



Robocall Mitigation Plan

DigiClick provides cloud hosted PBX services to small to medium customers. We connect these customers to the Public Switched Telephone System (PSTS) using two carriers ([REDACTED] and [REDACTED]). Both carriers provide STIR/SHAKEN services as described below. These two carriers are the only routes in from or out to the PSTN. Our customers do not have access to modify any connections to either [REDACTED] or [REDACTED]. In addition, they are unable to add any third-party carriers.

This document outlines a set of robocall mitigation rules that will ensure compliance with the STIR/SHAKEN framework to combat unwanted robocalls and protect our customers. By implementing these rules, our company will maintain the highest level of security and transparency for our customers and stakeholders.

- A. To ensure compliance with the STIR/SHAKEN framework, DigiClick Corp. has implemented the following robocall mitigation rules:

Regarding [REDACTED]:

Outbound IP-based calls from [REDACTED] customers using [REDACTED] U.S. phone numbers are signed with "A" or full attestation.

Outbound IP-based calls from [REDACTED] customers using non-[REDACTED] U.S. phone numbers are signed with "B" or partial attestation.

Any IP-based calls from [REDACTED] wholesale customers without STIR/SHAKEN ID Header information are signed with "C" or gateway attestation.

U.S. Origination customers can enable our Inbound Verification Service in the [REDACTED] App. This feature provides STIR/SHAKEN verification results to service providers in order to make decisions to either block calls or terminate them to the end user.

Features, like call forwarding or the ability to ring multiple devices simultaneously, change the destination called number and break the STIR/SHAKEN authentication process. The ATIS standard for "div" PASSporT allows service providers to confirm whether a call has been legitimately retargeted.

[REDACTED] is committed to implementing additional STIR/SHAKEN standards as they emerge.

Regarding [REDACTED]:

Inbound calls

[REDACTED] provides inbound calls to customers both of the following STIR/SHAKEN-based insights:

TN validation info via the 'verstat' tel URI, a parameter in either the P-Asserted Identity (PAI) header field or the FROM header field. This parameter will contain one of the following 3 values denoting the result of a TN validation check:

TN-Validation-Passed

TN-Validation-Failed

No-TN-Validation

If we get a "TN-Validation-Passed" result in the verstat, we will prepend "[V]" to the CNAM, right-truncating CNAM if the addition of "[V]" causes the 15-character limit to be exceeded.

For calls that have the above-mentioned verstat result, we're also putting logic in place that will overwrite any CNAM content that originating networks or customer's PBX would supply, so that the prepended [V] doesn't inadvertently communicate invalid/nefarious CNAM content.

Finally, if the CNAM content from our content provider is either blank or the response is NULL, the CNAM will simply be "[V]"

All other calls will have normal CNAM treatment.

Additional comments regarding inbound calls:

We do not block inbound traffic based on STIR/SHAKEN verification results.

The spirit of offering both (1) and (2) together is to allow customers who can handle/parse SIP headers to apply their own treatment if they so choose, while also providing for others who cannot; the CNAM-based approach solves for a large variety of end-customer-device restrictions without the need for service providers to individually do so.

Outbound calls

For outbound calls from customers, generally speaking,

Calls from TNs that a customer purchased from [REDACTED], and are associated with that specific customer's [REDACTED] account, should get attestation A.

Calls from TNs other than those that a customer purchased from [REDACTED] should get attestation B.

Calls from a customer whose [REDACTED] account is in 'Pending' status will get attestation C.

Calls from toll-free numbers not hosted on [REDACTED], invalid TNs (invalid per North American Numbering Plan) or with caller ID "Anonymous" will get attestation C.

We pass through unaltered, any attestation we receive on calls arriving at [REDACTED].

B. Summary of Steps we take to mitigate Robocalls

- I. We use origination and termination services provided by [REDACTED] and [REDACTED] to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls. All have implemented STIR/SHAKEN within their IP network.
- II. We do not accept any auto-dialed traffic.
- III. We restrict the rate at which a customer can initiate calls.
- IV. We place explicit limits on the number of calls per second (CPS) the customer can initiate.

- V. We routinely audit call records to ensure that no auto-dialed traffic has infiltrated what is expected to be conversational calling.
- VI. DigiClick utilizes the mitigation technique of “Know Your Customer.” We are a small, long-established provider that maintains a close relationship with its subscribers.
 - a. Businesses requesting large volume calling capability must provide a tax ID and verification as to the nature of the business.
 - b. A DigiClick representative may visit the premises of the business to verify the number of users at the location is appropriate for the volume of calling.
 - c. We require a thorough list of items examined to vet customer legitimacy (web site, references, social media, regulatory and state filings, physical address, business purpose, description of traffic).
- VII. We do not allow customers to access or modify the PBX connections to the PSTN.
- VIII. We have implemented Caller ID Name Service. An easy integration of Caller ID name lookup service.
 - a. We require that the caller-ID value be a number assigned to the calling party only.
 - b. Caller-ID is constrained appropriately; specific values verified and white-listed to ensure customer is using only values assigned to them or used with express permission.
- IX. We will provide a point-of-contact for traceback and takedown requests from bona fide sources. For credible requests that include sufficient supporting detail, we will not require a subpoena or similar documentation.
- X. We will insist that our service provider partners implement these same practices and impose this same requirement on their partners, or face restrictions on their use of our platform (including, if necessary, complete loss of access).
- XI. We apply a finite dollar credit to a customer account. If the customer exceeds that number, the customer is blocked from making outgoing calls.
- XII. We provide our customers with call blocking tools to stop unwanted and/or illegal calls. These tools give them the ability to send calls directly to voicemail or deny the call entirely from reaching their phones.

C. Monitoring and Compliance

By adhering to these robocall mitigation rules and maintaining STIR/SHAKEN compliance, DigiClick Corp. can protect our customers from unwanted robocalls and preserve the integrity of our communications network.

- I. Our company will continuously monitor our compliance with the STIR/SHAKEN framework and these robocall mitigation rules. We will also regularly review and update these rules to ensure that they remain effective and aligned with industry best practices.

D. Traceback and Enforcement Cooperation

- I. DigiClick Corp. will actively cooperate with the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG) to investigate and stop illegal robocalls. DigiClick will dedicate sufficient resources to provide prompt and complete responses to traceback requests.
- II. If we discover that traffic originally flagged as illegal is in fact legitimate, we immediately suspend service and share that information with the proper authorities.
- III. We respond to all traceback requests within 24 hours from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.