

## **Robocall Mitigation Plan**

### Business Information

Mint Mobile, LLC  
12920 SE 38<sup>th</sup> St.  
Bellevue, WA 98006

### Contact Information

Saul Milgram  
Director, Strategy & Business Realization  
(949) 239-9461  
[Saul.Milgram1@T-Mobile.com](mailto:Saul.Milgram1@T-Mobile.com)

### Overview

In the Commission’s release, In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (rel. March 17, 2023) (“R&O”) it is stated that all voice service providers (“VSPs”) must file robocall mitigation plans (“RMPs”) that, among other things, outline “reasonable steps” taken to avoid originating illegal robocalls.

In addition to the “reasonable steps,” the FCC requires that a RMP include:

- “know your customer” procedures;
- “know your upstream provider”;
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

### Purpose

Mint Mobile, LLC (“Mint”) is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. Because Mint lacks control of the infrastructure necessary to implement STIR/SHAKEN, it is not required to be STIR/SHAKEN compliant. In compliance with the R&O, Mint submits this RMP and certification.

### Know Your Customer (“KYC”)

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity

that has a business relationship with Mint in which it transmits, originates, and/or terminates calls based on behalf of the subscriber.

Mint vets its subscribers by collecting their names, email addresses, addresses, and Wi-Fi calling addresses. Mint also has payment velocity restrictions based on subscribers' activity and behaviors. Mint leverages digital fingerprinting (device, IP and geolocation), which is passed to Mint's payment processor's FPA (Fraud Protection Advanced) system. Mint utilizes a third-party service at the e-commerce and activation points to help prevent bad actors from accessing the network and using it for illegal purposes. Mint's internal policies include policies concerning subscribers' dollar amount, payment frequency, velocity, attribute-based velocity, geo-location, fraud risk score models, and blacklists. Mint has also placed greater restrictions for transactions of larger dollar amounts to protect Mint's higher value merchandise from getting targeted by fraudsters. This system translates into a Fraud Risk score that Mint uses to apply rules that will reject a payment if certain criteria are met.

#### Know Your Upstream Providers

In accordance with the Commission's directive in Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59 (Rel. May 19, 2023) ¶¶ 49-51, Mint provides the following information concerning its upstream voice service carrier. Mint's upstream provider is:

T-Mobile USA, Inc.  
12920 S.E. 38th Street  
Bellevue, WA 98006  
Brian Gavin  
Brian.A.Gavin@t-mobile.com

While Mint and its upstream provider have no contractual provisions regarding robocall mitigation, T-Mobile USA, Inc. ("T-Mobile") has provided a letter to its customers (including Mint) that it has implemented robocall mitigation practices. T-Mobile is also listed as STIR/SHAKEN compliant in the FCC's Robocall Mitigation Database. Both parties work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

#### Acceptable Use Policy ("AUP")

Mint maintains an AUP that subscribers must accept before being permitted to use Mint's network. See <https://www.mintmobile.com/acceptable-use-policy/>.

### Analytics for Monitoring Traffic

Mint works with its upstream carrier to analyze high-volume voice traffic to identify and monitor patterns consistent with robocalls. The upstream carrier's system alerts it to calling patterns with unusual spikes, traffic patterns, and related matters. This includes accessing T-Mobile's Scam Block & Shield.

If a calling pattern is detected that is consistent with illegal robocalls, Mint and its upstream provider will identify the party that is using its network to transmit those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

### Investigate Suspicious Activity

When new fraud is detected by T-Mobile's Fraud Management team or when other carriers send notifications of fraudulent usage, T-Mobile's Fraud Management team notifies Mint. Mint then takes prompt action to block or otherwise ensure that the perpetrator is identified, and the suspicious activity is investigated. If the FCC's robocall rules are violated, and/or other applicable laws and regulations are breached, Mint and T-Mobile will take the appropriate measures to rectify the situation, including cancellation of the offenders' service.

Information on T-Mobile processes for identifying and mitigating spam calls is described here:

<https://www.t-mobile.com/benefits/scam-shield-app> (consumer page)

<https://www.t-mobile.com/business/solutions/call-protection> (business page)

### Blocking

Mint works with its upstream carrier to abide by any Do Not Originate requests it receives from the Industry Traceback Group ("ITG"). Mint will cooperate with Investigative Bodies (provide a single point of contact) to address traceback requests from law enforcement and regulatory entities such as state attorneys general, the FCC, and/or ITG; as well as documenting requests & actions taken in response thereto.

### Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Mint will monitor industry best practices and continuously improve internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, Mint will file an update to the FCC Robocall Mitigation Database within ten (10) days.

### **Certification of Saul Milgram**

I, Saul Milgram, Director of Strategy and Business Realization of Mint Mobile, LLC (“Mint”) do hereby certify, under penalty of perjury, the following:

a. Mint is not required to implement STIR/SHAKEN, due to its lack of control over the necessary infrastructure.

b. Mint’s business name and primary address are as follows:

Mint Mobile, LLC  
12920 SE 38<sup>th</sup> St.  
Bellevue, WA 98006

c. Mint has no other business name.

d. Mint has not previously used any other business name.

e. The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.

f. Mint is 100% owned by T-Mobile USA, Inc. (“T-Mobile”). T-Mobile is a direct, wholly owned subsidiary of T-Mobile US, Inc. (“TMUS”), a publicly traded company. T-Mobile's principals - executive leadership and board members - are available at <https://beta.t-mobile.com/our-story/executive-leadershipteam>. T-Mobile's corporate structure, including FCC-regulated affiliates, subsidiaries, and parent companies, is contained in T-Mobile’s most recent FCC Form 602 on file with the Commission. Mint has no subsidiaries.

g. As an MVNO, Mint relies on T-Mobile’s implementation of network-level functionalities to support call authentication, traceback response, and mitigation actions, such as blocking, suspension, or termination of suspect traffic when illegal robocalling is suspected or confirmed.

h. Mint is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

i. Mint has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

j. Mint is not required to, and does not have, an Operator Code Number.

A handwritten signature in black ink, appearing to read 'S. Milgram', is written over a horizontal line.

Saul Milgram