

Robocall Mitigation Plan for Shield Security, LLC

About Shield Security, LLC:

Shield Security, LLC ("Shield Security") is a publisher of mobile applications that, among other functions, enable end-users to communicate via SWS and voice. Inbound and outbound voice implementations are provided to Shield Security by underlying vendors that have substantially implemented STIR/SHAKEN across their networks and sign calls made on behalf of Shield Security. Shield Security does not provide direct access to any underlying voice infrastructure via API or any other mechanism.

STIR/SHAKEN Implementation Status:

Shield Security has not directly implemented STIR/SHAKEN because it is not eligible to obtain an Operating Company Number ("OCN"). As a result, Shield Security is unable to obtain a Service Provider Code (SPC) token under the STI Governance Authority's revised SPC Token Access Policy and is eligible for an extension from STIR/SHAKEN implementation obligations until such time as Shield Security becomes eligible for an SPC Token. As noted above, Shield Security relies on its underlying vendors that have substantially implemented STIR/SHAKEN to sign calls originated on behalf of Shield Security customers.

Shield Security protects against robocalls within its own infrastructure with the following safeguards

Know Your Customer Measures:

Shield Security takes substantial measures to ensure the identity of its customers and prevent use of the service by customers for the origination of robocalls.

Prior to initiating service, all Shield Security end users must have their accounts directly linked to (1) a verified phone number or (2) a verified email address. The phone number must be from a vetted carrier with a certificate in the Robocall Mitigation Database. In addition, Shield Security conducts reputation checks on each prospective consumer Shield Security end user to ensure the user has not previously violated Shield Security's Terms of Service. All customers who create an account must agree to Terms of Service whereupon they agree to and understand the terms that apply to use Shield Security's voice and messaging services. The Terms of Service require customers to agree to provide and maintain true, accurate, current and complete information as necessary. In addition, customers must either be the owner of the voice and/or data plan for the mobile device on which Shield Security's services will be used or have authorization and consent from the device owner to use services on the mobile device.

The Terms of Service prohibits the use of the service for illegal purposes, which prohibited users include transmission of unsolicited or unauthorized advertising, promotional materials, commercial activities and/or sales, “junk mail”, “spam”, “chain letters”, “pyramid schemes”, “contents”, “sweepstakes”, or any other form of solicitation. Shield Security also reserves the right to restrict use of the service where such use may expose Shield Security to liability of any type. The Terms of Service also prohibit the use of the services to violate any applicable local, state, national, or international law, any regulations having the force of law, and use for high volume or multi-person calling purposes. Customers who become aware of a prohibited use of the service must immediately notify Shield Security and provide reasonable assistance in any resulting investigation.

Shield Security reserves certain rights through its Terms of Service to ensure that the service is not used for prohibited purposes. For example, Shield Security is permitted to monitor the use of the service to ensure compliance with applicable laws and to ensure customer compliance with the Terms of Service. Shield Security may discontinue (temporarily or permanently) the service with or without notice to the customer and may block access to the service. Shield Security reserves the right to refer to appropriate law enforcement any suspected fraudulent, abusive, or illegal activity through the service.

Know Your Upstream Provider Measures:

Other than its end user customers, Shield Security does not receive voice traffic from any other party. All outbound voice communications initiated from an eligible account via Shield Security mobile applications are passed to other voice providers, all of who attest to outbound calls using STIR/SHAKEN. Outbound call initiation occurs via a manual user interface; no volume dialing, robo-dialing, or other automation is possible.

Traffic Monitoring and Mitigation Measures:

Consistent with its Terms of Service, Shield Security’s systems monitor for users/accounts that exhibit abusive behavior (e.g., frequency of calls per period of time, use of multiple devices on the same account simultaneously, minutes used per period of time, called destinations per period of time, specific dialing patterns, etc.) and if any accounts are deemed abusive, they are automatically blocked by Shield Security’s telephony platform and the accounts suspended.

Inbound voice communication is screened against a list of known robocallers and blocked upon matching against our internal list that is updated over time.

In addition to its own traffic monitoring and mitigation efforts, Shield Security relies on the analytics, monitoring, and mitigation measures adopted by its underlying providers to identify and address suspected robocalls that originate by Shield Security customers.

Traceback Commitments:

In the event of a traceback request from the Commission, law enforcement, or the traceback consortium, Shield Security will respond within 24 hours and will fully cooperate to help investigate and stop any illegal robocallers that originate calls from our service.

Enforcement Matters:

In the most recent two-year period, none of Shield Security or any entity with Shield Security shares common ownership, management, directors, or control, has been the subject of a formal investigation or action regarding actual or suspected wrongdoing due to facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database filing or mitigation program description.