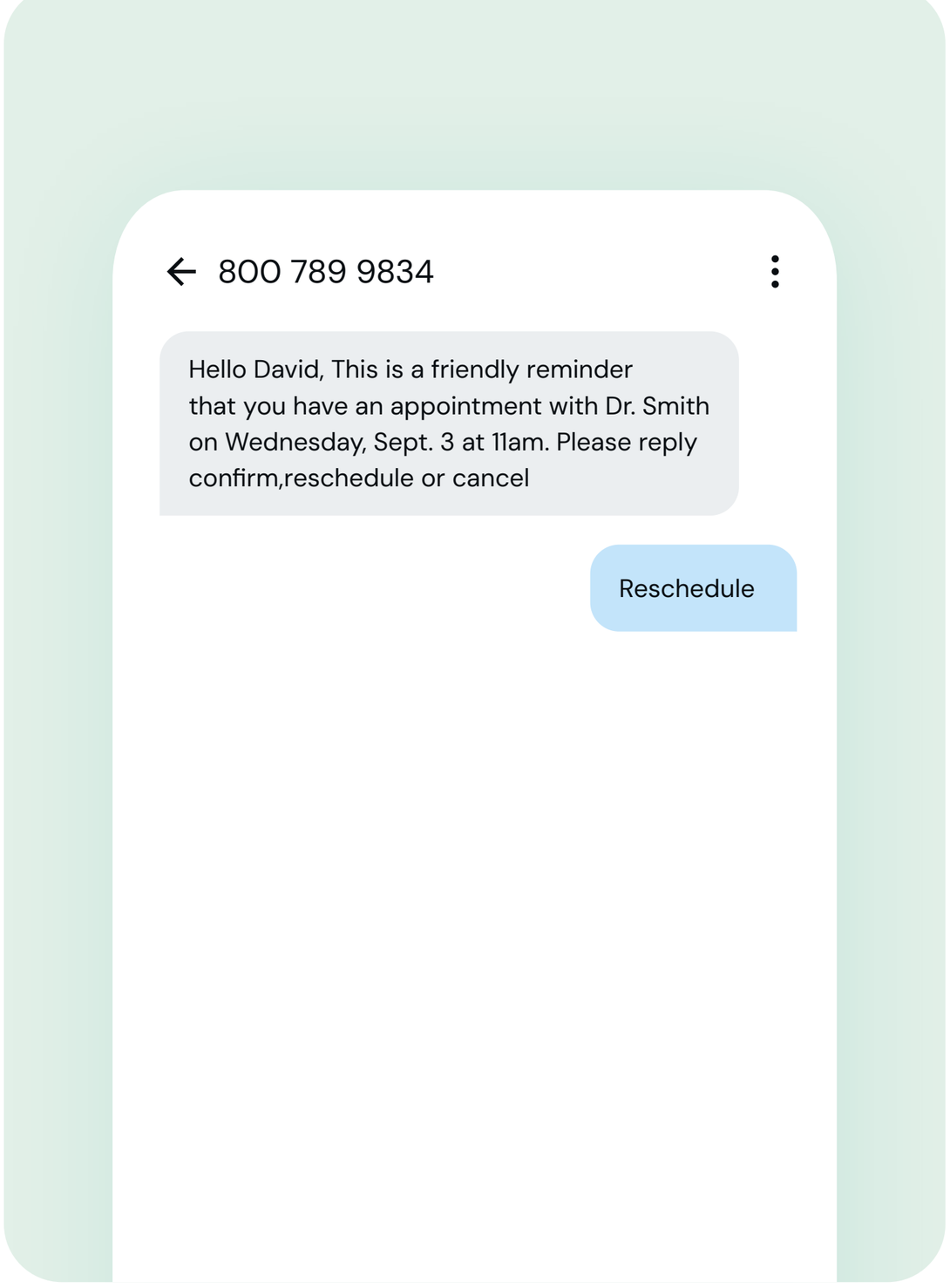
Next, let's dive into long codes – these go by many different names like 10-Digit Long Codes (10DLC), Long Number, Local Virtual Number (LVN), and Landlines, but they all share one thing: 10 digits. Unlike short codes, they have a quicker provisioning cycle and handle voice, SMS and MMS.

The industry is shifting to a registered A2P 10DLC model that incorporates identity checks, vetting, and campaign approval during onboarding.

10DLC numbers are a new messaging solution in the United States which use a local number tied to your business. They support voice services and MMS, but not delivery receipts. These area-code specific numbers let you send two-way conversations and send powerful messages with images and videos so you can stand out in campaigns. Plus, with 10DLC, you avoid getting caught up in spam filters with carrier campaign registration.

Find out more about Sinch 10DLC – we're here to help you get up-and-running!





Toll-Free Numbers (TFN)

Toll-free numbers are what they sound like in that there's no charge for the end user. The caller or sender pays for the costs of the phone call or text, making these numbers more trusted by customers. Toll-free numbers begin with one of the following three-digit area codes: 800, 888, 877, 866, 855, 844, or 833. These all belong to the North American Numbering Plan (NANP), and just like other 10-digit numbers, they can be used for SMS, MMS, and voice. They're quick to set up – you can get them up and running in just three to five days. Also, like other long codes, toll-free numbers can be filtered by the carrier if established guidelines aren't followed. Toll-free numbers can support fast throughput, at speeds comparable to short codes, depending on the use case.

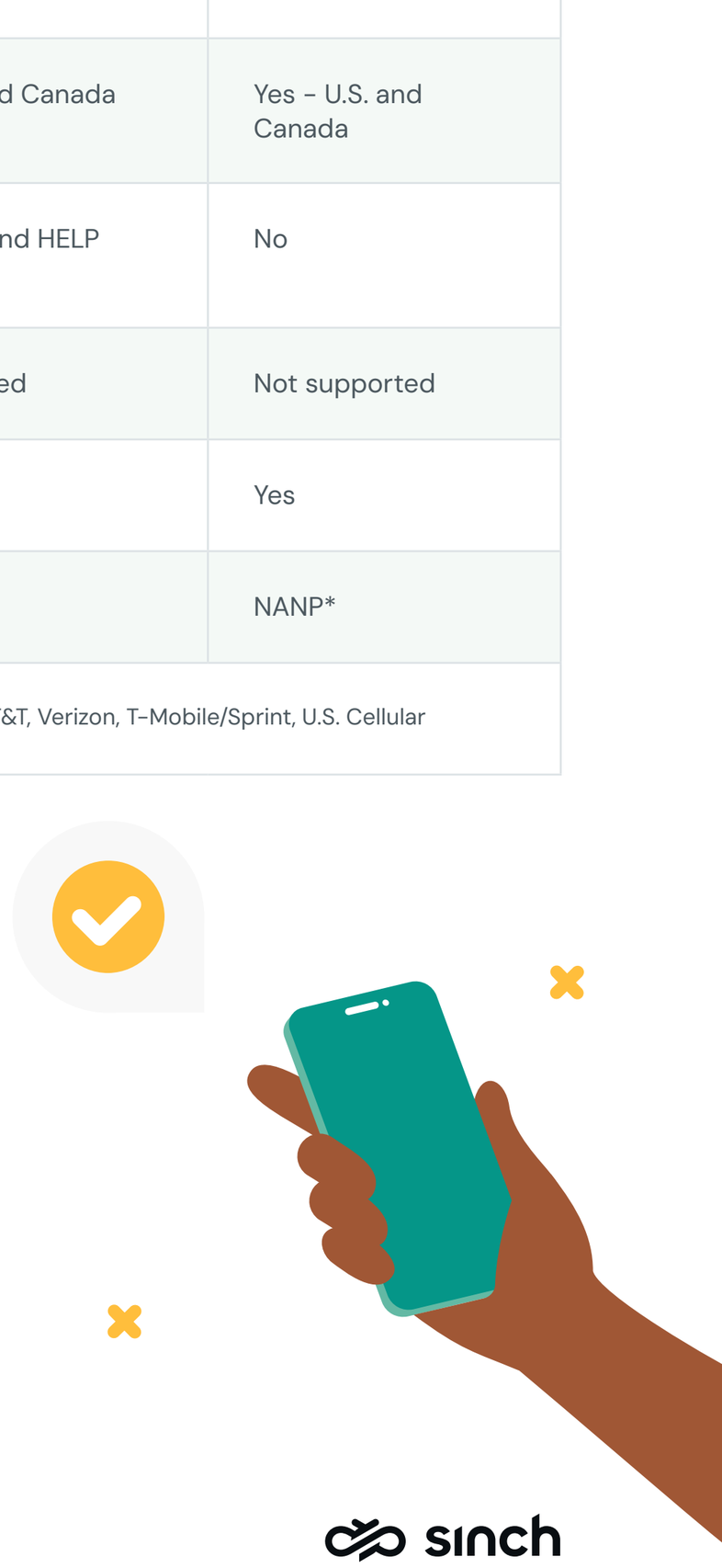
Want a memorable number? Then you need a toll-free vanity number – it's a customized number that spells and means something or it contains an easily recognized numeric pattern. An easily remembered number is valued as a branding and direct response tool in business advertising.

To summarize: there are different types of numbers with different benefits and different aspects to consider. Here's a useful chart for reference.

Product Features	Short Code	Toll-Free Number	10DLC(10 Digit Long Code)	Traditional Long Numbers
Digit length	5-6 digits	10 digits	10 digits	10 digits
Messaging model	A2P	A2P	A2P	P2P
Voice enabled	No	Yes	Yes	Yes
Requires brand vetting	No	No	Recommended	No
Requires campaign approval	Yes	Yes	Yes, via TCR (The Campaign Registry)	No
Provisioning	3-6 weeks	3-5 days	Standard: 3-5 days SBC: 3-4 weeks	1-3 days
Throughput	500 msg/sec	10 msg/sec default (higher TPS available based on use case)	Up to 75 TPS with MNO approval	1 msg/sec
Delivery Receipts	Yes	Yes, U.S., partial in Canada	No handset DLR, SMSC DLR in most of NANP*	No
MMS	Yes - U.S. only	Yes, U.S. and Canada	Yes - U.S. and Canada	Yes - U.S. and Canada
2-way/Keywords required	Opt-in/out and HELP	STOP, UNSTOP - network managed	Opt-in/out and HELP	No
FTEU	Available	Not supported	Not supported	Not supported
Vanity numbers	Yes	Yes	Yes	Yes
Reach	Country-specific	NANP*	NANP*	NANP*

*NANP: North American Numbering plan countries: U.S., Canada, U.S. territories , and the Caribbean Supported US Carriers for 10DLC: AT&T, Verizon, T-Mobile/Sprint, U.S. Cellular

There are also some things you need to keep in mind regardless of number type – so let's move on to the fun part!



Compliance commandments

It’s time for the Golden Rule of compliant A2P messaging: Consent, consent, consent!

These rules and regulations exist to make sure customers only get the messages they want. Following the CTIA Messaging Guidelines, all A2P messaging needs customer consent, with the level depending on message type and frequency,

Every A2P messaging campaign must include opt-out keywords – if a customer wants to revoke their consent, your campaign must let them.

Types of messaging content and required consent

Consumer-initiated conversational	Informational	Promotional
Conversational messaging is a back-and-forth conversation via text. If the consumer initiates the conversation and the business simply responds, then it is likely conversational and no additional permission is expected.* *Please note, this applies only if you send a single message back or if it’s a direct response to a single message from the consumer. You can’t continue to message them regularly otherwise.	Informational messaging is when a consumer gives their phone number to a business and provides their consent to be contacted in the future for a non-promotional purpose. Appointment reminders, welcome texts, and other non-promotional alerts fall into this category.	Promotional messaging 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. Businesses require the consumer’s written consent to send promotional messages..
First message is always sent by the consumer Two-way conversation Message responds to a specific request	First message is sent by the consumer or business One-way or two-way conversation Message contains information	First message is sent by the consumer or business One-way or two-way conversation Message contains information
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 needs to give permission before a business sends them a text message. They can give consent over text, on a form, on a website, or verbally. * Please note, you need prior written consent for any recurring messaging. Informational content is not an exception.	EXPRESS WRITTEN CONSENT The consumer should give express written permission before a business sends them a text message. This could be via signing a form, checking a box online, or some other method.

Require consent (aka opt-in)

An opt-in is when you ask a customer if you can message them, and they say yes. You need to be clear about what the customer can expect: What type of messages do you intend to send, and for what purpose?

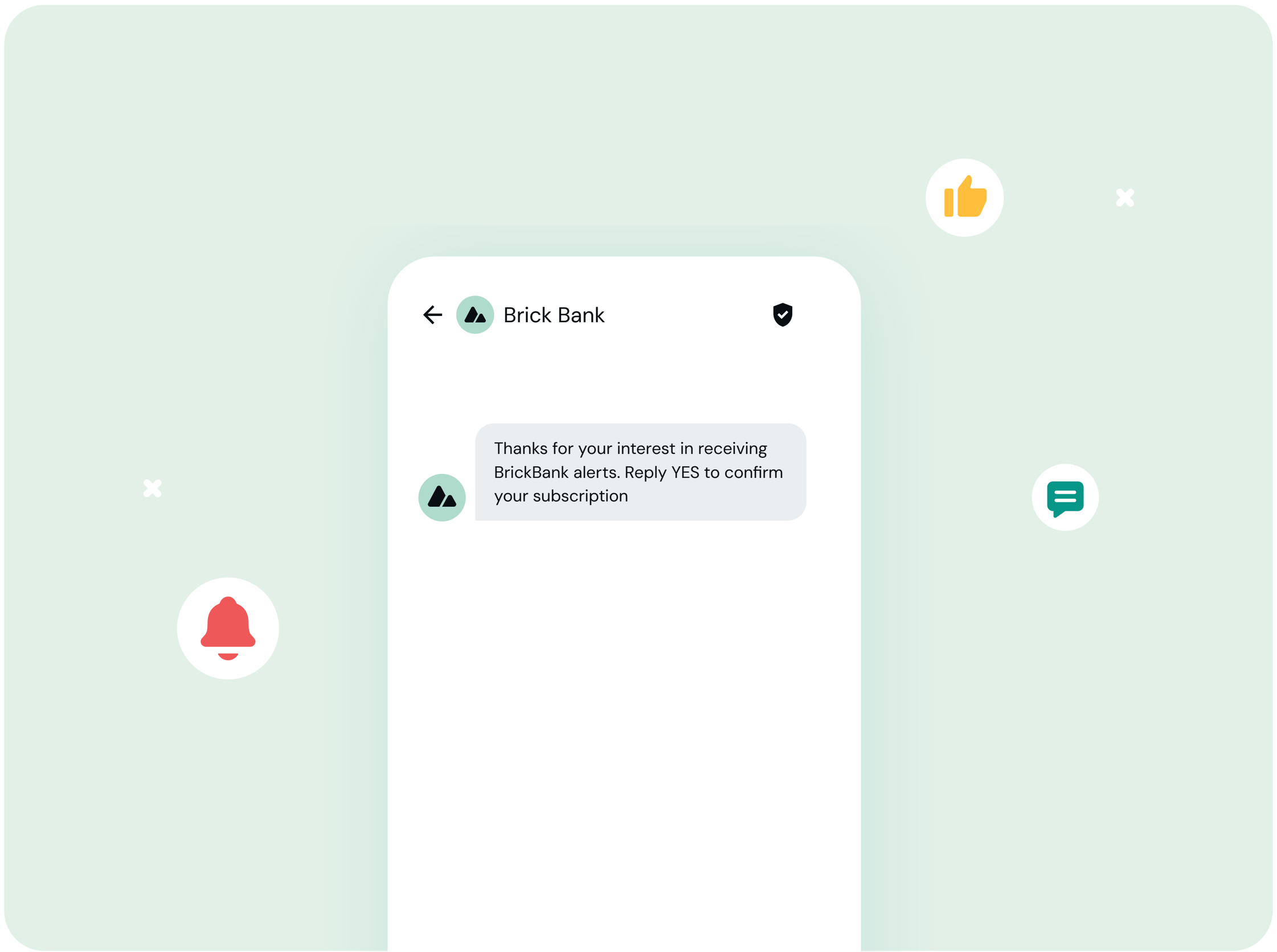
It's also important to note that you can't re-purpose an opt-in for one kind of communication for other kinds of communications. For example, a user who gives you consent to receive a one-time password (OTP) via text message is not consenting to marketing texts.

Under TCPA rules, there are also certain types of opt-ins, like automated recurring SMS marketing messages, that need written documentation. It's important to note that not all automated SMS messages require prior written consent. For example, a single interaction automated SMS response does not require prior written consent.

If you plan on sending promotional messages to customers, be thorough in logging all opt-ins, and keep consent records of when and how you received their consent.

Documenting all opt-ins for a minimum of 90 days is best practice. This provides proof that you've received consent to send to that destination number. Better safe than sorry!

Note that many companies use double opt-ins. After the initial opt-in, they send a welcome or first message, reminding them that they signed up. They then ask for a positive confirmation through a Keyword (Y, Yes, OK, Begin, etc.) This isn't an industry rule, but it's a best practice – and you want to be the best, right?



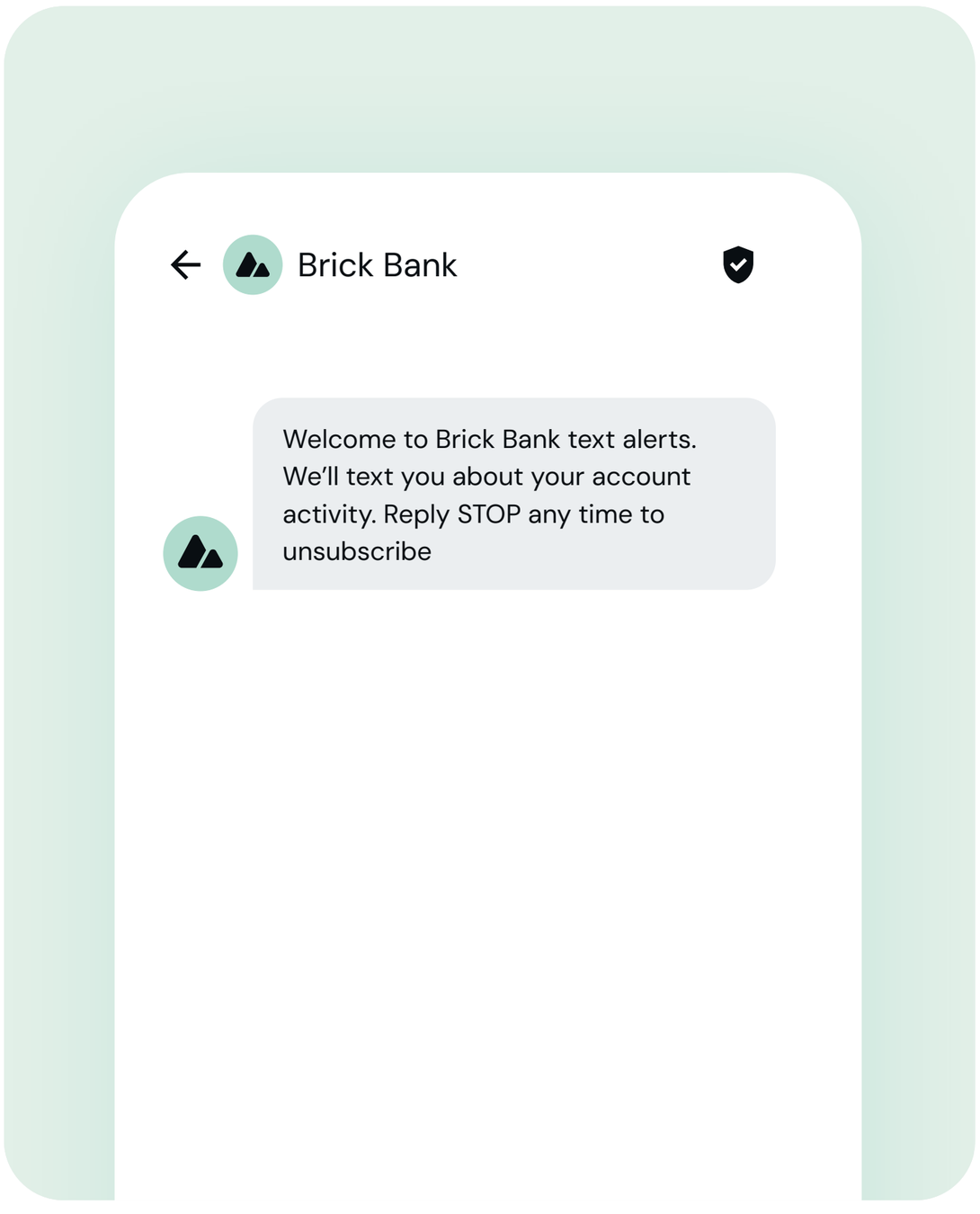
Honor opt-outs

Even if a customer agrees to let you message them with an opt-in, they can always change their mind – and you need to make it easy for them to do so.

The most common and minimum required opt-out method is to let consumers respond to the SMS with the text “STOP,” but there are other ways to handle opt-outs as well. The Federal Communications Commission (FCC) states that customers must be able to opt-out through “any reasonable means.” This could be a phone call, a text message, a web form, etc. – as long as it’s not too complicated for the user. Businesses are required by carriers that at least one message per month contains STOP info for users to have the option of opting out of receiving further messages.

Make sure that when users send an opt-out request, you acknowledge it. Failing to do so can get you into trouble (Please note that Sinch is not responsible for any action taken against a business due to messaging complaints).

Brands should also watch out for variations of common opt-out keywords. Those variations to STOP could be “STIP, S T O P. S t op. S TOP, S-T-O-P, SPAM, sstop, Stip, stop, sTOP. There are numerous variations that brands should be aware of and looking for.



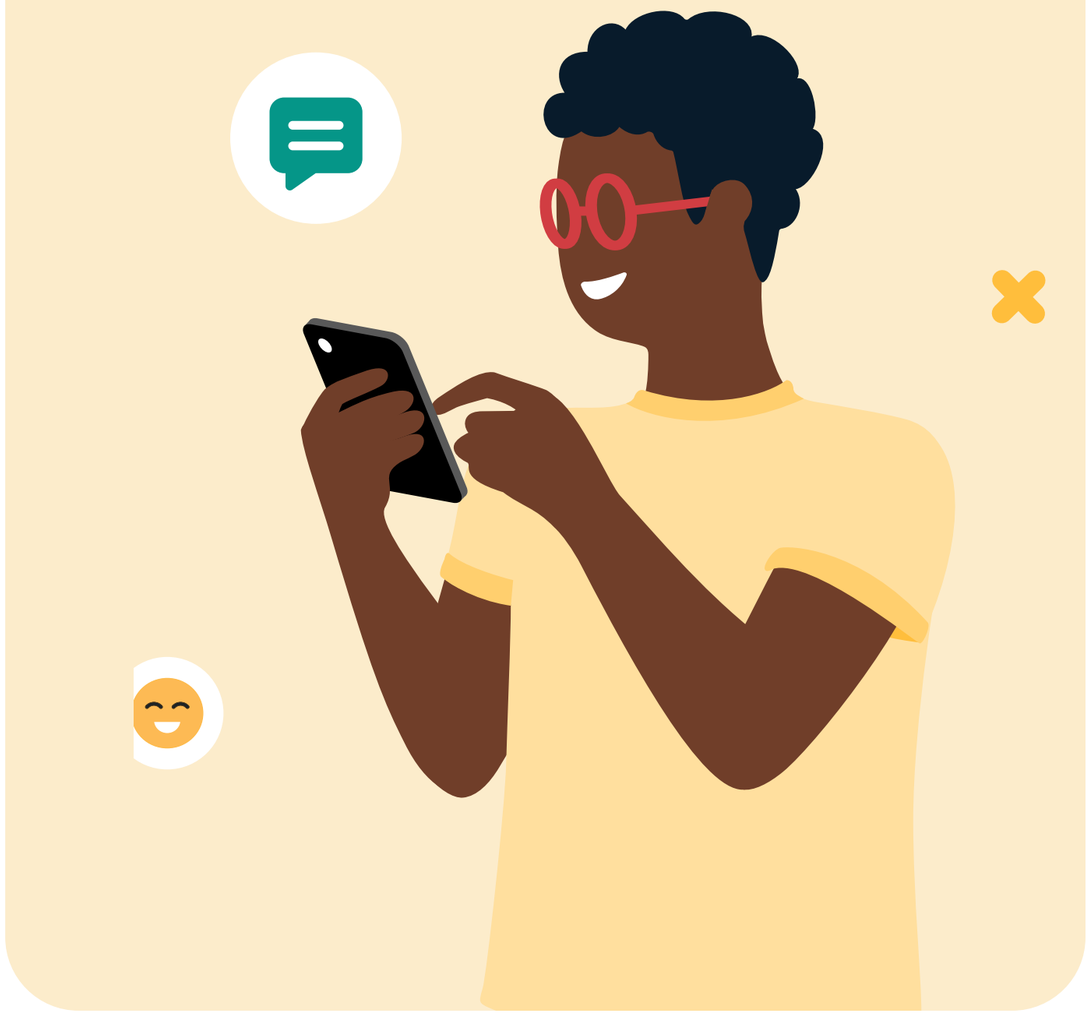
Avoid public URL shorteners for TFN and 10DLC campaigns

Although shortened URLs help make messages more concise, it’s crucial to follow some important rules and best practices to ensure successful message delivery and a good user experience.

When sending your 10DLC and TFN campaigns, never use shared public URL shorteners, such as free TinyUrl or Bitly links.

U.S. carrier policies strongly discourage the use of shared public URL shorteners due to the frequency of use by spammers, scammers, and other bad actors. The use of these public shared shorteners will result in higher risk of filtering and blocking.

When sending SMS or MMS messages with shortened URLs to users in the United States, use a dedicated, branded domain owned by your business.



Keep it SHAFT-free

In addition to honoring opt-ins and opt-outs, we've got another commandment for you: Stay free of SHAFT! SHAFT is a handy acronym to help you remember types of content that's either forbidden or subject to special rules (also called age-gating rules).

S: Sexually inappropriate content

H: Hate speech or profanity

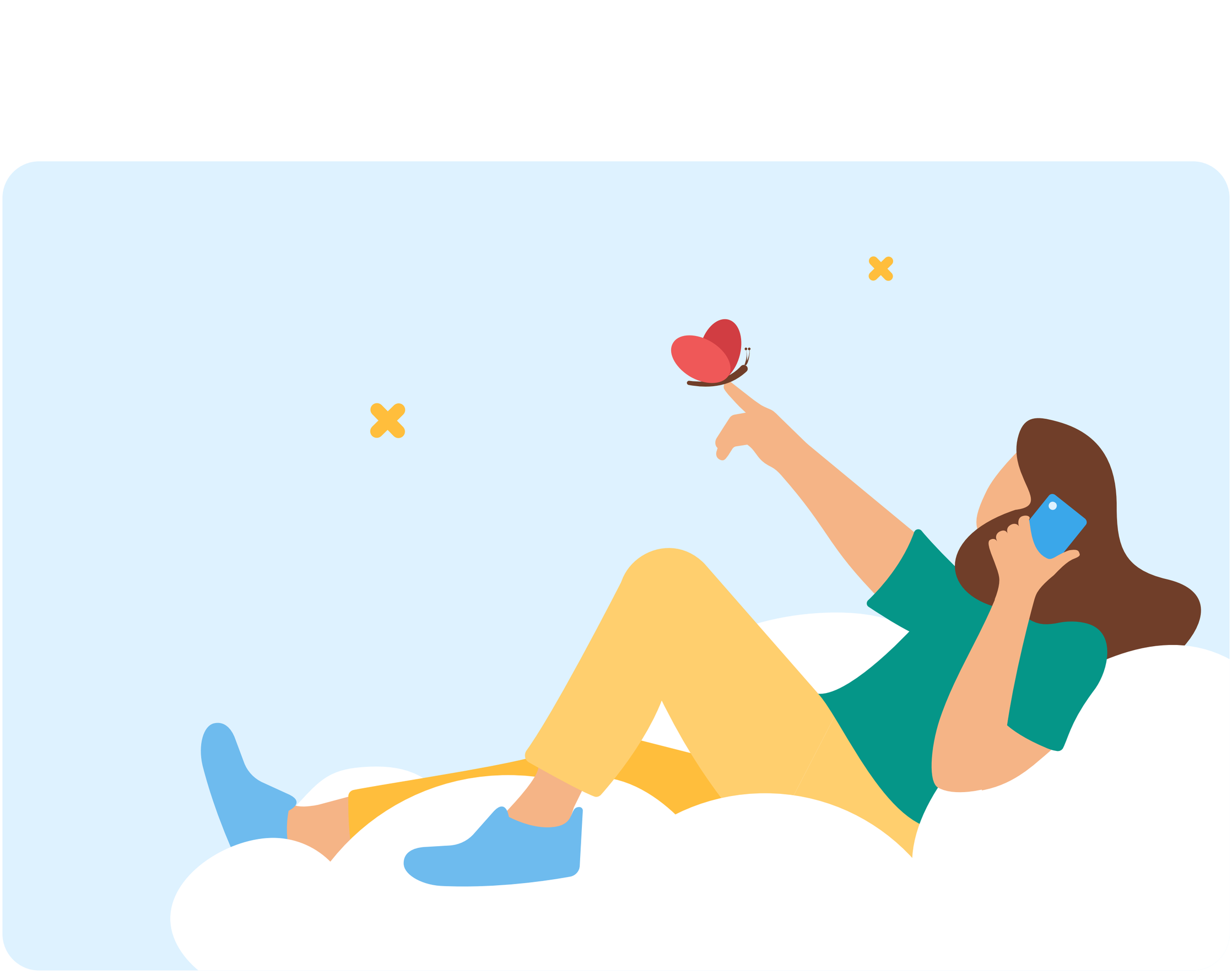
A: Alcohol (Only with proper age-gating)

F: Firearms, and depictions or endorsements of violence (Only with proper age-gating)

T: Tobacco (Only with proper age-gating)

Note: Some of this content, like that from "adult" businesses like nightclubs, bars that serve alcohol, and firearms or tobacco sales, may be allowed by certain carriers if a campaign is submitted and approved in advance and a functioning "age-gate" is in place. However, content promoting the use of marijuana, including businesses selling cannabidiol must not be sent on a U.S. short code, TFN or 10DLC.

Additionally, promoting gambling is not allowed, but, a casino may run other types of campaigns (For example, Harris Casino: Come check out our buffet! or Harris Casino: Hey Karlton come check out JLo in concert on May 28th!).



Understanding carrier expectations for short code campaigns

There are some extra guidelines you should keep in mind when running short code campaigns. For detailed information, see the Common Short Code Handbook (CSC) from the CTIA.

When planning a short code campaign, try to keep in mind five key questions from the customer's perspective. The answers should be clear:

- Who's the sender?
- What's the offer?
- Where can I learn more?
- When will this service contact me?
- How do I use the service, and how do I opt-out?

We recommend having a strong call to action (CTA) for every campaign.

Please keep in mind that even though the CSC Handbook is specific to short codes, the same rules and guidelines are applied to TFN and 10DLC campaigns.

Call to action

Getting your short code program off the ground starts with a solid call to action (CTA). A CTA both describes a mobile program and instructs potential users on how to participate.

Carriers audit live short code programs regularly to ensure ongoing compliance starting with the program certification process. So, a good start is key. Remember, carrier aim for a consistent user experience across all short code programs.

Example CTAs

The following is an example of a live call to action:

Text SMS to 12345 for mobile marketing tips from Sinch Messenger. 2msgs/mo. Msg&dataRatesMayApply.
Privacy Policy: [Link to privacy policy]
Mobile Terms & Conditions: [Link to Terms & Conditions]

Please keep in mind that on a web page, the T&Cs and Privacy Policy may take the form of linked text, but in print CTAs the full URL must be explicitly shown.

Cross-media CTA requirements

What's required for a successful call to action depends on the media it's published in. Carriers look for specific elements in all CTAs

- X Company name
- X Program name
- X Description of offer
- X Where to find terms and conditions
- X Privacy policy location
- X Customer support information*
- X Opt-in instructions
- X Opt-out instructions (if recurring) **
- X Message and data rates disclaimer
- X Message frequency

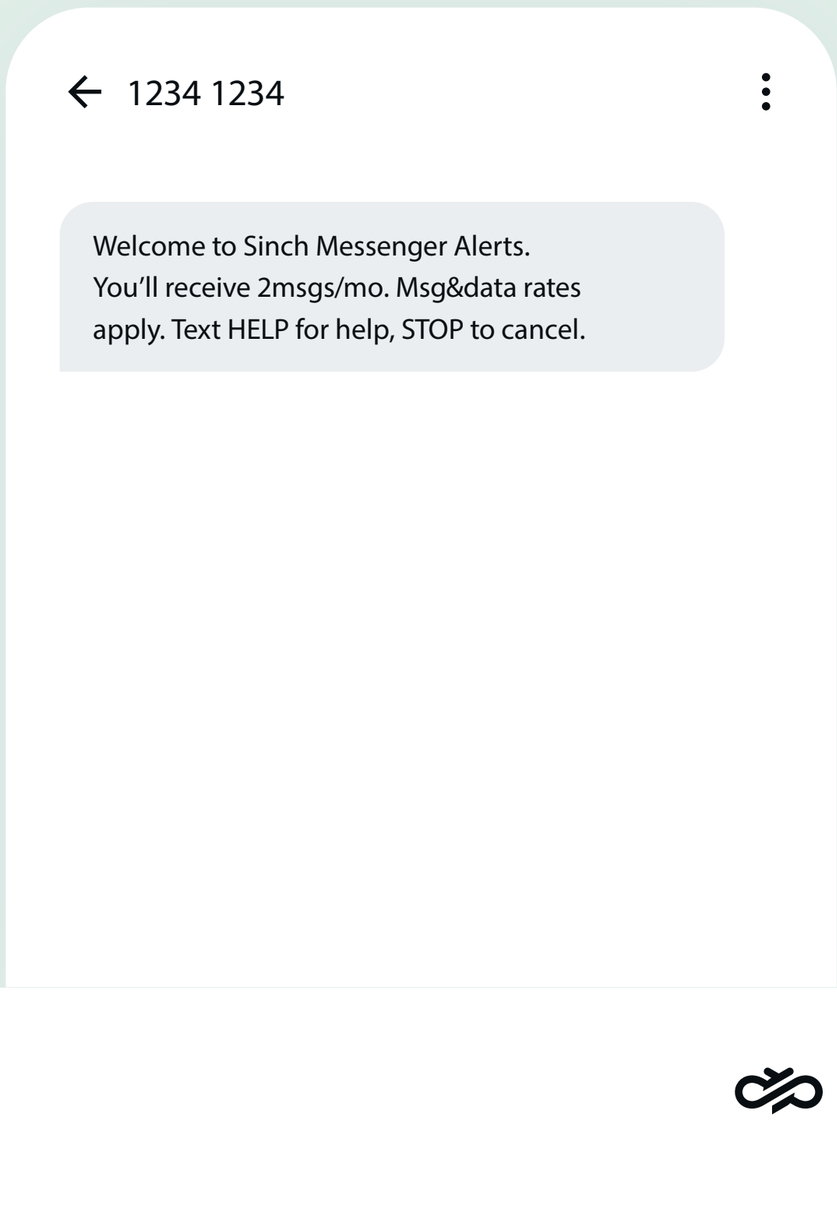
*Opt-out instructions and customer support information may be left out of the CTA if described within the Terms & Conditions, and the terms are properly linked from the CTA.

**Although single-message programs are not required to display HELP and STOP keywords, they should still support HELP and STOP commands.

Confirmation messages

A consumer's opt-in must be confirmed in the first message sent to the consumer for all recurring programs. Brands must state explicitly to which program the consumer enrolled and provide clear opt-out instructions.

Here's an example of a confirmation message a subscriber receives for a recurring program:



Deactivation File compliance

One last thing: Don’t forget to cross-check and clean up your database records against carrier deactivation files.

Let us explain what this is and how it works.

Every day, mobile subscribers switch carriers or deactivate their numbers. Deactivated mobile numbers generally go through a period on each carrier’s network where they’re unassigned, recycled, and then eventually assigned to new subscribers. Any messages sent to these numbers are technically unsolicited, since the opt-in was tied to the original owner. To tackle this, U.S. wireless carriers publish daily a list of deactivated mobile phone numbers for the sole purpose of removing any number found in the list from being messaged.

All messaging clients have access to the carrier deactivation files. U.S. wireless carriers provide these deactivation files to Sinch, and in turn, we make them accessible to you. That way you can maintain your customer lists in line with industry best practices, carrier rules, and legal requirements.

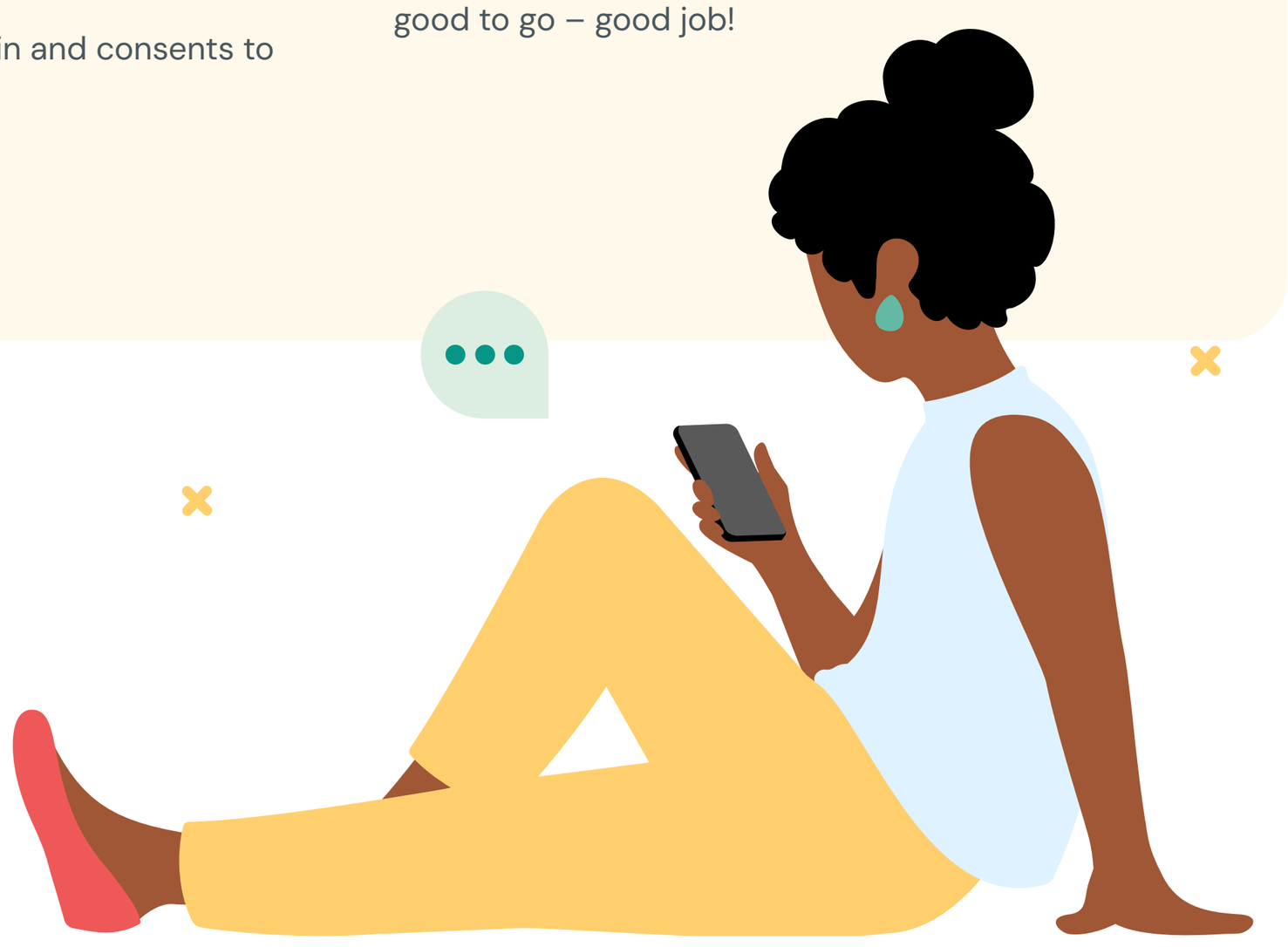
Compliance self-check

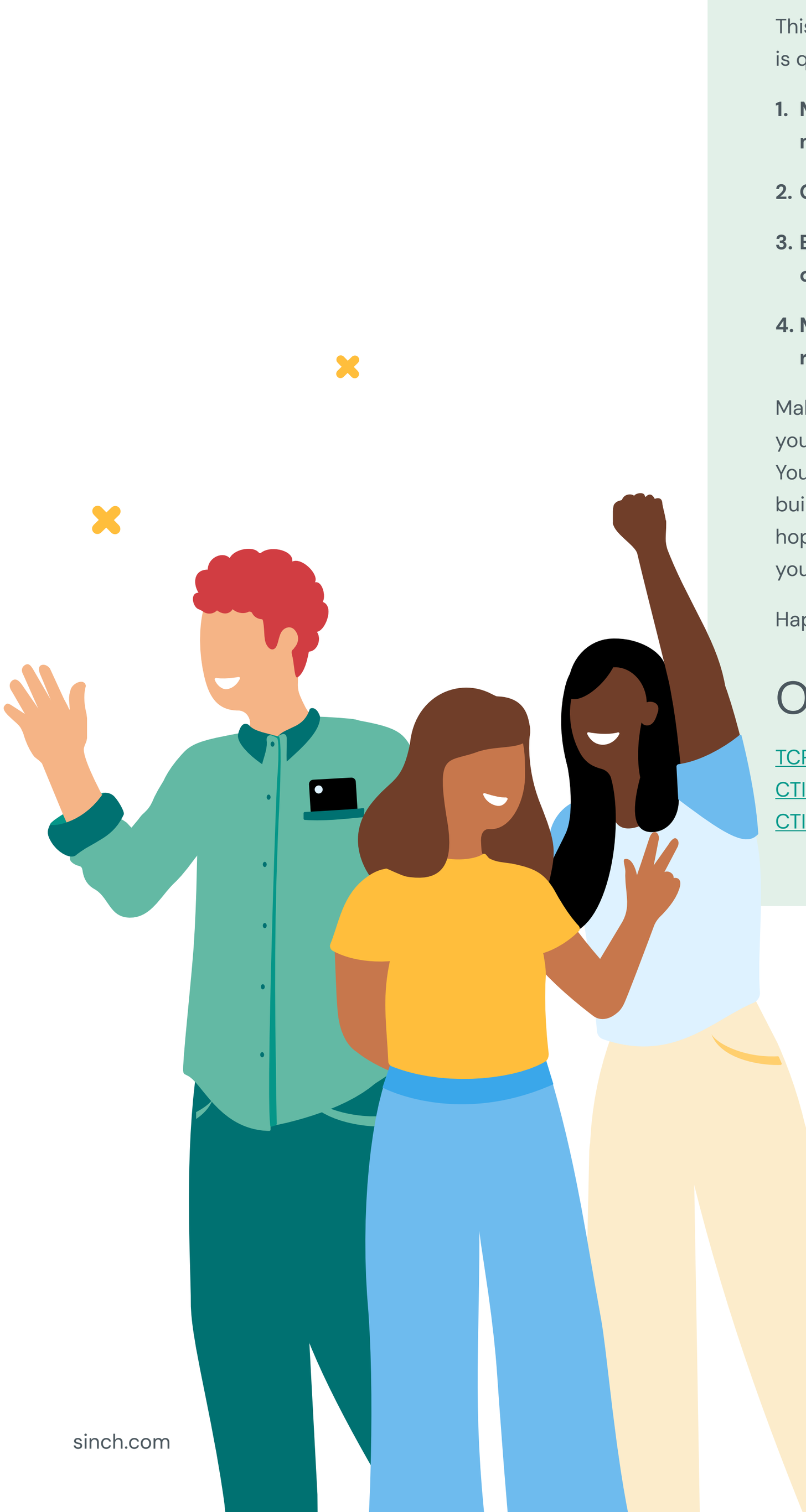
Phew! That's a lot of information, we know. Keep this document on-hand so you can refer back to it – and of course, make sure to always consult with your legal team on how these rules and regulations affect your business specifically.

To summarize, we made a handy little checklist for you to go through before sending any campaign. If you answer "no" to any of the following questions, your campaign is at risk of noncompliance.

- Is your campaign SHAFT-free?
- Do your CTAs display opt-in, opt-out (STOP), and HELP instructions where applicable?
- Did you include a "message and data rates may apply" disclaimer, clear program terms, and privacy policies?
- Did you use a dedicated branded short URL for your TFN and 10DLC campaigns?
- Are all your mobile programs clearly identified?
- Have all your mobile end-users provided express written consent as defined by the CTIA?
- Is it clear that your user opted-in and consents to this specific program?
- Are all your end-users who opt in via web forms put through a double opt-in procedure?
- Are your HELP and STOP, END, CANCEL, QUIT, and UNSUBSCRIBE keywords functioning properly?
- Do you fulfill all opt-out requests within 72 hours of the end-user texting "STOP"?
- Have you implemented Carrier Deactivation Files?
- Have you scrubbed your database on a weekly basis against the Deactivation Files, RND, DNC lists

If you answered "yes" to all these questions, you're good to go – good job!





Conclusion

That’s all for now, folks!

This may seem like a lot to digest, but much of it is quite intuitive:

1. **Make sure you’re sending people messages that they want to get.**
2. **Get consent.**
3. **Be clear with what customers are consenting to.**
4. **Make it easy for them to opt-out and respect their wishes.**

Make the experience easy and positive for your customers. Do that, and everybody wins: You’ll get higher customer engagement and build longer-lasting customer relationships, hopefully resulting in more revenue for your company.

Happy messaging!

Other resources

TCPA
CTIA Short Code Monitoring Handbook
CTIA Messaging Principles and Best Practices