

Robocall Mitigation Plan for PocketSuite, Inc.

About PocketSuite, Inc.:

PocketSuite, Inc. ("PocketSuite") is a publisher of mobile applications that, among other functions, enable end-users to communicate via SMS and voice. In- and out-bound voice implementations are provided to PocketSuite by underlying vendors that have substantially implemented STIR/SHAKEN across their networks and sign calls made on behalf of Ad Hoc Labs customers. PocketSuite does not provide direct access to any underlying voice infrastructure via API or any other mechanism.

STIR/SHAKEN Implementation Status:

PocketSuite has not directly implemented STIR/SHAKEN because it is not eligible to obtain an Operating Company Number ("OCN"). As a result, PocketSuite 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 PocketSuite becomes eligible for an SPC Token. As noted above, PocketSuite

¹

relies on its underlying vendors that have substantially implemented STIR/SHAKEN to sign calls originated on behalf of PocketSuite customers.

PocketSuite protects against robocalls within its own infrastructure with the following Safeguards.

Know Your Customer Measures:

PocketSuite 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 PocketSuite end users must have their accounts directly linked to (1) a verified phone number or (2) a verified Google, Apple, or Facebook account via a single sign-on process. All customers who create an account must agree to Terms of Service whereupon they agree to and understand the terms that apply to use of PocketSuite' voice and messaging services. The Terms of Service require customers to agree to provide and maintain true, accurate, current and complete information about the customer as required by the registration form, and to update the information as necessary. In addition, customers must either be the owner of the voice and/or data plan for the mobile device on which PocketSuite' services will be used or have authorization and consent from the device owner to use the services on the mobile device.

The Terms of Service prohibits use of the service for illegal purposes, which prohibited uses include transmission of unsolicited or unauthorized advertising, promotional materials, commercial activities and/or sales, "junk mail," "spam," "chain letters," "pyramid schemes,"

See 47 C.F.R. § 64.6304(b) ("Voice service providers that are incapable of obtaining an SPC token due to

¹

Governance Authority policy are exempt from the requirements of § 64.6301 until they are capable of obtaining a SPC token." "contests," "sweepstakes," or any other form of solicitation. PocketSuite also reserves the right to restrict use of the service where such use may expose PocketSuite 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, caller ID spoofing, use for high volume or multi-person calling purposes, and attempts to mislead others as to the identity of the sender or origin of any communication made using the service. Customers who become aware of a prohibited use of the service must immediately notify PocketSuite and provide reasonable assistance in any resulting investigation.

PocketSuite reserves certain rights through its Terms of Service to ensure that the service is not used for prohibited purposes. For example, PocketSuite 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. PocketSuite may discontinue (temporarily or permanently) the service with or without notice to the customer and may block access to the service. Ad Hoc Labs 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, PocketSuite does not receive voice traffic from any other party. PocketSuite uses only two underlying suppliers of telephone numbers to provide its voice services. All outbound voice communications initiated from an eligible account via Ad Hoc Labs mobile applications are passed to other voice providers, all of whom 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, PocketSuite 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 the PocketSuite telephony platform and the accounts suspended. Inbound voice communication is screened against a list of known robocallers and blocked upon matching against a commercially available list that is updated in real time. In addition to its own traffic monitoring and mitigation efforts, PocketSuite relies on the analytics, monitoring, and mitigation measures adopted by its underlying providers to identify and address suspected robocalls that originate by PocketSuite customers.

Traceback Commitments:

In the event of a traceback request from the Commission, law enforcement, or the traceback consortium, PocketSuite, Inc. 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 PocketSuite or any entity with which Ad Hoc Labs 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.