

Verification Technologies LLC Revised Robocall Mitigation Plan¹

Pursuant to the applicable orders and regulations of the Federal Communications Commission ("FCC" or "Commission"), this Robocall Mitigation Plan ("RMP") details the reasonable steps undertaken by Verification Technologies LLC ("Verification Technologies" or the "Company") to comply with FCC regulations and prevent the origination, carrying, or processing of illegal robocalls.

SECTION 1: INTRODUCTION

Background: Verification Technologies serves as the primary intermediary for telecommunications inputs for a highly select group of customers, for which it facilitates the connection, transmission, and management of telecommunications services. As such, Verification Technologies is dedicated to combating illegal robocalls and fraudulent traffic, and has taken affirmative, effective measures to avoid originating, carrying, and processing illegal robocall traffic, as detailed herein.

Location: Verification Technologies main office is located at 177 Cassia Way, Suite B-112, Henderson, NV 89014.

Other Names: The Company also operates under the name "NumberVerifier." It has not previously used any other business names.

Common Ownership: The Company is a wholly owned subsidiary of The Blacklist Alliance, Ltd., and shares common ownership, management, directors, or control with the following entities: (1) Plura AI LLC; (2) Plura Connect LLC; and (3) Plura Holdings, LLC.

Call Chain Role: Pursuant to 47 C.F.R. § 64.6305(d)(4)(vi), (e)(4)(vi), and (f)(4)(vi), the Company's role in the call chain includes:

- A Voice Service Provider with a STIR/SHAKEN implementation obligation serving end-users; and
- A Non-Gateway Intermediate Provider with a STIR/SHAKEN obligation.

OCN: Pursuant to 47 C.F.R. § 64.6305(d)(4)(vii), the Company's OCN is 002L.

¹ This Revised Robocall Mitigation Plan replaces and supersedes any and all prior Verification Technologies Robocall Mitigation Plans filed with the Commission.

SECTION 2: CERTIFICATIONS

In submitting this RMP for filing, Verification Technologies certifies that:

- All calls originating on its network are subject to the protocols outlined in this version of the Company's RMP.
- During the past two years, neither the Company, nor The Blacklist Alliance, Ltd., Plura AI LLC, Plura Connect LLC, or Plura Holdings, LLC, have 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 description.
- Neither the Company nor affiliate thereof is a foreign voice service provider, nor does the Company or any affiliate thereof offer services to international call originators using North American Numbering Plan numbers.
- No prior robocall certification submitted by the Company has been removed by FCC action.
- The Company has not been prohibited from filing this RMP in the Robocall Mitigation Database (RMP).
- The Company has fully implemented the STIR/SHAKEN authentication framework in the IP portions of its network and complies with the STIR/SHAKEN requirements.
- The Company has not received or claimed any extension under 47 C.F.R. § 64.6304, as it has fully implemented STIR/SHAKEN.

Non-Gateway Intermediate Provider Certifications under 47 C.F.R. § 64.6305(f): In addition to its obligations as a voice service provider serving end-users, Verification Technologies certifies the following in its capacity as a non-gateway intermediate provider:

- All calls the Company carries or processes are subject to the robocall mitigation program described in this Robocall Mitigation Plan.
- The Company has implemented affirmative, effective measures to prevent its new and renewing non-gateway intermediate customers from using its network to carry or process illegal calls.

- The Company complies with the requirements of 47 C.F.R. § 64.6305(c) and (f), including accepting traffic only from upstream providers that maintain a valid Robocall Mitigation Database filing that has not been delisted by the Commission.

SECTION 3: ROBOCALL MITIGATION PLAN

The Company has adopted a robust RMP comprised of the following detailed practices that can reasonably be expected to significantly reduce the carrying, processing, or origination of illegal robocalls.

1. **STIR/SHAKEN Implementation.** The Company has fully implemented the STIR/SHAKEN authentication framework in the IP portions of its network and complies with the STIR/SHAKEN requirements. The Company uses the framework in furtherance of this RMP to: (i) authenticate and verify caller ID information for all calls originated on its network; and (ii) transmit authenticated caller ID information on all calls. The Company also regularly updates its STIR/SHAKEN implementation to comply with evolving standards.
2. **Call Analytics and Blocking.** All calls originating from the Company's network are analyzed internally and through third-party analytics vendors to identify and prevent illegal robocall traffic.
 - (a) **Internal Analytics Methodologies:** Verification Technologies' internal analysis methodologies includes monitoring real time call traffic patterns on its network to detect patterns indicative of potential illegal call traffic, such as high call volumes from a single source. Calls that exceed thresholds are flagged or blocked dynamically. The Company also utilizes AI-powered systems to analyze large datasets to detect patterns associated with robocalls, such as repetitive call attempts or known scam tactics. These automated detection methods are supplemented by intensive manual reviews of customer accounts that have been flagged as suspicious.
 - (b) **Third Party Analytics:** YouMail is known within the telecommunications industry for its analytics offerings and partners closely with the Industry Traceback Group (ITG), the FCC, and other law enforcement authorities. The Company utilizes YouMail's Watch service, a robust solution designed to detect and mitigate illegal robocall traffic and other harmful activities on carrier networks that leverages YouMail's extensive sensor network, including over 10 million active users and millions of "honeypot" numbers, to identify problematic call traffic.
3. **DNO Compliance.** Pursuant to 47 CFR § 64.1200(p), the Company utilizes the Somos RealNumber Do Not Originate (DNO) database to identify phone numbers marked as DNO, and blocks all numbers identified by Somos as invalid, unallocated, unused, or inbound-only government or private numbers. The Company also accesses real-time updates to the SOMOS DNO database to ensure call screening accuracy.

- (a) **Publicly Available Error Reporting Mechanism:** The Company has established a dedicated email address (blocking@verificationtechnologies.ai) to receive reports of erroneous blocking from customers and other voice service providers. This information is published on the Company's public-facing website, <https://www.verificationtechnologies.ai>.
4. **Caller ID/Number Verification Controls:** One of the primary mechanisms for illegal robocalls is caller ID spoofing—using numbers not assigned to the caller. To prevent this, Verification Technologies independently verifies that any existing numbers to be used by customers are actually assigned to them prior to account approval and only allows customers to acquire new numbers directly from the Company.
5. **Know Your Customer (KYC) Procedures.** In accordance with 47 C.F.R. §64.1200(n)(4), Verification Technologies has implemented robust, multi-tiered KYC procedures for all customers originating calls on its network to effectively identify customer entities and the individuals controlling them to prevent and mitigate potentially fraudulent or illegal activity.
- (a) **Prospective Customer Review and Assessment:** Each customer must first undergo an extensive vetting process before their new account can be approved. The prospective customer's business entity, along with the identity of the individual(s) applying for the account, are verified by the Company's in-house legal department. A business entity must have an Employer Identification Number (EIN) or equivalent tax ID (e.g., social security) and provide a verifiable physical location for its place of business.

Individuals and business entities associated with an account application may be further investigated by the Company's in-house legal department, which utilizes investigatory resources including WestLaw and LexisNexis to access official public records, business and fictitious name filings, domain registrations, and other records, to search for any official records that contradict the information provided by the prospective customer, or that might otherwise serve as a red flag.

Prospective customers must also provide a detailed description of how they intend to use the Company's services, anticipated monthly volume for each enabled service, and a detailed description of consumer contact data collection practices, including consent collection methodologies. In addition, each existing telephone number a customer desires to use with its account is independently verified by the Company to ensure it is actually assigned to that customer.

All information submitted in connection with the intended use case is viewed with an eye towards ensuring that the prospective customer will utilize Company services solely as an end-user in full compliance with applicable statutes, rules, and regulations.

- (b) **Certifications:** Each prospective customer is required to certify:

- (i) Whether the business entity or any of its owners or users have been subject to any prior enforcements or judgments for alleged illegal activity.
- (ii) That it has adopted internal compliance practices and procedures to ensure compliance with the Telephone Consumer Protection Act (TCPA), and any other applicable statute, rule, and regulation that applies to outbound calling and/or texting.
- (iii) That it will fully cooperate with the Company in connection with any traceback requests or internal investigations of suspicious activity.

(c) **Account Monitoring:** All approved and activated customer accounts are monitored on a regular ongoing basis for potentially unusual or suspicious usage, which may include:

- (i) ITG Traceback requests.
- (ii) Reports of alleged improper communications as flagged by YouMail, or reported by downstream service providers, the general public, or others.
- (iii) FCC and FTC consumer complaint data.
- (iv) Flagged numbers that customers are unwilling or unable to remediate.
- (v) Call traffic statistics, including short call duration percentage, average call duration, answer seizure ratio, etc. and
- (vi) Requests for high capacity (calls per second or concurrent calls), particularly if disproportionate to the size of the account.

(d) **Enforcement Framework.** The Company employs a graduated, documented enforcement framework that moves from detection of illegal traffic through remediation to resolution through the following steps:

(i) **Immediate Response (0-24 Hours)**

- Automated blocking of the specific traffic or number(s) identified as illegal, triggered by analytics flags, DNO list matches, or traceback notifications.
- Temporary suspension of the originating customer's account pending investigation.
- Preservation of call detail records (CDRs) and any associated metadata for the suspect traffic.
- Acknowledgment of any traceback request from the ITG, FCC, or law enforcement within the 24-hour traceback cooperation window

(ii) **Investigation (24-72 Hours)**

- **Root cause analysis:** Determine whether the illegal traffic originated from a direct customer, was passed through from an upstream provider, or resulted from a compromised account.
- **Customer contact:** Notify the account holder of the suspension, identify the specific traffic at issue, and request an explanation with supporting documentation (e.g., proof of consent, call campaign authorization).

- Upstream provider notification: If the traffic entered via an upstream provider, notify that provider and request its own investigation and remediation.
 - Downstream provider notification: If illegal traffic was transmitted to a downstream provider, notify that provider so they can take their own protective measures.
- (iii) **Remediation Decision**: Based on investigation findings, the Company will apply one of the following graduated outcomes:
- Reinstatement with corrective action: If the violation was minor, unintentional, and the customer demonstrates credible remediation (e.g., a consent process error that has been corrected), restore service subject to enhanced monitoring, reduced call volume caps, and a formal written warning.
 - Continued suspension with conditions: If the violation is significant but the customer cooperates and provides a credible compliance remediation plan, maintain suspension until the plan is implemented and independently verified.
 - Permanent termination: If the traffic was clearly fraudulent, the customer fails to cooperate, the customer cannot provide proof of consent or lawful authority, or the customer has any prior violation history
- (iv) **Documentation and Prevention**: Each of the above-referenced steps is documented and time-stamped. Following the remediation decision, the Company will conduct a post-incident review to determine whether analytics thresholds, KYC procedures, or contractual provisions need tightening to prevent similar incidents.
- (e) **Contractual Protections**. Among other restrictions, the Company's customers are required to adhere to the terms of its Acceptable Use Policy (AUP) which outlines an extensive but non-exhaustive list of prohibited conduct. The Company's customer agreements grant it the right to suspend or terminate service for any customer suspected of violating the AUP or otherwise using the Company's services in a suspicious manner, as determined by the Company in its sole discretion. When suspected violations of the AUP or other contractual provisions occur, the Company's legal department evaluates the violation and takes appropriate enforcement action.
6. **Traceback Cooperation**. Verification Technologies is committed to responding within 24 hours to all traceback requests from the Industry Traceback Group, law enforcement agencies, or the FCC. The Company will fully cooperate with these entities in investigating and stopping any customers that may be using its service to originate, carry, or process illegal robocalls.
7. **Know Your Upstream Provider (KYUP) Program**. In accordance with 47 C.F.R § 64.6305(g)(1), Verification Technologies only accepts calls directly from upstream providers that have filed a Robocall Mitigation Plan in the RMD, and that filing has not been de-listed pursuant to an enforcement action. To further minimize the likelihood of receiving illegal robocall traffic from an upstream provider, the Company:

- Only routes traffic using Tier 1 providers.
- Maintains a vetted list of approved upstream providers.
- Regularly monitors traffic patterns from each upstream provider.
- Implements traceback procedures to identify the source of suspicious traffic.

In addition to the operational measures described above, Verification Technologies conditions its relationships with upstream providers on written agreements that require such providers to: (i) maintain a current, accurate, and non-delisted Robocall Mitigation Database filing with the FCC; (ii) implement and enforce their own robocall mitigation and STIR/SHAKEN authentication programs consistent with applicable FCC rules; (iii) fully cooperate with the Company, the ITG, the FCC, and law enforcement in connection with traceback and related investigations, including timely provision of call records and other relevant information; and (iv) refrain from originating, carrying, or processing illegal robocalls or unlawfully spoofed traffic. These agreements expressly authorize the Company to immediately suspend or terminate the routing of traffic from any upstream provider that fails to meet these obligations or that is reasonably suspected of transmitting illegal or noncompliant traffic.

8. **Designated Officer and Employee Training.** To further ensure the Company's network is not utilized for the origination, termination, carrying, processing, or routing of unwanted and illegal robocalls, Verification Technologies has designated the following company officer to oversee all matters related to robocall mitigation and the implementation of this RMP.

Officer Name: Daniel McKeehan
Title: Chief Technology Officer
Department: Operations
Email: dan@verificationtechnologies.ai
Address: 177 Cassia Way, Suite B-112
Henderson, NV 89014
Phone: 702-291-8243

The aforementioned officer is also responsible for responding to traceback inquiries from the FCC, ITG, and law enforcement agencies, and for training employees to identify potential illegal robocall activity and implement the Company's robocall mitigation measures. Such training ensures that all relevant employees understand this RMP and the Company's obligations to prevent illegal robocalls.

9. **Regular Audits and Updates.** This RMP and the procedures outlined herein are regularly reviewed and audited to assess the effectiveness of current measures to prevent the origination, carrying, or processing of illegal robocalls, and identify areas for improvement. This includes a review of the third-party solutions providers used to implement the RMP. To

that end, additional solutions, new technologies, and best practices that may further contribute to the effectiveness of the Company's robocall mitigation efforts are reviewed, assessed, and (if warranted) adopted as they become available.

10. Compliance with FCC Rules. The Company certifies its compliance with all applicable FCC rules, including, without limitation:

- Annual recertification of its Robocall Mitigation Database filing.
- Updating any changes to company information, including entity name, contact name and title, address, email address, and taxpayer identification number, in CORES within 10 business days.
- Maintaining accurate and up-to-date information in the Robocall Mitigation Database.

OFFICER CERTIFICATION

Under penalty of perjury, the undersigned officer of Verification Technologies, LLC, does hereby certify that, to the best of his knowledge, the information set forth in this Revised Robocall Mitigation Plan is true and correct.

Daniel McKeehan

Daniel McKeehan

Chief Technology Officer