

Robocall Mitigation Policy
December 20, 2024
On behalf of Cardstock, LLC
Version 1

Objective: Establish and follow a policy that is compliant with TRACED Act

I. Overview

The FCC requires that all providers certify in the Robocall Mitigation Database their status for compliance with STIR/SHAKEN. Those not yet fully compliant must implement and certify to the implementation of a Robocall Mitigation Plan to ensure that this illegal traffic does not originate on their networks as they work within the industry to become fully compliant.

The Commission requires voice service providers to develop a Robocall Mitigation Plan that:

- Details the reasonable steps taken to avoid originating illegal robocalls;
- Demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls; and
- Is filed in the Robocall Mitigation Database

This Robocall Mitigation Plan is submitted on behalf of Cardstock, LLC, a provider of voice and messaging services to K-12 schools in the United States.

All of Cardstock, LLC's customers are public, non-profit schools operating to communicate effectively home to parents and students, and the people initiating calls on Cardstock's platform are all either teachers, administrators, or school-based staff.

II. General Prohibition Against Illegal Robocalling

Cardstock's end user services are subject to restrictions contained in our Terms of Service, including but not limited to its acceptable use policy, which prohibits end users from using its voice (and messaging) services for any illegal use, fraudulent activity, or forgery and impersonation activities. Each customer of Cardstock's platform agrees to its terms of services.

Cardstock users are aware through training and documentation that misuse of its platform may result in suspension or termination of service.

III. Know Your Customer

Cardstock utilizes the mitigation technique of know your customer. Cardstock is a small provider, and we maintain close relations with operational staff at each of our client

schools. Teachers and staff (our end users) are personally onboarded by Cardstock staff at the beginning of each school year, and that training includes information on both legal duties and best practices for using the platform.

In addition, Cardstock uses regular data analysis to review customers for possible misuse of the service, and school administrators also can access data on how their teachers are using (or misusing) the platform.

All schools using Cardstock provide a Tax ID to verify their non-profit status.

IV. Know Your Upstream Provider

Cardstock's current upstream provider for its services is Bandwidth. Cardstock has had a relationship with Bandwidth since 2017, and Bandwidth is a trusted STIR/SHAKEN implementer. As part of Cardstock's relationship with Bandwidth, we are bound by policies and terms of service which include contractual provisions tailored to preventing unlawful robocall activity.

These contract provisions include:

- Prohibitions against unlawful robocalls
- Prohibitions against unlawful, unsolicited, and/or repetitive calls
- Required compliance with FCC STIR/SHAKEN rules
- Identification of unusual call patterns and/or excessive usage

V. Network Monitoring

As noted earlier, Cardstock is a small vendor of voice and messaging services to K-12 public schools. "Know Your Customer" is its primary mitigation technique. In addition, we utilize

- **User Authentication:** Every user with access to the platform has an email address matching the domain of the customer school district.
- **Data Analysis:** Both Cardstock and the administrators of its customer-schools have access to data on individual teacher usage to monitor for effective and legal use of the platform.

VI. Traceback and Enforcement Cooperation

Cardstock will actively cooperate with the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG) to investigate and stop illegal robocalls. Cardstock will dedicate sufficient resources to provide prompt and complete responses to traceback requests within 24 hours in accordance with CFR Section 64.1200(n).