



Robocall Mitigation Plan for Vxt Communications Ltd

VXT is a phone system built specifically for professional services firms. We provide software for placing and receiving phone calls that integrates with other software used by professional services firms to help them save time on administrative tasks associated with communications with their clients.

As we exclusively offer our services to businesses, we implement a stringent manual onboarding screening and due diligence process for all new customers. However, our commitment to preventing illegal robocalling extends further, as we routinely use both automated and manual checks to detect suspicious activity and avoid facilitating illegitimate traffic.

Our upstream provider in the United States is Bandwidth Inc., which is itself registered in the Robocall Mitigation Database (RMD), with registration number RMD0002564. Through our partnership with Bandwidth Inc., all calls we originate are signed with full ("A") STIR/SHAKEN attestation.

Our overall approach to robocall mitigation can be roughly divided into two key strategies: Prevention and Monitoring. These strategies are described further below.

Prevention

Businesses that sign up to use our services must verify their email address and submit proof of address documentation as part of the in-app setup process.

Their registration then goes through a manual onboarding screening and due diligence process before they can begin using our services. During this process, our screening team checks the proof of address documentation against the customer's public business records, as well as against information published on the customer's official website to ensure consistency. Our team additionally checks that the domain name of the customer's verified email address matches their official website to ensure the applicant is an authorized representative.

Should our team be unsatisfied that a prospective customer is legitimate during this screening process, we do not approve them to start using our services, and blacklist them from signing up again in the future.

Monitoring

We have our own call analytics system, which tracks a wide range of metrics including call volume, direction, answer rate, and call time across all users. We routinely use both automated and manual monitoring of these metrics to flag and investigate potentially suspicious activity.

If illegitimate activity is identified, we immediately disable the account, including blocking any associated payment methods from ever being used for our services again (even under a different business name), immediately revoking access to calling services, and deleting the account.

We are prepared to respond without delay to traceback requests from the relevant authorities, where we will investigate reports of illegal robocallers.

In addition to our own analytics and monitoring systems, our upstream provider (Bandwidth Inc.) also has call analytics monitoring systems in place for the detection of illegitimate traffic, as described in their RMD registration (RMD0002564). Should they detect suspicious activity, we can work directly with them to identify the corresponding account on our end and follow the same process to terminate and block the account.