

**STX Group, LLC d/b/a Twigby Mobile
Robocall Mitigation Certification and Plan**

STX Group, LLC, d/b/a Twigby d/b/a Silvercell Wireless ("Twigby or Silvercell or "the Company"), a voice service provider, submits this robocall mitigation certification and attached Robocall Mitigation Plan pursuant to section 64.6305 of the Federal Communications Commission's ("FCC's" or "Commission's") rules.

STIR/SHAKEN

The Company is a voice service provider without a STIR/SHAKEN obligation serving end-users. Cellco Partners ("Verizon") is the Company's underlying voice service provider. The Company relies on procedures, policies, and safeguards implemented by Verizon to ensure that the Company's residential and business customers are sufficiently protected against robocall and spoofing activities.

ENFORCEMENT

All voice traffic that originates on our network is subject to the attached Robocall Mitigation Plan.

The Company and/or any entity for which the filing entity shares common ownership, management, directors, or control have never been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program.

The Company has not been prohibited by the Commission from filing in the Robocall Mitigation Database.

TRACEBACK

The Company commits to cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any robocallers that use our service to originate unlawful robocalls. The Company will respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use our service to carry, process, or originate robocalls.

IDENTIFYING AND OTHER INFORMATION

- Primary address of the provider: 1418 Kensington Square Ct Bldg D, Murfreesboro TN 37130
- Other business names in use by the provider: Twigby and Silvercell Wireless (consumer products)
- All business names previously used by the provider: N/A
- Twigby is not a foreign voice service provider. Only Serve US as an Illinois LLC
- OCN: N/A, Verizon provides all MDNs
- Person within the company responsible for addressing robocall mitigation-related issues: Jason Narrell, CFO, 1418 Kensington Sq CT Bldg D Murfreesboro TN, 37130 jason.narrell@twigby.com ,405 209 8094

I, Jason Narrell, for STX Group, LLC, submit this certification on behalf of the Company, which has implemented the STIR/SHAKEN authentication framework as indicated in the Robocall Mitigation Database. Pursuant to section 1.16 of the FCC's rules, I certify, under penalty of perjury, that the information and statements contained herein are true and correct to the best of my knowledge and belief.

Jason Narrell sign/date 2-25-26

Robocall Mitigation Plan

Twigby has taken specific reasonable steps, as set forth below, to avoid originating and processing illegal robocall traffic.

The Company relies exclusively on Verizon as its voice service provider and procedures, policies, and safeguards implemented by Verizon to ensure that Twigby's customers are sufficiently protected against robocall and spoofing activities.

The Company relies on Verizon's call analytics to monitor call traffic and does not utilize any other third-party analytics. In its Robocall Mitigation plan, Verizon states that it adheres to Anti-Robocall Principles published by state attorney's general. In its Robocall Mitigation filing Verizon states,

[it] has heightened procedures to monitor outbound traffic in order to identify potentially illegal robocalls and take action when we do. That monitoring includes automatically generating reports that include metrics such as call volumes, SIP response codes, answer rates, call duration, honeypot hits, Industry Traceback Group traceback volumes, "neighbor" spoofing calling patterns, and calls that trigger crowd-sourced complaints. We have developed methodologies for synthesizing various data points in order to create a single "roboscore" that can be used to identify potentially problematic traffic." Verizon has responsibility to address reasonable corrective actions when monitoring activity identifies potential fraud, which Verizon describes as taking, "appropriate action to curb the behavior, including submission of tracebacks, termination of the customer relationship and referrals to law enforcement...and to the extent a Verizon retail customer's traffic has characteristics consistent with illegal robocalling, Verizon analysts and attorneys who are experts in the Telephone Consumer Protection Act and other anti-robocalling laws review the traffic to ascertain if it may potentially be illegal and take action accordingly.

The Company has not received information suggesting that robocalls are likely to originate on our network. Therefore, we do not consider our network at high risk of originating illegal robocalls.

Our Terms and Conditions prohibit unlawful, fraudulent, or harmful use of our network/services. To the extent that a customer or someone else violates our Terms and Conditions, service may be cancelled, disabled, or discontinued.

Know-Your-Upstream Provider Processes.

Twigby relies on Verizon's know-your-upstream provider processes. Twigby verified that Verizon has registered in the Robocall Mitigation Database.

In its Robocall Mitigation Plan, Verizon states that it follows procedures for ensuring it knows the identities of all upstream carriers from which it accepts traffic.

For any business related accounts, we do not sell voice services that allows outbound calling.

Know-Your-Customer Processes.

Twigby relies on multiple points of data when activating new residential lines. Most importantly our system monitors traffic patterns for fraud or robo-traffic and we take measures to eliminate those lines. Our retail voice customers are in or near the geographic service area in which we serve under Verizon MVNO agreement. The vast majority of our voice or data capable end-users customers are residential or minimum line business accounts. These customers are limited to one call path, thereby minimizing the overall risk of robocalls originating from our customers.

The Company takes action on any sign of fraud or heavy calling patterns. Devices shipped to parties are assisted in confirmation by Paypal and Braintree services which includes a proprietary trust threshold on new device sales. For business customers, any multi-line business accounts is only with a contract, the Company confirms:

- Contact Person's name, and phone number,
- Physical business location,
- Federal Tax ID,
- Home state registration
- Nature of Business.
- More importantly, we block voice calling and any outbound text service to prevent issues.

Additionally, Verizon states that it follows procedures for ensuring it knows the identities of its customers, especially ones whose service permits them to engage in high volume calling campaigns.

Traceback.

The Company will respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and will cooperate with such entities in investigating and stopping any robocallers that use our network to originate robocalls.