

(1) Meeting existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls

All outbound traffic from customers originates from notification application systems. We do not offer general outbound dialing, end user telephone service, or trunking for any other purpose.

All outbound traffic is only allowed to be terminated to the PSTN if the destination TN is registered in our application. Customers are unable to use outbound services for any TN that has not been registered to a user. Customers are not allowed, and do not have access, to use SIP trunking service for any other application, end user, or trunking purpose.

All outbound traffic originates from, and complies with STIR/SHAKEN protocols, using an original TN provided by upstream carrier. CID/TN manipulation is not implemented, offered, or allowed for any outbound traffic.

All outbound calls are sent to upstream provider, and therefor to the PSTN, in STIR/SHAKEN compliant methods.

All new, existing, renewing, and non-renewing customers are not able or allowed to originate any general, or non-application based, outbound traffic. All outbound traffic generated by customers is only for legitimate notification purposes.

All new, existing, renewing, and non-renewing customers are screened for legitimate outbound traffic uses before service activation and during use of outbound services. All customers are bound by contractual agreements to use outbound services only for legitimate traffic and use cases.

All new, existing, renewing, and non-renewing customers outbound origination services can be blocked by provider and/or upstream provider in the event of illegitimate use of outbound services.

All non-renewing, terminated, or suspended customer outbound services are immediately deprovisioned or restricted following either a suspension or termination event.

All calls that are originated by customers are from notification applications only. We do not trunk, provide gateway services, handle, or forward any outbound traffic from any other sources, carriers, providers, third parties, customers, or end users to the PSTN.

All customers; new, existing, renewing, and non-renewing, are bound contractually to the above requirements and restrictions for outbound traffic.

(2) “Know-your-upstream provider” procedures

All calls are sent via SIP trunking service from Bandwidth LLC., Bandwidth has deployed several layers of call validation and STIR/SHAKEN services across their network. All calls sent to Bandwidth to be routed to the PSTN are complaint, and use native DID/TN outbound CID. We do not offer or implement caller ID manipulation on any call or trunk. All calls sent to upstream provider utilize CID and STIR/SHAKEN protocols on the original trunk DID furnished by upstream provider only. Our upstream provider requires we comply with, and only route traffic that is, STIR/SHAKEN compliant. We have several contractual obligations with our upstream provider that requires us to fully participate in and support STIR/SHAKEN compliance, in addition to agreements that require us to only use upstream services for legitimate traffic. Upstream Provider reserves the right to block outbound traffic originating from our network if we violate agreements, or send illegitimate traffic to upstream provider. We do not interconnect with any carriers, or use other upstream carriers.

(3) Describe any call analytics systems to identify and block illegal traffic

All outgoing calls are authenticated by our application before any outbound call is allowed to dial. Outbound calls are only allowed to be placed to telephone numbers that are registered in our database, we do not offer any outbound dialing to non-registered telephone numbers. All outbound calls originate from our applications, and we do not offer end user telephone services. All calls are logged internally and compared with our upstream provider's (Bandwidth) CDRs to verify all traffic is legitimate.

Since we do offer end user telephone services and only allow outbound calling from a single notification application, all terminated outbound calls are legitimate traffic. No end users, customers, or third-party services/carriers are allowed to use outbound calling for any other calling/trunking purpose. Customer trunks are rate limited and sized in terms of trunk capacity, call requests per minute, and regional calling capabilities to the minimal requirement of the customer notification system. Customers do not have unlimited access to concurrent channels, call requests, or calling plans.

All unrecognized outbound traffic will not be sent to upstream providers, as we do not play an intermediary in any call chain for other end user, customer, third party, or carrier. Our network does not allow for outbound origination to the PSTN from any other end user, customer, third party, or carrier.

All suspicious or misuse of outbound services by customer notification system will be blocked on the application layer before outbound origination occurs to upstream provider and therefor the PSTN. Any outbound event that violates outbound origination enforcement rules will be denied origination. Verification services are implemented to identify call legitimacy before origination. Additionally, any outbound services that violate established rate limit parameters, or fail verification, are denied outbound origination. All active call session, channels, and call requests are monitored concurrently and in the highly unlikely event of abnormal traffic-outbound requests are blocked, and services are rate limited further.