



Simwood Inc.

Robocall Mitigation Plan

Updated – February 19, 2026



The following is Simwood Inc. ("Simwood") submission to the Robocall Mitigation Database, pursuant to the FCC's directives outlined in the Report and Order(s) DA 24-73 (<https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf>) (RMD Public Notice)

Simwood is a wholly owned subsidiary of Simwood Group PLC located at Simwood House Cube M4 Business Park Old Gloucester Road Bristol BS16 1FX United Kingdom +44 330 122 3000. Registered in England 03379831 - USA +1 833 857 3277

Simwood Inc. USA Address

4935 Main St., STE 7-306

Spring Hill, TN 37174-2735

Indicated below are the robocall mitigation measures employed by Simwood switching platform. Simwood implements the features on their network and traffic. Simwood certifies that its switching platform follows required traceback standards. Simwood will continue to implement new robocall mitigation measures as they become available.

24 Hour Response

Simwood certifies that it will respond to all Traceback Requests from the Industry Traceback group (ITG) within 24 hours and civil and criminal law enforcement agencies, cooperating fully in efforts to investigate and eliminate illegal robocalls, while following CPNI requirements.

Full STIR/SHAKEN implementation

Simwood has fully implemented STIR/SHAKEN attestation. Simwood is a USA CLEC carrier, with the address of 4935 Main St., STE 7-306 Spring Hill, TN 37174-2735. All compliance or questions with the RMD and/or STIR/SHAKEN should be reported to team@simwood.com.

Simwood RMD Verification

Simwood policies require refusing traffic from any provider not registered in the Robocall Mitigation Database (RMD).

Simwood KYC Verification

Simwood performs Customer Due Diligence and KYC, Mandating that all potential customers complete a Know Your Customer (KYC) form and undergo a due diligence process.

Simwood DNO Compliance

Simwood is utilizing Do Not Originate ("DNO") lists, primarily leveraging the ITG list, as well as adding additional numbers reported outside the ITG list manually.



Simwood Mitigation Certification

Simwood certifies that all calls originating on our network are subjected to a robocall mitigation program that meets the specified requirements. We affirm that our prior certifications remain unrevoked by Commission action and that we are not barred from participation in the Robocall Mitigation Database. Simwood has fully implemented STIR/SHAKEN across our network.

The following plan shall outline specific “commercially reasonable efforts/steps” Simwood has undertaken to prevent origination and transmission illegal robocall traffic.

Simwood operates in multiple capacities: As a direct service provider, an intermediate provider, and a U.S.-based gateway provider. Simwood also has direct retail customers in addition to our wholesale operations.

Analytics

Simwood relies in part on third-party analytics. Simwood relies up on ITG Communications for Do Not Originate lists, and Simwood relies upon Peeredge Telecom for spam filter services to block and label calls as SPAM.

The following plan shall outline specific “commercially reasonable efforts/steps” Simwood has undertaken to prevent origination and transmission illegal robocall traffic. Simwood operates in multiple capacities: As a direct service provider, an intermediate provider, and a U.S.-based gateway provider. Simwood also has direct retail customers in addition to our wholesale operations.

Third-Party Token Signing

UNICHIP does sign/attest certain calls for customers, not engaged in resale operations. We do not sign or attest for any companies we determine involved in gateway, wholesale, resale, using the US calling numbers calling US toll destinations. We will Attest “C” for Non USA calling numbers, to US toll destinations, showing we are the gateway into USA, only for customers who are truly KYC compliant, Enterprise customers.

Regulatory Compliance

Simwood is not currently, nor has it ever been, subject to any Commission, law enforcement, or regulatory agency action or investigation related to suspected unlawful robocalling or spoofing activities.



Operating Company Numbers (OCN)

Reseller Company Number: 107J

Additional OCNs

AR: 741J
CA 647J
CO: 612J
FL: 600J
GA: 601J
ID: 538J
IN: 602J
KY: 539J
MO: 540J
MT: 106J
NC: 604J
ND: 511J
NY: 603J
OH: 605J
OR: 512J
RI: 648J
SD: 606J
TX: 541J
WI: 542J
WV: 631J
WY:: 614J

Traceback CPNI

For handling sensitive customer information (CPNI), Simwood adheres to strict protocols, ensuring that such information is exclusively shared through the official ITG portal. It is important to note that CPNI is only disclosed within the secure transmission such as ITG portal.

To facilitate the traceback process, the official channels through which Traceback Requests can be initiated:

Email: Requests can be directed to team@simwood.com - Upon receipt, Simwood personnel will verify the request before proceeding.

Direct Contact: Peter Farmer (Compliance Officer), is the designated contact in the Robocall Mitigation Database, via email at Peter Farmer peter.farmer@simwood.com.

NOC: Available around the clock, our support center can be reached at team@simwood.com. Upon receipt a ticket is assigned, and tracked to completion.



Methods and Efforts Employed to Avoid Carrying or Processing Illegal Robocalls

- Do Not Originate “DNO” queries (ITG Database) are utilized to confirm compliance with proper DNO requirements.
- Know Your Customer “KYC” measures have been implemented, and are reviewed yearly for customers, to ensure compliance.
- ANIs and DNISs are tracked and documented from customer through vendor delivery, including all voice “hops” and stored for 90-days.
- Originating and termination numbers are profiled by traffic analytics engine for irregular behavior including, but not limited to:
 - High Volume / Short Duration Traffic
 - Calls to Unallocated Numbers
 - Calls with excessive cancels
 - Calls from numbers that exist on a known robodialer list.
- Automated filtering for both inbound and outbound traffic to our voice network.
- Simwood commits to respond within the 24-hour requirement 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 that use its service to originate calls.
- Simwood will continue to monitor the FCC publicly released listings of VSPs who have triggered requests, and promptly block any traffic when notified by the FCC and/or respond to commission as to the source of the traffic.
- Simwood shall take action when notified by the FCC of potentially illegal calls utilizing its network and will promptly inform the Commission that it is not the originating or gateway provider for the identified traffic, specify which upstream VSP with direct access to the U.S. public switched telephone network it received the traffic from, and, if possible, take lawful steps to mitigate this traffic.
- Simwood will block any VSP immediately downstream when notified by the FCC that the VSP has failed to satisfy its obligations under these rules.
- We conduct a review of our measures in an effort to combat new techniques that scammers use to compromise the PSTN in the US.
- Simwood maintains an Acceptable Use Policy (AUP) that subscribers may sign before being permitted to use Simwood’s network. Simwood’s contractual terms with subscribers specify that Simwood may take action up to suspension or termination of service for violation of the AUP. Among other things, the AUP prohibits:
 - providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
 - violating any applicable law;
 - violating applicable industry accepted guidelines; and
 - Using Simwood’s service to engage in or in connection with fraudulent activities.
- Simwood works with its upstream carriers to detect a calling pattern consistent with illegal robocalls. If such a call is detected, Simwood will identify the party that is using our network to originate 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.



- When traffic analysis indicates the presence of likely illegal robocalling, Simwood may follow certain procedures on investigating such subscribers.
The procedures established may include but are not limited to:
 - checking recent and past call detail records and benchmark against expected trends;
 - checking recent and past account activity and purchases;
 - investigating if any system issue generates the strange behavior;
 - verifying that the call originating path is valid; and
 - contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.
- New customers requesting an excessive number of calls per second “CPS” will be screened for legitimate call usage needs.
- New and existing customers with an excessive number of call paths may receive Robocall outreach
- Simwood utilizes KYC measures to eliminate illegal robocalling customers from terminating to Simwood's network.

Traceback Requests.

Simwood certifies that its software follows required traceback standards. Simwood commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, regulators, and the industry traceback consortium.

STIR/SHAKEN Implementation.

Simwood has implemented STIR/SHAKEN to all egress traffic. STIR (Secure Telephony Identity Revisited) and SHAKEN (Secure Handling of Asserted information using toKENS) is an industry framework that is being developed to prevent the completion of calls where the originating provider does not own or is not authorized to use the Caller ID associated with the call (a “spoofed call”). STIR/SHAKEN uses digital certificates, based on common public key cryptography techniques, to ensure the calling number of a telephone call is secure. The expectation is that the certificate technology will enable the called party to verify that the calling number is accurate and that it has not been illegally spoofed.

Thomas Hadden
COO
4935 Main St., STE 7-306
Spring Hill, TN 37174-2735
Updated 02/19/2026

Thomas Hadden

02/19/2026