

Creative Computer Communications, LLC

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 - Contact Info

Roger Vanderslice - jason@creativecomputers.com

Bobby Watts - bo@creativecomputers.com

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.

We will contact our network provider to secure whatever information is requested and will notify them to do whatever the authorities would ask us to do. We would also contact our end user to take whatever action authorities asked us to take.

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.

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 receive a copy of the customer's Customer Service Record or telephone bill which lists the telephone numbers on their account when a company signs up with us.

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 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 our provider to restrict / suspend service on those telephone numbers being used for robocalling. We do 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 and / or our provider to make that determination.

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 are not capable of implementing STIR/SHAKEN authentication. This is being handled by our underlying carrier.