**FCC Robocall Mitigation Database Certification**

**Voice Service Provider and Non-Gateway Intermediate Provider – 47 CFR § 64.6305(d) and (f)**

Plan revision: November 2026 (supersedes all prior versions – Last Plan Rev. March 2026)

Enguity LTD L.C. ("Enguity"), together with its wholly owned subsidiary Enguity Technology Corp., is a small, facilities-based interconnected VoIP voice service provider that originates and terminates calls for its own end-user customers, a wholesale originating provider for the end users of select reseller providers that operate on Enguity's platform, and a non-gateway intermediate provider that carries calls for select small and mid-sized U.S. facilities-based interconnected VoIP providers and carriers, over a dedicated nationwide ring-protected network on which all voice, signaling and control traffic is IP (SIP). Enguity previously relied upon the small voice service provider extension under 47 CFR § 64.6304(a), which expired on June 30, 2023, and formerly relied upon the continuing extension for non-IP network portions under 47 CFR § 64.6304(d) for the TDM/ipTDM portions of its network; in October 2026 Enguity completed the upgrade of those portions to IP, and Enguity's network is now 100% IP. Enguity no longer operates any non-IP network segment and no longer relies upon any extension under 47 CFR § 64.6304. **Effective June 8, 2021, Enguity fully implemented the STIR/SHAKEN caller ID authentication framework on the IP portions of its network, and since October 2026, upon completion of its transition to an all-IP network, STIR/SHAKEN caller ID authentication is implemented across Enguity's entire voice network.**

This Robocall Mitigation Plan ("Plan") is submitted with Enguity Technology Corp.'s certification in the FCC Robocall Mitigation Database ("RMD") as a voice service provider pursuant to 47 CFR § 64.6305(d) and as a non-gateway intermediate provider pursuant to 47 CFR § 64.6305(f), and describes the specific reasonable steps Enguity has taken to avoid originating, carrying, or processing illegal robocall traffic. All calls that Enguity originates, carries, or processes on its network are subject to this Plan. This filing is made under FCC Registration Number 0023384621 and updates Enguity Technology Corp.'s existing certification (RMD0008025), which has not been removed by Commission action; Enguity Technology Corp. has not been prohibited from filing in the RMD by the Commission. Enguity Technology Corp. is a wholly owned subsidiary of Enguity LTD L.C., which holds Operating Company Number 037G and Enguity's STI-PA registration and STI certificate on behalf of the Enguity group. Enguity has implemented this Plan in accordance with the TRACED Act and the Commission's efforts to reduce or eliminate illegal robocalls.

**Enguity's Role in the Call Path and STIR/SHAKEN Implementation Status:**

**Role in the call path:** Enguity is (1) a voice service provider that originates and terminates calls for its own end-user customers; (2) a wholesale originating provider for the end users of select reseller providers whose services are provisioned on Enguity's SIP platform using telephone numbers held under Enguity's OCN; and (3) a non-gateway intermediate provider for calls it receives from, and delivers for, select small and mid-sized U.S. facilities-based interconnected VoIP providers and carriers that originate those calls on their own networks. Enguity is not a gateway provider: it has no international interconnection to its United States facilities and does not accept foreign-originated traffic that uses U.S. North American Numbering Plan numbers for delivery to U.S. subscribers. Should Enguity's role in the call path change, including any international interconnection, Enguity will update its RMD filing within ten (10) business days.

**STIR/SHAKEN implementation obligation (47 CFR § 64.6305(d)(4)(vi)):** Enguity is a

provider with a STIR/SHAKEN implementation obligation that (A) serves end users directly and (B) acts as a wholesale originator of calls for other providers, namely the reseller providers whose end users are served on Enguity's platform. Enguity authenticates and signs, with its own STI certificate, every call originated on its network in either capacity. Calls that Enguity receives from facilities-based carriers in its intermediate role are originated and authenticated by those carriers.

**STIR/SHAKEN certification option:** As a voice service provider, Enguity certifies to COMPLETE STIR/SHAKEN implementation (47 CFR § 64.6305(d)(1)(i)): Enguity has fully implemented the STIR/SHAKEN authentication framework across its entire network, and all calls that Enguity originates are authenticated in compliance with 47 CFR § 64.6301. As a non-gateway intermediate provider, Enguity certifies pursuant to 47 CFR § 64.6305(f)(1) that it has fully implemented STIR/SHAKEN on its network in compliance with 47 CFR § 64.6302: it passes authenticated caller ID information (SIP Identity headers) unaltered to the next provider in the call path, and it authenticates, using its own STI certificate, any unauthenticated SIP call that it receives directly from an originating provider (47 CFR § 64.6302(e)). Enguity does not claim any extension under 47 CFR § 64.6304 (47 CFR § 64.6305(d)(2)(i), (f)(2)(i)). All calls Enguity originates, carries, or processes nonetheless remain subject to the robocall mitigation measures described in this Plan.

**SPC token, STI certificate and third-party authentication:** Enguity is registered with the STIR/SHAKEN Policy Administrator (STI-PA, iconectiv) under Service Provider Code (SPC) 037G, has obtained its own SPC token, and has obtained its own STI certificate from Martini Security, LLC, an STI-PA-approved STIR/SHAKEN Certificate Authority (see "STIR/SHAKEN Credentials" below). All calls authenticated on Enguity's behalf are signed using Enguity's own certificate, by Enguity, and Enguity alone makes all attestation-level (A/B/C) decisions in accordance with the ATIS STIR/SHAKEN standards. Enguity signs all calls directly and does not use any other third-party signing authentication services.

From June 2021 until October 2026, Enguity relied upon a hosted third-party signing arrangement with one of its interconnection partners under a written STIR/SHAKEN implementation agreement executed June 29, 2021, primarily for its former TDM segments, upon out-of-band authentication. Both arrangements have ended: Enguity registered directly with the STI-PA and obtained its own SPC token and its own STI certificate from Martini Security, and retired its TDM facilities in October 2026. Enguity now signs all calls directly using its own STI certificate and does not use any third-party signing service. Enguity retains records of the prior arrangements and will provide them to the Commission upon request, consistent with the Commission's third-party authentication rules effective September 18, 2025 (Eighth Caller ID Authentication Report and Order, FCC 24-120).

**Enguity's Network:**

Enguity operates an all-IP, SIP-based voice network. As of October 2026, Enguity has retired its legacy TDM and ipTDM voice trunking infrastructure and no longer operates any network segment that cannot initiate, maintain, carry, process, and terminate SIP calls. All calls originating from or terminating into Enguity's network are processed and transported primarily by privately managed network infrastructure and/or are encrypted utilizing Xcorpeon ASIC (hardware based) Carrier Ethernet Transport systems.

**Enguity's Former Non-IP based Voice Network (Retired October 2026):**

Enguity historically operated TDM and ipTDM voice network segments that could not initiate, maintain, carry, process, and/or terminate SIP calls and that were deemed subject to the continuing extension under 47 CFR § 64.6304(d). In October 2026, Enguity completed the upgrade of its entire network to IP, satisfying 47 CFR § 64.6303(a)(1): Enguity's network is now 100% IP, every call Enguity originates is a

SIP call authenticated with a STIR/SHAKEN PASSporT signed with Enguity's own STI certificate, and Enguity no longer operates any non-IP network segment. Accordingly, the non-IP continuing extension under 47 CFR § 64.6304(d) no longer applies to Enguity, and Enguity does not rely upon any extension under 47 CFR § 64.6304.

Enguity's interconnection partners no longer sign any calls on Enguity's behalf, and Enguity no longer relies upon any out-of-band authentication arrangement. Enguity itself authenticates every call it originates, makes all attestation-level decisions, and signs with its own STI certificate, consistent with the Commission's third-party authentication rules. Enguity interconnects with its partners over IP (SIP) and has confirmed that the STIR/SHAKEN Identity headers it originates are passed downstream unaltered.

Enguity retains the engineering records, interoperability test results, and interconnection partner confirmations documenting the retirement of its TDM/ipTDM facilities and the completion of its all-IP STIR/SHAKEN implementation, and will provide them to the Commission upon request. Should Enguity ever reintroduce a non-IP network segment, it will update this filing within ten (10) business days and comply with 47 CFR § 64.6303.

**Enguity's IP based Voice Network:**

In accordance with our prior commitment and as noted in our prior RMD certifications: **Effective June 8, 2021, Enguity has fully implemented the STIR/SHAKEN authentication framework for all calls transiting Enguity's IP-based voice network.** Enguity authenticates caller ID information for every SIP call it originates on its IP network in accordance with 47 CFR § 64.6301 and the ATIS-1000074, ATIS-1000080 and ATIS-1000084 standards; assigns attestation levels (A, B or C) based on Enguity's own verified relationship with the customer and the customer's verified authorization to use the calling telephone number; and verifies caller ID authentication information on SIP calls that it terminates to its subscribers.

In October 2026, Enguity completed its transition to a 100% IP network by retiring its remaining TDM/ipTDM facilities. Enguity's direct and full STIR/SHAKEN implementation therefore now extends across Enguity's entire voice network, and every call Enguity originates is authenticated. This RMD filing has been updated within ten (10) business days of that change as required by 47 CFR § 64.6305(d)(5).

**STIR/SHAKEN Credentials (Eighth Caller ID Authentication Report and Order, FCC 24-120):**

Enguity authenticates its calls using its own STI certificate issued under the STI-PA (iconectiv) STIR/SHAKEN certificate policy (policy OID 2.16.840.1.114569.1.1.4) by an STI-PA-approved Certificate Authority. Enguity's current credentials are as follows:

STI-PA Service Provider Code (SPC) / TNAuthList: 037G (OCN 037G, assigned by NECA to Enguity LTD L.C. and used by Enguity Technology Corp.)

STI Certificate Authority (STI-CA): Martini Security, LLC – Martini Security SHAKEN G3 (Seattle, WA)

Certificate subject: CN = SHAKEN 037G; O = ENGUITY LTD L.C. (SPC 037G)

Key type / signature: ECDSA P-256 (prime256v1), ecdsa-with-SHA256, as required by ATIS-1000080 and ATIS-1000084

Certificate lifecycle: short-lived (90-day) certificates issued by Enguity's STI-CA under Enguity's SPC token and automatically renewed prior to expiry; revocation status published via the STI-PA Certificate Revocation List (authenticate-api.iconectiv.com).

Enguity makes all attestation-level decisions itself: A-level attestation is applied

only where Enguity has a direct authenticated relationship with the customer and has verified the customer's authorization to use the calling number; B-level where the customer relationship is verified but the number is not; and C-level otherwise. Enguity's SPC token, STI certificates and any written third-party signing agreement are maintained in accordance with the Commission's recordkeeping requirements, and Enguity will update this filing within ten (10) business days of any change in its STI-PA status or STI-CA.

**Industry Traceback Consortium (ITG) Cooperation:**

**Enguity commits to respond fully and in a timely manner, and in any event within twenty-four (24) hours, to all traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium (currently the USTelecom-led Industry Traceback Group ("ITG")), and to cooperate fully with such entities in investigating and stopping any illegal robocallers that use Enguity's service to originate, carry, or process calls, as required by 47 CFR § 64.1200(n)(1) and § 64.6305(a)(2), (c)(2), (d)(2)(iii) and (f)(2)(iii).**

Traceback requests are received through the contact points identified under "Network Traceback Requests" below, which are monitored twenty-four (24) hours a day, seven (7) days a week. Enguity responds to requests received through, the ITG Secure Traceback Portal. Enguity retains call detail records sufficient to identify the source of any call it originates for a period of not less than five years. (five and a half year rolling lookback)

**Response to Commission Notifications (47 CFR § 64.1200(n)(2)-(3)):**

Upon receipt of a Notice of Suspected Illegal Traffic from the FCC Enforcement Bureau, Enguity will promptly investigate the identified traffic, block it (and substantially similar traffic) on an ongoing basis where Enguity is the originating provider, cease transmitting it where Enguity is an intermediate provider, and report the results of its investigation to the Bureau within the time specified in the notice, including a description of the traffic, the steps taken, and whether Enguity has blocked it, as required by 47 CFR § 64.1200(n)(2). Pursuant to 47 CFR § 64.1200(n)(3), Enguity monitors EB Docket No. 22-174 and, upon release of a Final Determination Order against any upstream provider, will block and cease accepting all traffic received directly from that provider beginning thirty (30) days after release of the order. Enguity will likewise act upon credible notifications received from state attorneys general, the ITG, or downstream providers.

**Enguity's Traceback & Robocall history:**

As of the date of this filing, *No such traceback requests have occurred*, *nor has any other carrier identified potentially malicious traffic originating, terminating and/or transiting Enguity's voice and/or data network(s)*.

⋆ Should Enguity's "***clean call***" status change, Enguity shall update the Traceback & Robocall history section of this filing within ten (10) business days.

**Enguity's Additional Information (FCC):**

At no time since its formation, and in any event within the two (2) years preceding the date of this filing as required by 47 CFR § 64.6305(d)(2)(iv), has Enguity or any entity under common ownership, management, or control with Enguity (including any principal, affiliate, subsidiary, or parent company) 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 due to a deficient Robocall Mitigation Database certification or mitigation program description.

**Enguity has taken the following specific steps to detect and prevent originating robocall traffic:**

Enguity limits the number of end-user facing voice trunk channels, SIP registrations and number of originating call appearances on a per TN, per customer basis. Further, SIP subscribers have the option to set outgoing call limits beyond those already set by Enguity on the number of simultaneous originating calls.

Enguity has developed a proprietary, broad-based detection system and, in addition, utilizes industry-standard practices and third-party database and analytics services to raise network alarms based upon call volume thresholds (calls per second, calls per hour/day per customer and per telephone number), short-duration and low-answer-rate patterns, high volumes of calls to numbers on the National Do-Not-Call Registry, Do Not Originate database, unusual international or sequential-dialing patterns, and other indicators of illegal robocalling. Alarms are monitored continuously, and log and call detail records are reviewed and analyzed daily by Enguity Network Operations personnel.

Third-party analytics vendors (47 CFR § 64.6305(d)(2)(ii)): Enguity does not use any third-party analytics vendor.

In addition to the above: Enguity has artificially rate-limited the number of calls per second each customer/end-user interface can originate at any given time, while also proactively monitoring our overall network for any excess call origination attempts.

Enguity does not originate, and blocks at origination and in transit, calls that purport to originate from telephone numbers on a reasonable do-not-originate (DNO) list, including invalid, unallocated, and unused North American Numbering Plan numbers and numbers whose subscribers have requested that outbound calls not be originated from them, as required by 47 CFR § 64.1200(o). Enguity also restricts each customer to originating calls only from telephone numbers that Enguity has assigned to that customer or for which the customer has demonstrated authorization to use.

**Enguity has *at a minimum* taken the following steps to prevent unlawfully originating robocalling traffic:**

Pursuant to its know-your-customer obligation under 47 CFR § 64.1200(n)(4), Enguity takes affirmative, effective measures to prevent new and renewing customers, carriers, or interconnection partners from using its network to originate illegal calls. Procedures and automated systems are in place to confirm the identity of each new voice end-user before service is activated, by collecting and verifying information including the customer's legal name, physical business location, contact person(s), state or country of incorporation, federal tax identification number, the general nature of the end-user's business and intended use of the service, the expected calling volume and pattern, and the telephone numbers the customer is authorized to present as caller ID. A post office box, virtual office box, or other mail-forwarding or mail-drop address is not accepted; a physical business address is required and verified by Enguity staff. Customer information is re-verified upon each service renewal or contract term, upon any material change in the customer's calling pattern, and not less than annually.

Enguity goes well beyond industry standard practices, including but not limited to obtaining consumer and business credit profiles on any potential new business customer/entity, its owners, officers, and managers.

**Reseller (wholesale origination) know-your-customer measures:** For reseller providers whose end users are served on Enguity’s platform, Enguity (1) vets the reseller as a customer under the procedures above, and additionally verifies the reseller’s FCC Registration Number, Form 499 Filer ID (or basis for exemption) and current Robocall

Mitigation Database listing before activating service; (2) requires each reseller, by written agreement, to perform know-your-customer due diligence on its own end users to a standard no less stringent than Enguity's, to prohibit illegal robocalling and caller ID spoofing in its own terms of service, and to maintain its own robocall mitigation program; (3) requires each reseller to identify, upon request and in any event within the time needed for Enguity to meet its 24-hour traceback obligation, the end user responsible for any call; (4) applies per-reseller and per-end-user calling limits, rate limits and the analytics described above, with each reseller provisioned on separately identifiable trunks or accounts so that traffic is attributable to the reseller and end user; (5) assigns attestation levels according to what Enguity has itself verified — A-level only where Enguity has verified the end user's identity and authorization to use the calling number, and B-level where Enguity has verified the reseller but not the end user; and (6) suspends a reseller's end user, or the reseller, where illegal traffic is identified and not promptly remediated.

Enguity further requests criminal and civil background checks on any such potential new customer/entity, its owners, and shareholders.

Enguity's Terms of Service, Letter of Authorization, Interconnection Agreements and Acceptable Use Policies have been updated to reflect our position and the associated actions that will be taken upon receipt of unlawful voice traffic and/or robocalls.

Enguity shall send the required monthly reports to the Reassigned Numbers Database per the Second Report and Order on Advanced Methods to Target and Eliminate Unlawful Robocalls (FCC 18-177).

**Know-Your-Upstream-Provider Procedures (47 CFR § 64.1200(n)(5); § 64.6305(d)(2)(ii), (f)(2)(ii) and (g)):**

Enguity accepts voice traffic directly only from voice service providers, gateway providers, and intermediate providers whose certifications appear in the Robocall Mitigation Database and have not been de-listed pursuant to Commission enforcement action, in accordance with 47 CFR § 64.6305(g). Before establishing any new interconnection or accepting traffic from an upstream provider (including any foreign provider that uses U.S. North American Numbering Plan resources), Enguity: (1) verifies the provider's RMD filing, FCC Registration Number (FRN), Operating Company Number (OCN) and FCC Form 499 Filer ID; (2) confirms the provider's legal identity, principals and physical business address; (3) obtains a physically signed interconnection or service agreement that incorporates Enguity's Acceptable Use Policy and requires the upstream provider to maintain its own robocall mitigation program, to pass STIR/SHAKEN authentication information unaltered, and to respond to traceback requests; and (4) records the identity of the upstream provider's robocall mitigation point of contact.

Enguity re-verifies the RMD status of each upstream provider not less than daily via internally automated applications and upon notice of any Commission enforcement action, and will immediately cease accepting traffic from any provider whose RMD certification is removed. As of the date of this filing, Enguity receives traffic for termination to its subscribers only from its direct interconnection partners, each of which is listed in the Robocall Mitigation Database.

In its non-gateway intermediate provider role, and pursuant to 47 CFR § 64.1200(n)(5), Enguity takes reasonable and effective steps to ensure that the originating and intermediate providers sending it traffic are not using Enguity's network to carry or process high volumes of illegal traffic: each upstream provider is assigned dedicated trunk groups so that traffic is attributable to its source; per-trunk-group analytics (call volume, calls per second, average call duration,

answer-seizure ratio, invalid or unallocated calling numbers, and DNO hits) are monitored continuously and reviewed daily; the upstream provider's RMD listing and STIR/SHAKEN attestation rates are reviewed not less than quarterly; and Enguity requires each upstream provider, by written agreement, to maintain its own robocall mitigation program, to authenticate the calls it originates, and to respond to traceback requests within twenty-four (24) hours.

**Steps Enguity takes to avoid carrying or processing illegal robocall traffic (47 CFR § 64.6305(f)(2)(ii)):**

In addition to the measures above, Enguity: (1) accepts traffic directly only from providers listed in the Robocall Mitigation Database (47 CFR § 64.6305(g)); (2) passes SIP Identity headers it receives unaltered to the next provider in the call path and verifies them where it is the terminating provider; (3) authenticates, with its own STI certificate and the appropriate attestation level, any unauthenticated SIP call it receives directly from an originating provider (47 CFR § 64.6302(e)); (4) blocks calls from numbers on its reasonable DNO list in transit (47 CFR § 64.1200(o)); (5) throttles or suspends an upstream provider's trunk group upon detection of suspected illegal traffic pending the provider's explanation, and terminates the interconnection where the provider fails to mitigate; (6) blocks all traffic from any upstream provider subject to a Final Determination Order (47 CFR § 64.1200(n)(3)); and (7) responds to traceback requests concerning calls it carried within twenty-four (24) hours, identifying the upstream provider from which each call was received.

**Enguity has taken the following steps to mitigate illegal originating or transiting robocall traffic upon detection:**

Upon detection of suspected illegal robocall traffic, or upon notification from the Commission, law enforcement, the ITG, a state attorney general, or a downstream provider, Enguity will: (1) promptly investigate the identified traffic and the originating customer or upstream provider; (2) at its discretion impose network-level constraints, including throttling the rate at which the end-user or upstream provider can initiate calls; (3) suspend all non-emergency (non-911) outbound calling services during the investigation; (4) block the identified traffic and terminate service or the interconnection where illegal robocalling is confirmed, at Enguity's discretion and in accordance with its Terms of Service, Interconnection Agreements and Acceptable Use Policy; (5) preserve relevant call detail records and respond to any related traceback request within twenty-four (24) hours; and (6) where the notification is from the Enforcement Bureau, respond as described under "Response to Commission Notifications" above.

**Maintenance of this Certification; Annual Recertification; Recordkeeping:**

Enguity will update its RMD filing, including this Plan, within ten (10) business days of any change to the information submitted, as required by 47 CFR § 64.6305(d)(5), and will recertify on or before March 1 of each year that the information contained in its RMD filing is true and correct, as required by 47 CFR § 64.6305(h). Enguity keeps its FCC CORES registration, FRN contact information and this Plan current. Enguity retains records supporting this Plan — including customer identification and due-diligence records, upstream-provider verification records, any third-party authentication agreement, engineering and test records documenting its STIR/SHAKEN implementation across its entire network, its SPC token and STI certificate records, traceback responses, and call detail records — for not less than five years, and will make such records available to the Commission upon request.

**Enguity's Relevant Network Assignments:**

Robocall Mitigation Plan Certification – Original filing: 09/2021; Last update: 04/2024; ***Last annual recertification*: 03/2026; *This* revision: 11/2026**

==========

RMD Filing : RMD0008025 (this filing updates the existing certification)
FCC FRN : 0023384621 (Enguity Technology Corp.)
Business Name : Enguity Technology Corp.
Parent Company : Enguity LTD L.C.
Parent Company FRN : 0037142460
FCC Reg AoS : 1901 Pennsylvania Ave. NW, Suite #900 PMB#124 Washington DC 20006-3405
Other FRNs : 0037142460 (Enguity LTD L.C., parent company)
FCC Form 499 Filer ID : 837848
Foreign VSP : No (United States Domestic Only)
OCN : 037G (reassigned by NECA to Enguity LTD L.C.; used by Enguity Technology Corp.)
Role in call path : VSP - Voice Service Provider (originating and terminating, including wholesale origination for resellers) and Non-Gateway Intermediate Provider; not a gateway provider
STIR/SHAKEN obligation : Obligated provider – serves end users directly and acts as a wholesale originator for other providers (resellers)

STIR/SHAKEN certification : Complete implementation (entire network) – voice service provider and intermediate provider

Extension claimed : None

STI-PA SPC / TNAuthList : 037G STI-CA: Martini Security, LLC (SHAKEN G3)
ACNA : LNY

Other/Parent company : Enguity LTD L.C. (parent company of Enguity Technology Corp.; holder of OCN 037G and of Enguity's STI-PA registration and STI certificate)

==========

BGP ASN: AS40911

MAC OUI: 5C:4A:26 (Xcorpeon ASIC (hardware based) Carrier Ethernet Transport systems)

==========

IANA Service/Port Assignments (Xcorpeon ASIC (hardware based) Carrier Ethernet Transport systems):

| IANA Service Name | Port No. | Protocol | Assignee | Reg. Date |
|---|---|---|---|---|
| enguity-xccetp | 8041 | tcp | Enguity | 2017-06-28 |
| enguity-xccetp | 8041 | udp | Enguity | 2017-06-28 |

**Network Traceback Requests:**

| | |
|---|---|
| Carrier/Entity | : Enguity Technology Corp.<br>(Parent Company: Enguity LTD L.C.) |
| Global NOC E-Mail | : POC-AS40911@ENGUITY.COM (Best for non-exigent circumstances) |
| Network Operations | : 888.695.5905 |
| Customer Service | : 800.881.9531 |

**Robocall Mitigation Point of Contact (47 CFR § 64.6305(d)(4)(v)):**

| | |
|---|---|
| Name | : K.S. Beahn Jr. |
| Title | : CEO/CTO |
| Department | : Network Operations |
| Address | : 1901 Pennsylvania Ave. NW, Suite #900 PMB#124<br>Washington, DC 20006-3405 |
| Telephone | : 888.695.5905 (monitored 24x7) |
| E-Mail | : POC-AS40911@ENGUITY.COM |

**Network Traceback - Exigent Circumstances Requests:**

**Officer Declaration (47 CFR § 1.16):**

I declare under penalty of perjury that I am an officer of Enguity Technology Corp. and of its parent company Enguity LTD L.C., and am authorized to make this certification; that I have examined this Robocall Mitigation Plan and the accompanying Robocall Mitigation Database certification; and that all statements made herein are true, correct, and complete to the best of my knowledge, information, and belief.

Signature: _____ Date: November 3, 2026

Name / Title: K.S. Beahn Jr., CEO/CTO
Enguity LTD L.C. o/b/o Enguity Technology Corp.