

INCOGNITO IT, LLC

Robocall Mitigation Program Description | October 14, 2026

Provider: Incognito IT, LLC

Business address: 8350 W Grandridge Blvd, Ste 200, Kennewick, WA 99336

Responsible officer: Justin Bazinet, Owner & Managing Member

Traceback and abuse contact: Help@IncognitoIT.com | (509) 343-3775

1. Service Description and Role in Call Chain

Incognito IT, LLC provides managed, interconnected hosted Voice over Internet Protocol (VoIP) telephone service to business end users in Washington and Oregon. Customers use a centralized VitalPBX platform operated and administered by Incognito IT. Incognito IT obtains public switched telephone network (PSTN) access from a wholesale SIP carrier and bills its business customers directly for hosted telephone service on a per-seat basis. Customers use the service for ordinary business communications; Incognito IT does not offer automated bulk-calling, predictive-dialing, or prerecorded telemarketing campaign services.

2. Customer Due Diligence and Contractual Restrictions

Before provisioning service, Incognito IT collects the customer's business name, physical business address, authorized primary contact, billing information, and three trade references. These records support identification of the business responsible for calls placed through the service. Incognito IT maintains customer account records and supplies service to identified business customers rather than anonymous users.

Customer service agreements and written terms prohibit illegal robocalls, spam, fraudulent telephone use, and unauthorized caller-ID spoofing. Incognito IT retains contractual authority to suspend or terminate service immediately when suspected illegal calling or fraud is identified.

3. Caller ID and Calling Restrictions

Incognito IT limits each customer's outbound caller ID to telephone numbers authorized for that customer, including the customer's assigned direct inward dialing (DID) numbers. Customers may not present arbitrary unrelated telephone numbers as outbound caller ID. Outbound dialing is restricted to United States destinations; international dialing is not permitted. Each user is limited to two concurrent channels. These restrictions reduce exposure to fraudulent number presentation and uncontrolled calling.

4. Platform Security and Customer Isolation

The centralized VitalPBX deployment employs firewalls, Fail2Ban, IP access restrictions, strong SIP credentials, and logical separation of customer accounts and calling resources. Incognito IT maintains administrative control of these measures and can disable affected user extensions or customer outbound calling independently of other customers.

5. Traffic Analytics, Monitoring, and Intervention

Incognito IT uses a call-detail-record (CDR) analysis platform and automated call-volume monitoring to detect anomalous or potentially fraudulent traffic. Monitoring focuses on irregular calling volumes and calling patterns revealed by the records. When suspicious behavior is detected, personnel can review the relevant CDRs, determine the originating customer and extension, and promptly restrict or disable that customer's outbound calling or specific extensions. The company can coordinate investigations with its wholesale provider and apply contractual suspension or termination remedies.

Incognito IT retains CDRs for 90 days and can retrieve originating extension, called number, timestamp, and outbound carrier or SIP trunk for individual calls. These records support internal investigations, corrective actions, and traceback

responses. Automated analytics assist detection; service restrictions and suspensions are applied through operational controls.

6. Wholesale Carrier Coordination and Call Authentication

Incognito IT uses wholesale SIP connectivity for PSTN service and coordinates suspected calling abuse, network investigation, and relevant call records with the upstream provider. BulkVS is the company's intended sole wholesale provider. BulkVS has confirmed that it will sign outbound calls routed through its service using STIR/SHAKEN. Incognito IT remains responsible for its customer identification, caller-ID restrictions, traffic monitoring, response to suspected abuse, and cooperation with traceback requests. The company's independent STIR/SHAKEN regulatory obligations and implementation status are addressed through its separate FCC certification.

7. Complaint Handling and Enforcement

Upon receipt of a credible complaint, fraud alert, or suspicious-traffic finding, Incognito IT reviews the relevant calling records and customer information, determines the scope of the affected activity, and may immediately restrict the affected extension or customer's outbound service to prevent additional suspicious calling. The company may preserve pertinent records, coordinate with its wholesale provider, respond to appropriate investigative requests, and suspend or terminate service as permitted by its customer agreements.

8. Traceback and Regulatory Cooperation

Incognito IT will respond fully within 24 hours to traceback requests from the Federal Communications Commission, civil or criminal law enforcement, and the industry traceback consortium. It will cooperate in investigating and stopping entities using its service to originate illegal calls. Requests may be delivered to **Help@IncognitoIT.com** or **(509) 343-3775**. Justin Bazinet, Owner & Managing Member, oversees response and escalation. For a request involving its traffic, the company can identify the originating customer and extension, called destination, time, and wholesale route from available call records; it will provide responsive information as legally appropriate, coordinate with the provider as necessary, and restrict suspect calling when warranted.

9. Compliance Oversight and Program Updates

Justin Bazinet, Owner & Managing Member, oversees administration of this program, periodic review of its effectiveness, investigation and documentation of detected incidents, and maintenance of FCC filing information. The company will review its protective measures as service arrangements and risks change. Incognito IT reports that neither it nor its owners have been subject to an FCC or other regulatory investigation or enforcement action involving illegal robocalls, caller-ID spoofing, or telecommunications fraud in the preceding two years.

10. Adoption

This program applies to voice traffic originating through the Incognito IT managed hosted telephone system. Incognito IT implements the business controls and mitigation procedures described above and will cooperate with applicable federal and industry traceback and enforcement processes.

Responsible officer: Justin Bazinet, Owner & Managing Member

Effective date: October 14, 2026