

4T'S Computers Inc

Robocall Mitigation Plan

1. Is your Company a voice service provider (including a foreign voice service provider), as defined in §64.6300(l), and/or an intermediate provider as defined in §64.1600(i) of the FCC rules? (The type of provider is determined on a call-by-call basis, so your company could be both a voice service provider and an intermediate provider.)

Yes ☒ No ☐

If no, skip remaining questions; the Company is not required to implement STIR/SHAKEN, no Robocall Mitigation Plan is required, and the Company does not need to register in the FCC's Robocall Mitigation Database ("RMD").

If yes, and the Company is an intermediate provider only, it must fully implement STIR/SHAKEN in its IP network. As long as the Company is registered in the FCC's Intermediate Provider Registry, it will be automatically registered in the Robocall Mitigation Database and is not required to enter any additional information in the database.

2. Does the Company lack control of the network infrastructure necessary to implement STIR/SHAKEN (e.g., the Company operates as a pure reseller without any switching facilities)?

Yes ☒ No ☐

*If yes, the Company is not required to implement STIR/SHAKEN, but by June 30, 2021 it must register in the FCC's Robocall Mitigation Database and submit a Robocall Mitigation Plan. Skip to **Robocall Mitigation Plan Development**.*

3. Has the Company fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with §64.6301(a)(1) and (2)?

Yes ☐ No ☐

If yes, and the Company does not have non-IP network, the Company is not required to submit a Robocall Mitigation Plan. However, by June 30, 2021, it must register and certify in the FCC's Robocall Mitigation Database that it has fully implemented STIR/SHAKEN. (Skip remaining questions.)

4. Has the Company implemented the STIR/SHAKEN authentication framework on a portion of its network and the calls it originates on that portion of its network are compliance with §64.6301(a)(1) and (2) or not implemented on any portion of its network?

Partially implemented _____ Not implemented _____

By June 30, 2021, the Company must register in the FCC's Robocall Mitigation Database and upload a Robocall Mitigation Plan for the remainder of the calls that originate on its network.

5. Is the Company eligible for an extension of the June 30, 2021 STIR/SHAKEN implementation deadline under any of the following exemption criteria (§64.6304):

a) Company is a small voice service provider (a provider that has 100,000 or fewer voice service subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the provider's affiliates)?

Yes _____ No _____

b) Company is a voice service provider that cannot obtain a SPC token?

Yes _____ No _____

c) Company has services that are scheduled for section 214 discontinuance, filed as of June

30, 2021?

Yes _____ No _____

d) Portions of the Company's network are non-IP and rely on technology that cannot initiate, maintain, and terminate SIP calls; and the Company filed a certification with the FCC by December 1, 2020 that, for those portions of its network, it has taken reasonable measures to implement an effective call authentication framework, consistent with §64.6306 (b)?

Yes _____ No _____

If yes to any subpart above, by June 30, 2021 the Company must register in the FCC's Robocall Mitigation Database and upload a Robocall Mitigation Plan.

Robocall Mitigation Plan Development

Responding to Traceback requests:

1. Identify and provide contact information for the Company's point of contact to handle

traceback requests.

Name Title Contact Info

Joseph Shaffer Owner joseph@4ts.net

2. Describe the process the Company has in place to respond to traceback requests from the Industry Traceback Group, the FCC and law enforcement, including the specific tools it can use to conduct investigations of suspected illegal robocalls (e.g., call logs, Metaswitch call history) and the criteria that it intends to use to determine if the calls are actually illegal.

4T'S Computers has designated Joseph Shaffer to be the compliance officer. If a traceback request is made, He will engage with SkySwitch to gather all call details and notify the implicated customer and request corrective actions. Call logs, CDR and call history will be pulled for the client and provided to authorities as needed. We would review the caller IDs, dialed numbers and call patterns. We would look at the following criteria to determine if the calls are illegal. Non-compliance with the FCC regulations and Traced Act, High-volume, repetitive dialing patterns, Failure to authenticate caller ID (STIR/SHAKEN). We would enforce the following if calls are determined to be illegal. Suspend or terminate the offending accounts, Report the violators to authorities and block flagged numbers from our network.

Customer Vetting:

3. What process does the Company use to vet the identity of its retail and wholesale subscribers in order to determine the subscriber's identity and operational legitimacy (See *Best Practices*, pp. 6-11)? Examples of information that might be used to vet a business subscriber's identity include physical business location, contact person(s), state or country of incorporation, federal tax ID and the nature of the customer's business.

Before signing a customer, we receive a list of telephone numbers for the company, their physical address, e-mail address and the company representative's contact information. We also meet with them to evaluate their current network and phone system and specific needs.

Telephone Number Validation:

4. What process does the Company use to confirm an end user's right to use a telephone number?

Does the Company intend to use a third-party validation service for this purpose? (See *Best*

Practices, pp. 13-14.)

We request a recent copy of the clients telephone bill and CSR to verify the phone numbers currently in their account.

International Call Originators:

5. Does the Company sell services to international call originators using North American Numbering Plan Numbers?

Yes _____ No X

If yes, what process does the Company use to validate that the calling party is authorized to use

the telephone number or caller identity? (See *Best Practices*, p. 14-16.)

Other Robocall Mitigation Practices:

6. What other ongoing robocall mitigation practices has the Company put in place on its IP and non-IP networks for the purpose of detecting illegal robocalls? For instance, does the Company use call analytics and other tools to detect potentially illegal robocalls originating from its customers or the customer of its resellers?

We rely on our underlying carrier, SkySwitch to detect illegal robocalls originating from one of our customers telephone numbers.

7. If the Company determines that traffic is illegal, describe the steps the Company will take to mitigate that traffic. E.g., does it incorporate terms in customer contracts to allow it to suspend or terminate service to a customer suspected of generating illegal calls?

We would notify SkySwitch to restrict / suspend service on those telephone numbers being used for robocalling. We have a stipulation in our contract that our voice service cannot be used for any illegal activity or else it will be suspended.

Call Blocking:

8. What process will the Company use to determine that certain traffic should be blocked?

We will rely on authorities, our clients or SkySwitch to determine if a number should be blocked.

9. Does the Company have a process in place to block calls coming from companies not registered in the Robocall Mitigation Database by September 28, 2021? Describe how the Company will monitor the RMD to comply with that requirement.

We do not offer telephone service to resellers / wholesalers, so this would not apply.

STIR/SHAKEN Implementation:

10. Is the Company working to implement STIR/SHAKEN authentication of calls originating on its network? Describe the Company's efforts and timeline.

As a switchless reseller of voice services, we have no control over the network operations and cannot implement STIR/SHAKEN authentication. This is being handled by our underlying carrier, SkySwitch.