

ROBOCALL MITIGATION PROGRAM DESCRIPTION Arch Technologies ("Arch" or "Provider")

I. PROVIDER OVERVIEW

Arch Technologies ("Arch" or "Provider") is a competitive local exchange carrier (CLEC) that provides PSTN-enabled voice services to business and residential customers in New Hampshire and neighboring states using an IP-based VoIP network with interconnection to other carriers via SIP and, where necessary, TDM facilities.

Arch files this Robocall Mitigation Program Description pursuant to 47 C.F.R. § 64.6305 and the Federal Communications Commission's Public Notice DA 24-73 and related guidance. This description is intended to satisfy the requirement to upload a PDF robocall mitigation plan to the Robocall Mitigation Database and to describe, with particularity, the specific reasonable steps Arch takes to avoid originating, carrying, or processing illegal robocall traffic on its network.

Arch is certifying in the Robocall Mitigation Database as a domestic U.S. voice service provider with a STIR/SHAKEN implementation obligation serving end users. Arch also may function as an intermediate provider in certain call paths. For any call paths in which Arch receives a call directly from a foreign originating or foreign intermediate provider at its U.S.-based facilities and hands the call off to another U.S.-based provider, Arch will function as a gateway provider as defined in 47 C.F.R. § 64.6300, and apply this robocall mitigation program to that traffic. Any additional intermediate functionality is subject to the same or stricter mitigation controls described in this document.

Arch utilizes the services of third-party communications platforms, including Numbub and Infobip, to assist with number management, traffic routing, and traffic monitoring. These vendors operate under Arch's policies and direction, and Arch retains full responsibility for compliance with the Commission's robocall mitigation rules.

II. STIR/SHAKEN IMPLEMENTATION STATUS

Arch has implemented a robocall mitigation program consistent with 47 C.F.R. § 64.6305(d)(2). Arch's current caller ID authentication status is as follows:

1. IP traffic

Arch has deployed the STIR/SHAKEN caller ID authentication framework on the IP portions of its network. For calls that originate on or are handed off in SIP and for which Arch has sufficient information to determine the caller's identity and right to use the calling number, Arch authenticates and, where applicable, verifies calls in accordance with 47 C.F.R. § 64.6301 using appropriate attestation levels.

Where Arch uses platforms such as Numbub or Infobip for SIP trunking, numbering, or call origination/termination, Arch configures these services so that calls are authenticated and

passed with STIR/SHAKEN information where technically feasible and consistent with Arch's attestation policies.

2. Non-IP / legacy interconnection

For limited traffic that must traverse non-IP or legacy interconnection facilities that technically cannot support STIR/SHAKEN today, Arch relies on the applicable extensions under 47 C.F.R. § 64.6304. Arch is actively working with its interconnecting partners and vendors, including Numbub and Infobip where applicable, to complete migration to all-IP interconnection or to deploy alternative authentication solutions as they become available. All such traffic remains subject to the mitigation controls described in the sections below.

III. KNOW-YOUR-CUSTOMER (KYC) AND NEW / RENEWING CUSTOMER CONTROLS

Arch has implemented affirmative, effective measures to prevent new and renewing customers from originating illegal calls, consistent with 47 C.F.R. § 64.6305(d)(2)(ii) and 47 C.F.R. § 64.1200(n)(4). These measures apply to all customers that originate outbound traffic over Arch's network, including enterprise customers, contact centers, hosted PBX customers, and wholesale users.

1. Customer identity verification

- Arch requires prospective business customers to provide business formation documentation (such as articles of organization, corporate registration, or equivalent), a tax identification number, and government-issued identification for at least one responsible officer or principal.
- Arch verifies customer business information and tax identification through public and commercial databases to confirm that the entity is legitimate and in good standing.
- Arch collects and verifies physical address, billing address, and working contact telephone numbers and email addresses for responsible individuals.
- Arch screens prospective customers against internal risk lists and publicly available enforcement actions related to illegal robocalling, spoofing, or abusive telemarketing practices.

2. Use-case and traffic profile vetting

- As part of onboarding, Arch requires each prospective customer to describe its intended use of the service, including the nature of the business, the type of calls to be placed (transactional, informational, emergency, customer support, etc.), and whether outbound calls will be initiated using an automatic dialing system or platform.
- Arch reviews expected call volume, call patterns (including calls-per-second and calls-per-minute), mix of domestic and international destinations, average call duration, and typical time-of-day calling behavior to identify potentially high-risk profiles.
- High-volume outbound callers (such as call centers, dialing platforms, and notification services) are subject to enhanced due diligence, which may include additional questionnaires, review of the customer's consent and opt-out procedures, and references or documentation demonstrating legitimate calling practices.

3. Numbering and caller ID controls

- Arch assigns telephone numbers only after determining the customer's legitimate need for the quantity and type of numbers requested, taking into account the size of the customer, the scope of operations, and the anticipated calling profile.
- Where Numbub or Infobip are used for number provisioning and management, Arch configures and controls these services to ensure numbers are allocated in line with Arch's policies and regulatory requirements.
- Arch prohibits customers from manipulating caller ID information in a manner that is inaccurate or misleading. Customers may only present numbers that they control or are authorized to use.
- Arch enforces policies requiring accurate display of caller identity consistent with the Truth in Caller ID Act and the Commission's rules, subject to lawful caller privacy and blocking options.
- Arch employs controls to prevent assignment or use of numbers that are known to be invalid, unallocated, or present on internal do-not-originate (DNO) lists.

4. Contractual prohibitions and enforcement rights

- Arch's service agreements expressly prohibit customers from using the service to originate illegal robocalls, including calls that violate the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, the TRACED Act, and other applicable federal or state telemarketing and consumer protection laws.
- Customers must maintain their own compliant practices for consent, do-not-call processing, internal opt-out list maintenance, and recordkeeping, and must certify that they will do so upon request.
- Arch reserves the right to suspend or terminate service immediately upon evidence that a customer is originating illegal or abusive traffic, upon repeated tracebacks or investigations implicating the customer, or upon a customer's failure to cooperate with Arch's mitigation or traceback efforts.
- Arch's agreements include indemnification provisions placing responsibility on customers for regulatory penalties, damages, and other costs arising from their illegal or non-compliant calling activity.

5. Ongoing review of existing customers

- Arch periodically reviews existing customers, with heightened focus on high-volume dialers and customers whose calling patterns change significantly over time.
- Arch may request updated information about a customer's calling practices, consent mechanisms, opt-out process, and compliance controls when analytics indicate elevated risk or when tracebacks implicate that customer's traffic.
- Arch may impose additional controls on existing customers, such as stricter rate limits, narrower access to numbering resources, or enhanced monitoring, where doing so is necessary to mitigate risk.

IV. KNOW-YOUR-UPSTREAM PROVIDER PRACTICES

To the extent Arch receives traffic from upstream providers (including wholesale carriers and intermediate providers), Arch takes reasonable and effective steps to know its upstream providers, consistent with 47 C.F.R. § 64.6305(d)(2)(ii) and 47 C.F.R. § 64.1200(n)(5).

1. Upstream provider due diligence
 - Arch accepts traffic only from upstream providers that are listed as active entries in the Robocall Mitigation Database and that have not been de-listed or publicly identified by the Commission as non-compliant.
 - Arch verifies the identity, corporate status, and regulatory standing of each upstream provider and determines its role in the call chain (voice service provider, gateway provider, or non-gateway intermediate provider).
2. Contractual requirements for upstream providers
 - Arch's interconnection and wholesale agreements require upstream providers to maintain their own compliant robocall mitigation programs and to remain listed in the Robocall Mitigation Database with an up-to-date, non-deficient filing.
 - Upstream providers must agree to take reasonable steps to avoid transmitting illegal robocalls and to cooperate fully with Arch, the Commission, law enforcement, and the registered industry traceback consortium.
 - Arch retains contractual rights to restrict, block, or discontinue traffic from upstream providers that fail to maintain a valid Robocall Mitigation Database filing, that are subject to blocking obligations by Commission order, or that are repeatedly associated with illegal or abusive traffic.
3. Monitoring of upstream traffic
 - Arch applies call analytics (described below) to traffic it receives from upstream providers and monitors for calling patterns consistent with illegal robocalling, such as extremely high volumes of short-duration calls, unusual spikes to particular destinations, or calls to invalid or DNO numbers.
 - When Arch's analytics identify potentially problematic traffic associated with a particular upstream provider, Arch may:
 - Request additional information from the upstream provider about the source and purpose of the traffic;
 - Require that the upstream provider implement specific mitigation or blocking steps;
 - Apply rate limits, number-range blocking, or other technical controls; and
 - In serious cases, block specific traffic or terminate the relationship with the upstream provider.

V. CALL ANALYTICS, TRAFFIC MONITORING, AND BLOCKING PRACTICES

Arch employs call analytics and traffic-monitoring tools, using both internal systems and, where appropriate, third-party solutions, to identify and mitigate suspected illegal robocalls consistent with 47 C.F.R. § 64.6305(d)(2)(ii) and DA 24-73.

Arch utilizes capabilities available through platforms such as Numbub and Infobip, including number intelligence, traffic analysis, and reputation or fraud-detection features, and combines them with Arch's own policies and monitoring.

1. Analytics systems

- Arch's internal analytics platform monitors call volume per customer, per trunk group, and per calling number; average call duration and the distribution of call lengths; calls-per-second and calls-per-minute; answer rates; and destination profiles (including domestic vs. international traffic).
- Arch compares current traffic against historical baselines to identify anomalies such as sudden spikes, new calling destinations, or unusual time-of-day patterns.
- Where appropriate, Arch relies on third-party analytics and reputation tools provided by vendors such as Numbub and Infobip. These may include:
 - Number reputation and risk scoring;
 - Detection of calls to invalid, unassigned, or high-risk ranges;
 - Identification of patterns associated with robocall campaigns and fraud.

2. Detection of suspicious traffic

Arch configures rules and thresholds to flag traffic indicative of illegal or abusive robocalling, including:

- Extremely high volumes of short-duration calls;
- High calls-per-second or calls-per-minute relative to historical norms;
- Significant traffic to invalid, unassigned, or do-not-originate (DNO) numbers;
- Repeated calling to the same number or tight number ranges in rapid succession;
- Calling patterns consistent with caller ID spoofing or snowshoe-style campaigns; and
- Traffic that receives elevated risk or negative reputation indicators from Numbub, Infobip, or other third-party sources.

Alerts generated by analytics tools are reviewed by Arch's fraud, security, or compliance personnel, who may investigate traffic further, contact the customer or upstream provider, and implement mitigation measures.

3. Blocking and mitigation actions

- Arch may block or restrict traffic that has been identified as highly likely to be illegal or abusive, in accordance with the Commission's rules governing reasonable network management and call blocking.
- Mitigation actions may include:
 - Temporarily or permanently reducing allowed call rates for a customer, trunk group, or upstream provider;
 - Blocking specific calling campaigns, number ranges, or destinations;
 - Requiring customers to modify their campaigns, scrub calling lists, or strengthen consent and opt-out processes;

- Using configurable controls offered by Numbub, Infobip, or other vendors (such as rate limits, blocking rules, or number-range protections) to enforce Arch's mitigation policies; and
 - Suspending or terminating service to customers that originate illegal robocalls or refuse to cooperate with mitigation efforts.
- Arch seeks to ensure that blocking is narrowly tailored and periodically reviews blocking decisions to reduce the risk of inadvertently blocking lawful traffic.

VI. TRACEBACK COOPERATION

Arch commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the registered industry traceback consortium, consistent with 47 C.F.R. § 64.6305(d)(2)(iii).

1. Designated point of contact
 - Arch designates a robocall mitigation and traceback point of contact whose name, title, department, business address, telephone number, and email address are provided in the Robocall Mitigation Database filing.
 - This point of contact is responsible for receiving traceback and mitigation-related requests, coordinating internal investigations, and ensuring timely responses.
2. Traceback procedures
 - Upon receipt of a traceback request, Arch promptly identifies the relevant traffic in its call detail records and network logs, including any traffic routed or managed through Numbub, Infobip, or other third-party platforms.
 - Arch determines the originating customer or upstream provider associated with the identified call(s), collects relevant call records and any associated information (subject to applicable privacy and contractual obligations), and responds to the traceback consortium or requesting authority, generally within 24 hours.
 - When tracebacks indicate that a particular customer or upstream provider is a likely source of illegal robocalls, Arch uses its contractual and technical tools, including suspension, blocking, or termination of service, to mitigate and, where possible, stop future illegal traffic.

VII. ENFORCEMENT HISTORY AND REGULATORY ACTIONS

Pursuant to 47 C.F.R. § 64.6305(d)(2)(iv), Arch states as follows concerning whether it or any entity with common ownership, management, directors, or control has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation in the prior two years related to illegal robocalls, spoofing, or robocall mitigation database deficiencies.

As of the date of this document, Arch is not aware of any formal Commission, law enforcement, or other regulatory agency action or investigation commenced within the prior two years, by written notice or equivalent instrument, that contains findings or formal allegations of

wrongdoing by Arch relating to illegal robocalls, spoofing, or deficient Robocall Mitigation Database certifications or mitigation plans.

If this status changes, Arch will update its Robocall Mitigation Database filing and, if necessary, this program description, within the time required by the Commission's rules.

VIII. PROGRAM GOVERNANCE, REVIEW, AND UPDATES

Arch recognizes that robocall mitigation is an ongoing compliance obligation that must adapt to evolving calling patterns, emerging enforcement priorities, and changes in Commission rules and industry best practices. To that end:

- Arch designates internal personnel responsible for oversight of the robocall mitigation program, including representatives from network operations, security/fraud, vendor management, and regulatory compliance.
- Arch reviews this robocall mitigation program at least annually, and more frequently as needed, and updates its policies, analytics rules, and contractual templates to reflect new threats, regulatory guidance, and capabilities offered by Numbub, Infobip, and other vendors.
- Arch trains relevant staff involved in customer onboarding, network operations, vendor management, and fraud and compliance functions on this program and on the company's robocall mitigation responsibilities.
- Arch will update its Robocall Mitigation Database filing, including this program description where material, within 10 business days of any material change to its STIR/SHAKEN implementation status, mitigation practices, role in the call chain, or identification and contact information, consistent with 47 C.F.R. § 64.6305(d)(5).

IX. CONCLUSION

Through the combination of:

1. Robust know-your-customer controls;
2. Know-your-upstream provider diligence;
3. Careful assignment and monitoring of numbering resources and caller ID;
4. Active analytics-based traffic monitoring and blocking, including through services provided by Numbub and Infobip; and
5. Prompt cooperation with traceback and enforcement entities,

Arch has implemented reasonable and effective steps designed to significantly reduce the origination and transmission of illegal robocalls over its network, as required by the Commission's robocall mitigation rules.

This Robocall Mitigation Program Description is accurate to the best of Arch's knowledge as of the date below and reflects the policies and procedures that Arch has implemented and enforces in the ordinary course of its operations.

Arch Technologies

Name: Lewis Arch

Title: Owner/Operator

Date: 12/01/2025