

Text Messaging and TCPA Compliance Statement

Telephone Consumer Protection Act, 47 U.S.C. § 227 — KFRM LLC d/b/a Fundraising University

Effective date: August 4, 2026

Last updated: August 4, 2026

Contents

1. Purpose and overview
2. Two-tier messaging architecture
3. Summary of messaging architecture
4. Consent framework
5. Opt-out mechanisms
6. What Fundraising University does not do
7. Competitive differentiation
8. Technical implementation details
9. Compliance obligations for franchise owners
10. Contact information

Section 1: Purpose and Overview

This document describes how Fundraising University's text messaging practices comply with the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227, and related Federal Communications Commission (FCC) regulations. It is intended for schools, school districts, parents, donors, franchise owners, and any other stakeholders who need to understand how text messages are sent in connection with the Fundraising University platform.

Key takeaway: Fundraising University's platform is designed so that fundraising outreach messages are sent by students from their own personal phones to people they already know. Fundraising University does not send bulk marketing messages, does not use automated telephone dialing systems (ATDS) for fundraising outreach, and does not use corporate shortcodes to contact donors.

Section 2: Two-Tier Messaging Architecture

Fundraising University's platform involves two distinct categories of text messages, each with different technical delivery mechanisms and different TCPA implications. Understanding this two-tier architecture is essential to understanding our compliance posture.

2.1 Tier 1: Peer-to-peer fundraising outreach (native SMS)

What it is: All student-to-donor fundraising messages — including initial outreach, first follow-up, and second follow-up — are sent by the student from their own personal phone using the device's native SMS application.

How it works technically:

1. The student logs into the Fundraising University Student Portal and enters up to 30 donor contacts (friends and family the student personally knows).
2. The student selects a contact and clicks a "Text" button.
3. The platform records the outreach attempt in its database (contact ID, timestamp, message text).
4. The platform then opens the student's native SMS application (for example, iMessage or Android Messages) with the recipient's phone number and a pre-composed message already populated.
5. The student reviews the message in their native SMS app and manually sends it.
6. The message is transmitted through the student's own cellular carrier, from the student's own phone number.

What Fundraising University does NOT do in this flow:

- We do not transmit the message. The student's cellular carrier transmits it.
- We do not use an automated telephone dialing system (ATDS). There is no system that dials or sends messages to a list of numbers automatically.
- We do not use a corporate shortcode or shared sender number. The message comes from the student's personal phone number.
- We do not send automated follow-ups. Each follow-up message requires the student to click the "Text" button again, review the message in their native SMS app, and manually send it.
- We do not queue, batch, or schedule messages for later delivery. Each message is sent individually, in real time, by the student.

TCPA analysis for Tier 1: Because Tier 1 messages are personal, one-to-one communications sent by an individual (the student) from their own phone to people they personally know, using their own cellular carrier, these messages are not subject to the TCPA's restrictions on calls made using an ATDS or prerecorded or artificial voice messages. Fundraising University is not the "caller" or "sender" of these messages within the meaning of the TCPA. The student is the sender. The platform facilitates message composition but does not transmit the message.

2.2 Tier 2: Transactional and system messages (Twilio)

What it is: Fundraising University does send certain text messages through its own infrastructure using Twilio, a third-party SMS delivery service. These messages are transactional or system-generated and are sent in response to specific user actions.

Categories of Tier 2 messages:

- **Student verification and authentication:** SMS codes sent to students during the login and verification process for the Student Portal.
- **Helper invitations:** SMS invitations sent to individuals whom a student has invited to help with their fundraiser, containing an activation link.
- **Fundraising reminders:** SMS reminders sent to students who have explicitly opted in to receive reminders (via the IsOptedIn preference in the Student Portal).
- **Checkout completion links:** SMS messages sent to donors who have initiated a checkout, containing a link to complete their transaction.
- **Keyword-triggered donation links:** SMS replies sent to individuals who text a configured keyword to Fundraising University's Twilio number, providing a link to make a donation.
- **Inbound SMS processing:** Automated replies to inbound text messages received at Fundraising University's Twilio number, based on configured keyword routing.

TCPA analysis for Tier 2: Tier 2 messages fall within established TCPA exemptions and safe harbors:

- Verification and authentication messages are transactional messages initiated by the recipient's own action (attempting to log in) and are not marketing.
- Helper invitations are one-time messages initiated by a student's explicit request, sent to a specific individual the student has identified, and are not marketing.
- Fundraising reminders are sent only to students who have affirmatively opted in via the IsOptedIn preference. These messages go to the student (a known user of the platform), not to third-party donors.
- Checkout completion links are transactional messages initiated by the donor's own action (beginning a checkout), sent to complete a transaction the donor has already started.
- Keyword-triggered messages are initiated by the recipient themselves (they texted the keyword first), constituting express consent to receive a reply.

Section 3: Summary of Messaging Architecture

Table 1: Message types, delivery method, initiating party and TCPA classification

Message type	Delivery method	Initiated by	TCPA classification
Fundraising outreach (initial)	Student's native SMS app	Student (manual send)	Personal communication; FRU is not the sender

Message type	Delivery method	Initiated by	TCPA classification
First follow-up	Student's native SMS app	Student (manual send)	Personal communication; FRU is not the sender
Second follow-up	Student's native SMS app	Student (manual send)	Personal communication; FRU is not the sender
Student verification code	Twilio (FRU infrastructure)	Student (login attempt)	Transactional; initiated by recipient
Helper invitation	Twilio (FRU infrastructure)	Student (explicit request)	One-time transactional; specific recipient
Fundraising reminders	Twilio (FRU infrastructure)	System (opted-in students only)	Consent-based; express opt-in
Checkout completion link	Twilio (FRU infrastructure)	Donor (initiated checkout)	Transactional; initiated by recipient
Keyword donation link	Twilio (FRU infrastructure)	Recipient (texted keyword first)	Recipient-initiated; express consent

Section 4: Consent Framework

4.1 Tier 1 — no TCPA consent required

Tier 1 fundraising outreach messages are personal communications between individuals. The student decides who to contact, composes the message, and sends it from their own phone. Because Fundraising University is not the sender and does not use an ATDS, TCPA consent requirements applicable to commercial callers do not apply to this tier.

Additionally, the nature of the student-donor relationship provides an inherent layer of implicit consent: donors are friends and family members of the student, the student's phone number is typically already saved in the donor's contacts, and the communication is personal in nature.

4.2 Tier 2 — consent mechanisms

For messages sent through Fundraising University's infrastructure (Twilio), consent is obtained as follows:

- **Student verification and authentication:** Consent is implied by the student's act of initiating the login process. The student provides their phone number and requests a verification code.
- **Helper invitations:** The student explicitly requests that an invitation be sent to a specific individual by providing the helper's phone number and name. The helper receives a one-time message.
- **Fundraising reminders:** Students affirmatively opt in to receive reminders during the account setup process via the IsOptedIn preference. Students who do not opt in do not receive reminders. Students can change their opt-in status at any time.

- **Checkout completion links:** The donor initiates the transaction by beginning the checkout process and providing their phone number. The checkout completion message is a transactional communication necessary to complete the donor's own transaction.
- **Keyword-triggered messages:** The recipient initiates the communication by texting a keyword to Fundraising University's number. The act of texting constitutes express consent to receive a reply.

Section 5: Opt-Out Mechanisms

5.1 Tier 1 — opt-out for donor recipients

Because Tier 1 messages are sent from the student's personal phone, donors can opt out by:

- Replying directly to the student (the student's phone number is the sender)
- Contacting the student's parent or school
- Contacting Fundraising University at support@fundraisingu.net to request that their contact information be removed from the student's contact list

Upon receiving such a request, Fundraising University will remove the donor's contact information from the platform.

5.2 Tier 2 — opt-out for system messages

- Students can change their opt-in status for fundraising reminders at any time through the Student Portal.
- Recipients of Twilio-delivered messages can reply STOP to the Twilio number to cease receiving messages from that number, in accordance with Twilio's standard opt-out handling.
- Any individual may contact support@fundraisingu.net to request removal from all Fundraising University communications.

Section 6: What Fundraising University Does Not Do

To provide absolute clarity about our practices, Fundraising University does **not** engage in any of the following:

- Mass marketing or bulk SMS campaigns to donors, prospects, or any third parties
- Use of an automated telephone dialing system (ATDS) to send fundraising messages to donor contacts
- Use of prerecorded or artificial voice messages for fundraising outreach
- Purchase or use of third-party phone number lists for outreach
- Sending unsolicited commercial messages to individuals who have not initiated contact or been individually identified by a student
- Automated sending of follow-up messages without direct student action (each follow-up requires the student to manually initiate and send the message)
- Sharing donor phone numbers with third parties for marketing purposes

- Using corporate shortcodes or shared sender numbers for fundraising outreach

Section 7: Competitive Differentiation

Fundraising University's messaging architecture is fundamentally different from platforms that send automated bulk messages on behalf of organizations. Many fundraising and outreach platforms use ATDS or shortcode-based systems that trigger TCPA compliance obligations. Fundraising University's peer-to-peer model avoids these obligations entirely for fundraising outreach because:

- The student, not Fundraising University, is the sender of fundraising messages.
- Messages are sent from the student's own phone number, which donors already recognize.
- No automated dialing system is used. Each message requires individual, manual action by the student.
- The relationship between the student and the donor is personal and pre-existing.
- Donors can respond directly to the student, creating a genuine two-way personal conversation.

This architecture provides schools, districts, and franchise owners with a significantly lower risk profile compared to competing platforms that rely on corporate messaging infrastructure.

Section 8: Technical Implementation Details

The following technical details are provided for legal counsel, compliance officers, and technical evaluators.

8.1 Native SMS invocation (Tier 1)

The Student Portal is a Blazor WebAssembly application. When a student clicks the "Text" button for a contact, the application calls a JavaScript function (`openSmsApp`) that constructs an SMS URI (the `sms:` protocol) with the recipient's phone number and message body. This URI triggers the device's operating system to open the native SMS application with the fields pre-populated. The student must then manually press "Send" within their native SMS app to transmit the message.

The platform records the outreach attempt (timestamp, message text) in its database **before** the native SMS app is opened. This means the platform's records reflect that an outreach was initiated, but do not guarantee the student actually sent the message (the student may close the SMS app without sending). This is a record-keeping nuance, not a compliance concern.

8.2 Twilio integration (Tier 2)

Tier 2 messages are sent through a communications queue service that calls the Twilio API (`MessageResource.Create`). Messages are sent from a configured Twilio phone number, not from the student's personal number. The Twilio integration handles:

- Outbound message delivery via Twilio's API
- Inbound message receipt and keyword routing via webhook controllers
- Standard opt-out processing (STOP keyword handling) per Twilio's compliance features

8.3 No automated scheduling or batch sending

The platform does not contain any scheduled job, cron task, or background process that automatically sends fundraising messages to donor contacts. Follow-up messages are stored in the database when the student initiates a follow-up, but the actual SMS delivery occurs through the same native SMS app flow as the initial outreach — the student must manually send each follow-up.

Section 9: Compliance Obligations for Franchise Owners

Fundraising University franchise owners should understand the following regarding TCPA compliance in their operations:

9.1 The peer-to-peer messaging architecture described in this document means that franchise owners are **not** sending or authorizing the sending of bulk commercial messages. Students send messages individually from their own phones.

9.2 Franchise owners should ensure that coaches and school staff understand the platform's messaging architecture and can explain it to parents who have questions.

9.3 Franchise owners should **not** instruct coaches or students to use third-party bulk messaging tools, auto-dialers, or any external system to send fundraising messages outside of the Fundraising University platform. Doing so could create TCPA liability that the platform's architecture is specifically designed to avoid.

9.4 If a franchise owner receives a complaint or legal inquiry related to text messaging, they should immediately contact Fundraising University at support@fundraisinguniversity.net.

Section 10: Contact Information

For questions about this TCPA Compliance Statement, about Fundraising University's messaging practices, or to report a concern, please contact:

Fundraising University

KFRM LLC d/b/a Fundraising University

Email: support@fundraisinguniversity.net

Phone: (602) 529-8293

[Privacy Policy, including the COPPA Compliance Statement](#)

[Accessibility Statement and Conformance Report \(ACR/VPAT\)](#)

[Return to the Safety & Compliance Center](#)

Effective August 4, 2026. Last updated August 4, 2026. Published by KFRM LLC d/b/a Fundraising University.

KFRM LLC d/b/a Fundraising University

support@fundraisingu.net · (602) 529-8293

Published at **<https://fundraisingu.net/safety/text-messaging/>**. That page is the authoritative version of this document; where this PDF and the page differ, the page governs.