

ROBOCALL MITIGATION PLAN

The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) requires voice service providers to implement STIR/SHAKEN authentication on Session Initiation Protocol (“SIP”) traffic on carrier networks as well as to implement a Robocall Mitigation Plan (“RMP”) covering non-SIP Time Division Multiplexing (“TDM”) traffic. The Federal Communications Commission (“Commission”) grants extensions through to June 30, 2023, for implementing STIR/SHAKEN authentication for carriers that qualify under the following conditions:

§64.6304 Extension of implementation deadline.

(a) *Small voice service providers.*

(1) Small voice service providers are exempt from the requirements of [§ 64.6301](#) through June 30, 2023, except that:

(i) A non-facilities-based small voice service provider is exempt from the requirements of [§ 64.6301](#) only until June 30, 2022; and

(ii) A small voice service provider notified by the Enforcement Bureau pursuant to [§ 0.111\(a\)\(27\) of this chapter](#) that fails to respond in a timely manner, fails to respond with the information requested by the Enforcement Bureau, including credible evidence that the robocall traffic identified in the notification is not illegal, fails to demonstrate that it taken steps to effectively mitigate the traffic, or if the Enforcement Bureau determines the provider violates [§ 64.1200\(n\)\(2\)](#), will no longer be exempt from the requirements of [§ 64.6301](#) beginning 90 days following the date of the Enforcement Bureau's determination, unless the extension would otherwise terminate earlier pursuant to paragraph (a)(1) introductory text or (a)(1)(i), in which case the earlier deadline applies.

(2) For purposes of this [paragraph \(a\)](#), “small voice service provider” means 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).

(b) ***Voice service providers and gateway providers that cannot obtain an SPC token.*** Voice service providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of [§ 64.6301](#) until they are capable of obtaining a SPC token. Gateway providers that are incapable of

obtaining an SPC token due to Governance Authority policy are exempt from the requirements of [§ 64.6302\(c\)](#) regarding call authentication.

(c) ***Services scheduled for section 214 discontinuance.*** Services which are subject to a pending application for permanent discontinuance of service filed as of June 30, 2021, pursuant to the processes established in [47 CFR 63.60](#) through [63.100](#), as applicable, are exempt from the requirements of [§ 64.6301](#) through June 30, 2022.

(d) ***Non-IP Networks.*** Those portions of a voice service provider or gateway provider's network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls are deemed subject to a continuing extension. A voice service provider subject to the foregoing extension shall comply with the requirements of [§ 64.6303\(a\)](#) as to the portion of its network subject to the extension, and a gateway provider subject to the foregoing extension shall comply with the requirements of [§ 64.6303\(b\)](#) as to the portion of its network subject to the extension.

(e) ***Provider-specific extensions.*** The Wireline Competition Bureau may extend the deadline for compliance with [§ 64.6301](#) for voice service providers that file individual petitions for extensions by November 20, 2020. The Bureau shall seek comment on any such petitions and issue an order determining whether to grant the voice service provider an extension no later than March 30, 2021.

(f) ***Annual reevaluation of granted extensions.*** The Wireline Competition Bureau shall, in conjunction with an assessment of burdens and barriers to implementation of caller identification authentication technology, annually review the scope of all previously granted extensions and, after issuing a Public Notice seeking comment, may extend or decline to extend each such extension, and may decrease the scope of entities subject to a further extension.

[[85 FR 73395](#), Nov. 17, 2020, as amended at [87 FR 3693](#), Jan. 25, 2022; [87 FR 42946](#), July 18, 2022]

Online Savings, Inc. (“OSI”) operates as a “small voice service provider” with 100,000 or fewer voice service subscriber lines, qualifying for all extensions to date. Moreover, OSI provides services as a “pure reseller” with no control over the network infrastructure necessary to implement STIR/SHAKEN with regard to either SIP or TDM calling. As such, in addition to qualifying for the extensions, OSI remains exempt from the Commission’s STIR/SHAKEN requirements. *See In the Matter of Call Authentication Trust Anchor Implementation of TRACED Act Section 6(a) — Knowledge of Customers by Entities with Access to Numbering Resources,*

Report and Order, FCC 20-42, WC Docket No. 17-97 (Mar. 31, 2020) at ¶ 40; In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Sixth Report and Order, FCC 22-37, WC Docket No. 1797 (May 20, 2022) at ¶ 213, n.558. OSI relies upon fully STIR/SHAKEN compliant underlying providers to authenticate all customer calls. OSI hereby submits this Robocall Mitigation Plan to the Robocall Mitigation Database describing and confirming the following:

(1) OSI's specific reasonable steps to avoid originating illegal robocall traffic as part of this RMP;

(2) OSI's intent to participate as a member of a working group, industry standards group, or consortium working to develop a non-internet Protocol caller identification authentication solution; and,

(3) OSI's commitment to respond fully and timely to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers using OSI's service to originate calls.

I. EFFORTS TO AVOID ORIGINATING ILLEGAL ROBOCALLS AS PART OF THIS RMP

OSI includes meaningful investments in new features within the budget to combat illegal robocalls as part of its RMP. OSI considers the benefit of deploying systems to detect potential robocall activity relying upon statistics such as averagecall duration, Answer Seize Ratio ("ASR"), and call count carrier/consumer reports. As part of OSI's RMP, OSI provides the following solutions to help minimize the impact of illegal or unwanted robocalls on customers:

- **Automatic Number Identification Management:** OSI seeks to identify and block originating telephone numbers deemed abusive based upon patterns of activity.
- **Proactive Blocking:** Per rules adopted by the Commission in FCC 17-151, OSI requests underlying carriers to block calls from phone numbers on Do-Not-Originate lists from US Telecom and Neustar.

- **Training:** OSI periodically trains sales teams to refrain from selling OSI voice services to suspected high call volume and low call revenue profiles, or if customer uses automated dialing systems.
- **Terms and Conditions of Customer Agreements:** OSI's voice service terms and conditions prohibit customers from originating any calls using auto-dialer or other automated call generator, further providing OSI with the right to suspend service if OSI suspects or detects such calls originating from the customer.

Through reports generated by Call Detail Record and pattern trends, fraud information sharing through industry organizations, and third-party notifications and complaints, OSI may identify potential unlawful robocalling. In instances where OSI suspects or identifies unlawful calling, in addition to taking the steps identified above, OSI reserves the right to take any action it deems necessary to eliminate the fraudulent activity.

II. Know Your Customer Program

OSI maintains established and implemented comprehensive Know Your Customer ("KYC") policies for any new and existing customers. One objective of the KYC policy includes preventing OSI from being used, intentionally or unintentionally, for spoofed or illegal traffic. KYC procedures enable OSI to identify and understand customers, which in turn helps OSI manage unlawful traffic.

III. LEADERSHIP ON STIR/SHAKEN DEVELOPMENT AND IMPLEMENTATION

OSI intends to participate in working groups, industry standards' group, or consortium working to develop further caller identification authentication solutions.

IV. COMMITMENT TO RESPONDING TO TRACEBACK REQUESTS

OSI remains committed to responding fully and timely to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to co-operating with such entities in investigating and stopping any illegal robocallers using OSI service to originate calls. OSI will work with the FTC and state attorney general counsel to participate in traceback

efforts, further demonstrating commitment to such important efforts.

V. COMMISSION, LAW ENFORCEMENT, OR REGULATORY ACTION

OSI is not barred from the Robocall Mitigation Database due to any law enforcement or Commission action. Further, OSI is not subject to any Commission, law enforcement, or other regulatory action or investigation due to suspected unlawful robocalling or spoofing.

VI. COMPANY INFORMATION

OSI operates under the business name Online Savings, Inc., and primary address is 10161 Park Run Drive, Suite 231, Las Vegas, Nevada 89145. OSI is not a foreign provider. The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation–related issues follows:

James Holmquist
Chief Executive Officer
Online Savings, Inc.
10161 Park Run Drive, Suite 231
Las Vegas, Nevada 89145
(612) 867-2451
jim@coremarkinc.com