



# SpoofCard

Robocall Mitigation Plan

# S U M M A R Y

This Robocall Mitigation Plan describes the specific measures that SpoofCard LLC (“the Company”) has implemented to detect and prevent illegal robocalls on its network. The Company is fully dedicated to stopping illegal robocalls from originating or terminating on its network. The Company will periodically review and evaluate the effectiveness of its policies and procedures and its capability to support the measures described. The Company will update its Robocall Mitigation Plan as required and upload the revised plan to the database in a timely manner.

The Company offers services that allow consumers to call and text through numbers owned and operated by the Company. These numbers are purchased from various upstream providers for this dedicated use. The Company also allows customers to verify numbers they own and operate to use in conjunction with the service.

# S U M M A R Y

Outbound voice communications initiated from an eligible account via the Company's mobile applications are passed to upstream voice providers, all of whom attest to STIR/SHAKEN integration and/or have a robocall mitigation plan in place. Outbound call initiation occurs via a manual user interface.

The Company certifies that all calls that originate on its network are subject to a robocall mitigation program meeting the requirements specified. Further, the Company certifies that any prior certification has not been removed by Commission action and the Company has not been prohibited from filing in the Robocall Mitigation Database.

## CUSTOMER VETTING PROCESS (KYC)

The Company's customer base is comprised of both individuals and businesses. As such, customer information is collected, such as name, email, phone number, etc. Also collected are meta-data about customers such as IP address, general geo-location, device types, and identifiers, etc. to use to help learn about the customer and to help combat and research fraudulent activities. Where applicable, business entity information, proof of address, and government ID are also collected.

The Company also automatically reviews all purchases made directly through the service platforms and assigns account scores based on multiple pieces of data. Data includes various patterns, credit cards used, IP location, whether their location matches the billing address, etc. If an account is above a specific score threshold, it will automatically be prevented from purchasing and will further be blocked from placing any calls through the service.

These systems are continually refined and improved with data to ensure continued improvement of detection.

# ROBOCALL MITIGATION PROCESS

## Vendor Collaboration with Telecom Trust Center:

- The Company leverages the capabilities of its trusted vendor specializing in real-time phone number intelligence to detect and mitigate fraudulent traffic on the Company's network.
- The Company implements real-time monitoring and analysis of call patterns and behaviors using advanced machine-learning algorithms to identify and block suspicious activities associated with robocalling.

## Upstream Provider Collaboration:

- The Company coordinates with upstream providers to enhance the effectiveness of robocall prevention measures at the network level.
- The Company interfaces with upstream providers to identify emerging robocall trends and deploy proactive mitigation strategies accordingly.

# ROBOCALL MITIGATION PROCESS

## Infrastructure Controls:

- The Company has implemented infrastructure-level controls to limit the number of calls that can be placed per minute per account, effectively reducing the potential for mass robocalling activities.
- The Company utilizes rate-limiting mechanisms to prevent abuse of the communication services and enforce fair usage policies across all accounts.

## DO - NOT - ORIGINATE (DNO) COMPLIANCE

The Company implements a layered Do-Not-Originate (DNO) blocking framework designed to prevent calls from originating with numbers that should never be used as outbound caller ID. This approach combines using Telecom Trust Center's real-time caller ID protection technology alongside our upstream vendor's network-level DNO enforcement. Together, these measures ensure the Company complies with the FCC's December 15, 2025, DNO requirement.

The Company's DNO list includes categories of numbers that should never be used as a caller ID. These include, but are not limited to:

- Numbers publicly identified as belonging to banks and financial institutions
- Government agency numbers
- Law enforcement numbers
- Emergency numbers (such as 911)
- Numbers designated as DNO by our vendor

These numbers are blocked through Telecom Trust Center's internal caller ID verification and other DNO enforcement logic.

# INVESTIGATION

We have not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling.

## TRACEBACK COMPLIANCE

The Company responds to traceback requests from groups such as US Telecom and will respond within 24 hours on business days to any inquiries received from the Industry Traceback Group. The Company leverages call logs, account registration metadata, and other similar sources to quickly take action on relevant accounts. Such action could include customer account suspension and/or termination.

## CONTACT INFORMATION

Abuse Reporting & Traceback Information:

Legal@Spoofcard.com