

Compliance Policies & Mitigation Plan under law and rules of:

Telephone Consumer Protection Act - 47 U.S.C. § 227 et. seq.: Telephone Robocall Abuse Criminal Enforcement and Deterrence Act of 2019(Pallone-Thune TRACED Act), as amended; Do-Not-Call Implementation Act of 2003 – 15 U.S.C § 6101 et. seq.

REVISED AND ADOPTED BY

Dorial Telecom LLC

801 BRICKELL AVE SUITE 800 MIAMI FL 33131-2979



CORES/FRN:	0034607606
FCC 499-A ID:	827369¹
RMD No.:	0012192²

REVISED AUGUST 6, 2026

EFFECTIVE DATE: AUGUST 6, 2026

¹ <https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=827369>

² https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robotcall_mitigation_data&sys_id=7913c5801bb199105e240f6fe54bcbd2&view=sp

LIMITATIONS IN SCOPE OF SERVICE

Dorial Telecom LLC (“Dorial”) is a competitive small sized provider of domestic services, specifically interstate call routing termination and resale within the U.S. Dorial Telecom has a wholesale VoIP routing line of business that focuses on interstate domestic calls within the United State. Dorial provides no Gateway, call origination or the last provider of call termination services in its intermediate call routing line of business. Effective with this Rev. 4.0 policy, Dorial has commenced a separate DID/ANI numbering resale line of business, under which Dorial acquires and resells U.S. Direct Inward Dialing numbers and associated Automatic Number Identification resources, with U.S. termination, to other communications and telecommunications providers and to end users. This numbering resale line places Dorial in an origination-adjacent regulatory role distinct from its intermediate routing business, as described in Section 14 below, and is governed by that Section in addition to the general provisions of this policy. This policy is applicable to the business were it acts as a domestic intermediate voice service provider.

NOTE: The reasonable measures undertaken by Dorial on particular calls are performed in real time vs based upon information that comes to the attention of Dorial through the FCC’s delegated ITG Consortium, the federal Do Not Call Registry of the FTC, to the extent required, Numbers that do not correspond as duly authorized by the North American Numbering Plan, Spoofed numbers of an agency or law enforcement agency to which a subpoena had been issued, and other Providers that have received Traceback requests and have informed Dorial Telecom as an intermediate provider in the call path. This policy details and supplements those reasonable measures.

DORIAL’S PARTICULAR VOICE SERVICES.

Dorial Telecom, LLC (Dorial) is an Intermediate IP-Enabled Voice Communications Provider that resells and re-transmits calls in mid-call path from originating call provider to terminating call provider. Dorial maintains no media boards in its operation of IP-Enabled voice call resale. It functions as a routing service between providers. It receives signaling from its customers of their requests to terminate calls and accepts call termination based upon a least cost routing (LCR) basis. Dorial’s customers ultimately

choose to terminate calls through Dorial based upon the LCR to any given destination based upon rates. Dorial obtains those rates through dealings with other IP-Enabled Voice Intermediate Providers, CLECs, ILECs or wireless/common carriers of scale or dominance. Dorial possesses no, and does not use, media boards within its networks to have access to call content. When providing resale traffic, Dorial does not originate or terminate calls into the call stream to have full view of the call path or purpose. Indication of a violative robocall is thus limited in the position that Dorial exists in the call path and transmission information alone may not be enough to make a reasonable real time determination without further verifiable secondary sources.

All U.S. IP-Enabled Voice providers that Dorial has dealings with are registered with the FCC under Blanket Authority to provide U.S. domestic long-distance services and/or interstate call termination through registration with the FCC: FRN (CORES ID) and FCC Form 499-A ID. It reports as an Other Toll telecommunication service because of its routing function. Both registrations are verified on an annual basis by Dorial with information found through the FCC's public information website and databases. This is done in the regular practice of business of Dorial to verify regulatory fee status and exemption(s) but is kept as record for other compliance purposes as well. This includes Intermediate Provider Registry registration. For all domestic IP-Enabled Voice provider Customers, Dorial requires that these providers be: 1.) Registered on the FCC Robocall Mitigation Database (as confirmed from the public portal at https://fccprod.servicenowservices.com/rmd/?id=rmd_listings; and/or, 2) Registered with FRN (CORES ID) and FCC Form 499-A ID, for all Domestic Providers. In addition, Dorial requires all its Customers, Domestic and International to fill up yearly the FUSF (Federal Universal Service Fund) Certificate pertaining to their status. This is a baseline of information that Dorial keeps with its customers and transmitting providers, regardless of the procedures and protocols established herein. This plan is implemented to specifically establish more reasonable methods and compliance with the following laws and rules. This plan may be amended from time to time.

Pursuant to Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and

Deterrence Act, Pub. L. No. 116-105 (2019) (TRACED Act), and Rules of the Federal Communications Commission (FCC) on call authentication framework and anti-Spoofing rules collectively known as STIR/SHAKEN under 47 C.F.R. § 64.6301 et. seq, and 47 C.F.R. § 64.6305 et. seq., the following Plan is hereby authorized as of this date and effective by June 1, 2025.

Dorial Telecom blocks short duration call traffic called numbers to numbers on the FTC DNC and FCC DNO Registries that have indication of illegal robocalls. For short duration call traffic from foreign origination to U.S. called numbers NOT on the FTC DNC Registry, Dorial Telecom must rely on verifiable secondary sources for transmission purposes. This may include but is not limited to traceback requests indicating a prior fraudulent purpose call (attempt to criminally defraud a called party of property or money with intent or by fraudulent means including threat, theft, or impersonation) from the originating number, Know Your Client Information it retains or other information to the same effect from law enforcement agencies indicating fraudulent purpose calls, be it an individual call or calls in mass.

The policies and protocols established by this policy to block unlawful or illegal robocalls weigh into consideration the reasonable information available, from transmission information and verifiable secondary sources at any given period. The policies and protocols established by this policy weigh into consideration adopted Rules by the FCC over Intermediate Voice Providers.

TABLE OF CONTENTS

1	LIMITATIONS IN SCOPE OF SERVICE	2
2	PARTICULAR VOICE SERVICES	2
	TABLE OF CONTENTS	5
3	MITIGATION OF FRAUDULENT CALLS.....	6
	A. SPOOFED CALLS	6
	B. FRAUDULENT CALLS	6
	C. TOLERANCE LEVELS.....	7
4	DNC/TCPA VIOLATIONS	7
5	RELIANCE ON FCC ITG CONSORTIUM FOR CORRECTNESS	8
6	KNOW YOUR CLIENT (KYC) INFORMATION RETAINED	8
7	KNOW YOUR CLIENT (KYC) INFORMATION RETAINED.	
8	STIR/SHAKEN COMPLIANCE	9
9	TRACEBACK TOKENS	
10	IP MANDATE.....	13
11	PROOF OF IMPLEMENTATION	13
12	SUSPENSION & ERMINATION OF CUSTOMER	15
13	OTHER FRAUD DETERRENCE TOOLS	15
	A. STIR/SHAKEN AUTHENTICATION POLICY IN COMBINATION WITH OTHER DETERRENCE	15
	B. ATTESTATION REQUIREMENTS BY DORIAL	15
	C. FRAUD AND TCPA COMPLIANCE FILTERING.....	16
	D. IMPLEMENTATION STANDARDS AND FLEXIBILITY TO TARGET BLOCKING WITH FRAUD FILTERS	17
	E. MANUAL INTERVENTION AND MANAGEMENT	18
14	DID/ANI NUMBERING RESALE COMPLIANCE PROGRAM	19

ADOPTED POLICY:

The policies and protocols established by this policy to block calls weigh into consideration the reasonable information available, from transmission information and verifiable secondary sources at any given period.

3. MITIGATION OF FRAUDULENT CALLS

Dorial is registered with the FCC Robocalling Mitigation Database at https://fccprod.servicenowservices.com/rmd/?id=rmd_listings. Dorial requires all suppliers or customers to be registered with the FCC Robocalling Mitigation Database and timely responsive to all Industry Traceback Group Consortium requests (ITG Traceback Requests) either passed by Dorial Telecom in response to a complaint or ITG Traceback Requests revived directly that come to the knowledge of Dorial. Dorial's target response time for ITG Traceback Requests is same day or no less than 24 hours if practicable based on the timing of the receipt of the request.

A. Federal TRACED Act Compliance. Dorial reserves the right to block or suspend traffic of any customer for Fraudulent Robocalls which at a minimum includes discovery of:

- 1. SPOOFED CALLS.** Dorial does not interfere or modify caller information, including ANI, it receives in the call path. Dorial does not strip ANIs for termination purposes. As of this Rev. 4.0 policy, Dorial procures and resells U.S. DID/ANI numbering resources acquired from regional CLECs, I-VoIP providers, and major carriers, subject to the sourcing verification, KYC, and attestation methodology requirements of Section 14 below; this routing-line description otherwise continues to apply to Dorial's intermediate call transport business. Where and when Dorial encounters an originating calling number not verifiable with the North American Numbering Plan, or an interstate call that purports to originate from 911 or law enforcement or has been reported as spoofed by a prior ITG Traceback Request, then the number will be deemed by Dorial as Spoofed and shall be blocked. Dorial relies on definition of Spoofed Calls under the Act and interpretations of the FCC.

2. **FRAUDULENT CALLS.** A fraudulent Robocall made through an automated telephone dialing system (ADTS) or similarly used software whose caller seeks to defraud the called party at the called number by misrepresentation or fraudulent means of any money, property or attempts steal or misuse personal information to defraud them or otherwise steal their identity for fraudulent purposes whether successful call connection is made or not. (Common fraudulent, but not all inclusive, schemes that fit this definition are: Unlawfully portraying themselves as a government or law enforcement agency demanding money or requesting government issued ID numbers, using the threat of kidnapping, jail or personal or financial harm to defraud the called party, Portraying themselves as an e-commerce or other online business with a debt or credit when neither is the circumstance, or otherwise using a fraudulent intent and guise to obtain anything of tangible or intangible value to which they do not have a right or power to obtain.) Notice of such fraudulent Robocalls will be based on notice to Dorial Telecom by called party complaint or Traceback request documenting the scheme and fraud. Where and when Dorial encounters a fraudulent call then the call will be blocked.
3. **TOLERANCE LEVELS.** The following tolerance levels of transmitted fraudulent Robocalls received or noticed to Dorial Telecom:
- Dorial Telecom has a low tolerance for fraudulent Robocalls (as they are fraudulent calls).
- If two (2) or less Fraudulent Robocall ITG Traceback Requests are received by Dorial in connection with a particular provider/customer within a 48-hour period for a calling number transmitted by the provider, A Fair Warning Letter will be sent to the Provider to investigate and mitigate such violative calls, or Dorial will suspend or terminate the account.
 - If two (2) or more Fraudulent Robocall ITG Traceback Requests are received by Dorial from a provider/customer within a 48-hour period for a calling number transmitted by the provider, the Provider's account will be automatically suspended and further written assurances of fraudulent Robocall mitigation complaint are given and verified before account released from suspension of account by Dorial. Dorial shall reasonably refuse termination until such time from the provider/customer.

- If a Fair Warning Letter is sent to Provider by Dorial Telecom, depending upon circumstances and nature of the Traceback or the ITG's request, regarding fraudulent Robocalls and within three (3) days another Fraudulent Robocall ITG Traceback Requests is received by Dorial Telecom for the Provider/Customer, the Provider's account will be suspended and further assurances of fraudulent Robocall mitigation will be requested and verified before account released from suspension.
 - If Fraudulent Robocall ITG Traceback Requests are received belated by ITG while Provider's account is suspended, the Provider's Account will be closed immediately.
 - If five (5) Fraudulent Robocall ITG Traceback Requests are received for the Provider at any time within a 30-day period, the Provider's Account will be closed immediately.
 - If six (6) or more Fraudulent Robocall Tracebacks are received for the Provider at any time within a 60-day period, the Provider's Account will be closed immediately.
 - If Dorial Telecom receives notice from to Industry Traceback Group Consortium that Provider is refusing to respond to a Fraudulent Robocall Traceback to them in connection with a call passed to Dorial Telecom, the Provider's account will be suspended and further assurances of fraudulent Robocall mitigation will be requested and verified before account released from suspension.
4. **DNC/TCPA VIOLATIONS.** It is the policy of Dorial to block all repetitive short duration call traffic to numbers on the FTC DNC Registry. This is integrated into automatic Robocall Filtering systems Dorial has implemented. See, **OTHER FRAUD DETERRENCE TOOLS** in these policies for systems and protocol. Dorial updates its database with the FTC DNC Registry in 30-day cycles. As for TCPA violations, Dorial cannot reasonably predict violations of expressed written consent not being lawfully obtained because that is a factual issue between the caller and the called party prior to the calling party making the call. Dorial will reasonably respond to information of TCPA violations given through ITG Traceback Request indicating a TCPA violation and take

appropriate action. Dorial shall rely on the ITG Traceback Consortium, as the FCC's authorized delegated agent through the TRACED Act, for correctness and legitimacy of claims and complaints of consumers. Upon reasonable information that is verified through a third party, such as ITG Traceback Consortium as the FCC's authorized delegated agent through the TRACED Act, Dorial shall block TCPA violative calls from a provider and escalate low tolerance levels with that provider as if the calls were fraudulent.

5. **RELIANCE ON FCC ITG CONSORTIUM FOR CORRECTNESS.** ITG Traceback Consortium as the FCC's authorized delegated agent through the TRACED Act is empowered by the FCC to verify consumer complaints of fraud and DNC/TCPA violations. As this power is a delegated authority under the TRACED Act, Dorial shall reasonably rely on the correctness, accuracy, and legitimacy of the Consortium's investigation of the underlying consumer complaint. If in fact the Consortium acted in this role based upon error or omission, Dorial relies upon safe harbor exemptions under FCC Orders of July 17, 2022.

6. **KNOW YOUR CLIENT (KYC) INFORMATION RETAINED.** Dorial collects and maintain KYC information prior to contracting and engagement by a customer:

- Full legal name and any *d/b/a*, tradename(s)/service marks, or trade names of the company (be they registered or at common law)
- State or nation of incorporation
- Information on owners, management, and affiliates to ensure nationality and that business is not alter ego for a dubious foreign provider.
- Licenses held to provide service and by which regulatory authorities.
- FCC FRN (CORES ID) & FCC 499-A Filer ID
- Proof of registration on FCC Robocalling Mitigation Database
- TOKENs for STIR/SHAKEN purposes used.
- History of any notices or settlement of robocall/DNC violations with FCC, FTC, or any state Attorney Generals.

- If customer services any providers originating or transmitting traffic for call centers, call shops, or telemarketers (Calls or SMS text message campaigns)
- If TRACEBACK policy or protocols have been established by the customer under Robocall mitigation plans.
- TRACEBACK history or volumes of traceback requests (as HOP or otherwise) in past 6 months.
- Typical TRACEBACK response time.

Dorial further collects and maintains KYC information after contracting and engagement by a customer or supplier, which includes:

- Owner name and contact information.
- Time Zone of NOC or accessibility by customer's staff to respond to TRACEBACKS.
- Contact information of technical staff.
- Geographical, city and local location of network (if physical or virtual)

In furtherance of collecting, keeping, and referencing the above information, Dorial has developed a KYC form based upon FCC Rules and Industry information updates. Record retention is ongoing after termination of a client. KYC Forms are updated annually, or semi-annually if needed.

7. **STIR/SHAKEN COMPLIANCE.** Dorial is a Communications Provider under 47 C.F.R. § 4.3 (b). Pursuant to Pallone- Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116- 105 (2019) (TRACED Act), the Federal Communications Commission (FCC) has issued certain rules requiring that communications providers to implement call authentication framework and other robocall mitigation practices collectively known as STIR/SHAKEN. See, 47 C.F.R. § 64.6301 et. seq, and 47 C.F.R. § 64.6305 et. seq. The STIR/SHAKEN framework allows voice service providers to verify that the caller ID information transmitted with a particular call matches the caller's number, while protecting consumer privacy and promoting the ability to complete lawful calls.

STIR/SHAKEN is an industry-developed framework designed to allow communications service providers to distinguish legitimate calls from illegally spoofed calls so that they can take steps to mitigate the illegal calls. STIR/SHAKEN utilizes an encrypted authentication and verification process that establishes a chain of trust between the calling party and the called party. Specifically, the originating carrier (or the earliest carrier in a call chain with authority) is responsible for authenticating calls by “signing” them with an encrypted digital signature and one of three attestations for the callers’ identity: (i) A (or “full”) attestation means the provider can confirm the identity of the caller and the legitimate use of the calling number; (ii) B (or “partial”) attestation means the provider can confirm the identity of the caller but not the telephone number; and (iii) C (or “gateway”) attestations means the provider is the point of entry to the IP network for a call that originated elsewhere, such as a call that originated abroad or on a domestic network that is not STIR/SHAKEN-enabled. When the terminating provider receives a call for delivery to an end user, it is responsible for verifying the call using a verification service and for determining how to treat the call, such as by allowing trusted calls to pass to the called party, showing the called party a warning that the call may be illegitimate, or blocking the call if the provider believes the call is illegal. STIR/SHAKEN only works on Internet protocol (IP) networks. FCC Rules require communication providers and “voice service providers” to implement STIR/SHAKEN in the IP portions of their network. DORIAL is such a provider as an intermediate carrier. For compliance purposes, Dorial provides attestation level A and occasionally gateway attestation B within the framework.

A “voice service” is broadly defined as any service that is interconnected with the public switched telephone network (PSTN) and that uses numbers from the North American Numbering Plan (NANP). It includes all common carrier voice providers, interconnected Voice over Internet Protocol (VoIP) providers, one-way VoIP services, fax transmissions and services, and over-the-top voice services (e.g., Skype, Google Voice).

A communications service provider’s obligations will vary depending upon the role that it serves for particular calls, or even whether it is the provider of voice service on a particular call. Therefore, providers should examine their services closely to determine the extent to

which the provider offers voice service on the call. The following supports the Certifications made.

The obligations of a voice service provider depend on where the provider is in the Call Path for a particular call, these are:

- *Originating* providers must: (a) authenticate and verify SIP calls originated and terminated on their networks, and (b) authenticate SIP calls it will exchange with other voice service providers.
- *Intermediate* providers must: (a) pass authentication information to the next provider in the chain unaltered, and (b) authenticate un-signed calls (subject to certain exceptions). We understand that intermediaries are not mandated to check databases or validate upstream/downstream partner traffic at this time.
- *Terminating* providers must verify SIP calls they receive from other providers for termination to the end user.

Dorial is an Intermediate provider/carrier that supplies wholesale services to retail carriers. Dorial DOES NOT Originate or Terminate calls. Per the STIR/SHAKEN Rules and framework, voice services provider definition, an individual service provider could serve separate roles for different calls. Thus, a provider may have originating provider obligations for some calls, intermediate provider obligations for others and terminating provider obligations for others. Service providers must be prepared to comply with all these obligations in their IP networks. Dorial has implemented protocols for all such scenarios. As a result, Dorial SHALL NOT modify or otherwise add or subtract from any IP Header received ANY information to prevent traceback request information as to the origin or termination of the calls it receives.

8. **TRACEBACK Tokens.** Before a provider can begin authenticating or verifying calls, it must obtain a certificate from the certificate authority designated by the FCC. This first involves obtaining a Service Provider Code (SPC) token from the FCC's selected governance authority, which indicates that the provider is qualified to receive a certificate. The service provider submits the SPC token to the certificate authority to obtain a

certificate. Once the certificate is obtained, the provider or third-party service can begin authenticating and verifying calls. This is a multi-step process with detailed qualification obligations. As an intermediate carrier, Dorial does not have direct access at this time to NANPA support facilities for an SPC. As such, Dorial has not implemented the protocol which **REQUIRES** that any call passed through its network **MUST** contain an SPC or otherwise be **BLOCKED**. Dorial passes the packets on by copying the identity header information from packets received to packets sent.

Exemptions

The following exemptions are observed by Dorial from implementing STIR/SHAKEN the above protocol:

- *Non-IP Portions of Networks* – The non-IP portions of a provider’s network have an **indefinite exemption** from STIR/SHAKEN implementation but are subject to other requirements discussed below. **Dorial qualifies for this exemption from the Rules.**
- *Case-by-Case Exemption by FCC* – Providers can petition the FCC’s Wireless Bureau for an exemption or extension for implementing STIR/SHAKEN on a case-by-case basis; the formal petition deadline has passed, but the Bureau may still consider new petitions.

No Petitions have been made Dorial under this exemption.

9. **IP Network Mandate.** As STIR/SHAKEN does not work on non-IP networks, the FCC has implemented other requirements for those network portions to mitigate illegal calls. Specifically, DORIAL must either (a) upgrade their entire network to IP, or (b) participate in the development of a call authentication standard for non-IP calls (either directly or indirectly through a trade group) *and* implement a robocall mitigation program for the non-IP portions of their networks. DORIAL has implemented a robocall mitigation program. This robocall mitigation program includes:

- a) Dorial takes reasonable steps to avoid originating illegal robocall traffic by use of reasonable information and analytics from information in its possession or made available to it.

- b) Dorial commits to respond to requests from the Industry Traceback Group to trace suspect calls for mitigation efforts. Dorial is a member of US Telecom and its Traceback Group. Staff has been reasonably trained in STIR/SHAKEN requirements, this Plan and interface with the Traceback Group for Traceback requests.
- c) As an intermediary provider, suspect or non-conforming SPC calls shall be blocked. Likewise, Dorial has implemented Other however suspect caller patterns that are believed to be illegal shall be logged and/or blocked as per our Customer discretion.

10. **Proof of Implementation.** Type of specific steps taken to avoid originating illegal robocalls:

- **Those Unable to obtain SPC directly.** Dorial has implemented a protocol matching this authentication framework and coordinates with its originating and terminating carriers as SPCs are unavailable to it directly. As an intermediate provider, **Dorial will block calls onto its network that do not contain an SPC unless reasonable information exists that the call is not fraudulent by KYC information or assurances from originating providers (ILEC, Regional CLEC and etc.).**
- Dorial has advised carriers/providers passing originating calls of its protocol. Dorial advises its terminating carriers of its protocol and should, for any reason, a call from Dorial's network does not contain a SPC to block the call and advise Dorial of the call details to investigate. As an intermediary, Dorial will copy inbound identity header information into its outbound packets and route the call accordingly for record.

Dorial's has trained key and technical personnel on the TRACED Act and will adapt to any changes in the Rules required for intermediaries regarding STIR/SHAKEN. Dorial has developed specific procedures to fully respond in a timely manner to all traceback requests; as well as to cooperate in investigating and stopping illegal robocaller(s) using its service.

Consequence of Failure to Comply. Dorial recognizes that intermediary voice service providers are prohibited from the acceptance of calls from any provider that has not filed a

certificate on the Robocall Mitigation Database. Non-Complaint traffic shall be blocked.

11. Further Applicable Considerations/Exceptions for Dorial's STIR.SHAKEN Compliance.

A. Waivers of the FCC requirements. No Waiver Petitions have been made by Dorial.

B. Mitigation/Implementation. Dorial implements identity header pass-through and stand uses Third-Party software modules.

Dorial's initial compliance requirements do not call for full STIR (Secure Telephony Identity Revisited) and SHAKEN (Signature-based Handling of Asserted information using TOKEN(s) (RFC8224, RFC8588), by using X509 certificate path check (ATIS "Signature-based Handling of Asserted information using TOKENs (SHAKEN), RFC5280 Certification Path Validation"). As an intermediary, Dorial does not originate calls, so it is strictly subject and has implemented functionality for the passing of inbound identity header information to the next provider in the chain unaltered, and (b) subject to certain exceptions authenticate un-signed calls.

12. SUSPENSION & TERMINATION OF CUSTOMER. Dorial reserves the right to suspend any customer that exhibits a volume or pattern of Traceback Requests for Fraudulent Calls or otherwise calls violative of DNC or TCPA at any time. Standards set by this plan are a benchmark, not an absolute. For the same reasons, Dorial reserves the right to terminate a customer on similar grounds.

13. OTHER FRAUD DETERRENCE TOOLS. Dorial maintains comprehensive analytics systems to identify, analyze, and block illegal traffic across all telecommunications services. These additional policies outline the automated and manual processes implemented to protect our network and customers from fraudulent activities. The following have been used by Dorial since 2024.

A. STIR/SHAKEN Authentication Policy in combination with Other Deterrence

Dorial presently has multiple STIR/SHAKEN tokens for attesting calls it passes at varying attestation level: A, B, and C. Dorial maintains a certifying authority for each, but utilizes Attestation Level A with its downstream customers. Upstream providers have long-standing relationships, none of whom are gateways or international providers, and Dorial receives traffic from one of two sources:

- i. From Dominant or Regional ILECs or CLECs who pass STIR/SHAKEN Authentication based upon their relationship with the calling party and calling party subscriber number (attesting level A or B).
- ii. From Competitive IPEnabled Intermediate Providers who have submitted complete and current KYC information, or any update requested by Dorial; are registered with the FCC's RMD registry, are current with FCC 499-A reporting as to services and activities; and authenticate calls with STIR/SHAKEN tokens.

B. Attestation Requirements by Dorial

- i. All trunks used by Dorial require minimum attestation levels for call routing. Dorial uses attestation Level A for calls it routes/transmits.
- ii. Only calls meeting or exceeding configured attestation standards will be processed.
- iii. Attestation filtering provides cryptographic verification of caller identity.

C. Fraud and TCPA Compliance Filtering

Dorial has implemented the following Real-Time Marketing and Fraud Filters. These are software solutions and protocols integrated into their routing services and set-up:

- i. All individual trunks used by Dorial are equipped with real-time fraud detection filters.
- ii. These Filters utilize third-party data sources (e.g., DNO lists and other industry lists of encountered illegal robocall numbers) including user feedback reports to generate risk scores for Automatic Number Identification (ANI).
- iii. Dorial uses a standard blocking threshold as a default minimum but regularly operates at the enhanced blocking threshold standard with these filters. The distinction is as follows:

- a) Enhanced blocking threshold Standard blocking threshold is set at 80% confidence level (Almost Certainly Fraudulent)
- b) Enhanced sensitivity mode at 60% confidence level (Likely Fraudulent) may be activated to increase fraud detection at the risk of minimal false positives at any time on demand.

D. Implementation Standards and flexibility to target blocking with Fraud Filters.

Dorial uses reasonable implementation standard in filtering:

- i. Trunk-level configuration allows Dorial to customized and target sensitivity settings on-demand.
- ii. Score-based blocking automatically rejects calls exceeding established and upholding thresholds.
 - a) **Source Protection Measures.** Dorial uses Score based systems to automatically blacklist and identify fraud. This includes:

1) Automated Media Blacklist

- A. System maintains self-populated blacklist of known spam and scam media sources.
- B. Automatic blocking of calls from identified malicious originators.
- C. Real-time updates to blacklist database enhance protection coverage.
- D. Provides additional security layer beyond standard fraud filters.

2) Neighborhood Spoofing Filter that enables:

- A. Automatic rejection of calls where dialed number and ANI share identical area codes.
- B. Prevents deceptive practices designed to simulate local calling patterns.
- C. Filter activation blocks attempt to manipulate call recipient behavior.

3) Wireless ANI Authentication and Mobile Origination Filtering

- A. Telemarketing calls from wireless devices are flagged as suspicious.
- B. Automatic rejection of calls identified as originating from mobile phones.
- C. Helps identify randomly generated ANI patterns used in fraudulent schemes.

4) Auto Do-Not-Call (DNC) List Enforcement

- A. Integration with US National Do-Not-Call registry
- B. Automatic rejection of calls targeting numbers on DNC list.
- C. Trunk-level activation ensures compliance with federal regulations.

5) Auto Do-Not-Originate (DNO) Filter Implementation

- A. Rejection of calls from numbers prohibited from originating calls.
- B. Combined data sources from SOMOS and ITG databases
- C. Prevents unauthorized use of restricted number ranges.

6) ANI LERG Database Verification

- A. Validation against Local Exchange Routing Guide (LERG) database
- B. Detection and blocking of randomly generated ANI not conforming to official numbering plans.
- C. Enhanced protection against dialer-generated fake caller IDs

7) Spam Traffic Analysis

- A. Regular generation of repetitive ANI reports with risk assessments
- B. Investigation tools provide access to user comments and external recordings.
- C. Click-through analysis reveals call source information and patterns.

8) Blocking Action Protocols

- A. Customer-level ANI/DNIS blocking any account-specific issues.
- B. System-wide blacklisting for network-level threats
- C. Escalation procedures for persistent fraud patterns

- iii. Regular updates from external fraud databases ensure current threat intelligence allow filters to be maintained current and up to date.

E. Manual Intervention and Management

In addition to the foregoing, Dorial maintains staff to react to threats on a regular and on-demand basis of monitoring through its software systems on its platform. This includes:

- i. **System Blacklist Management from control panel through Smart Shield™**
 - a. Manual addition of fraud sources not captured by automated filters.
 - b. Entry of system-wide rejection of calls from manually identified threats
 - c. Access to regular review and maintenance of blacklist entries
- ii. **Manual Account-Level Blocking**
 - a. Entry of customer-specific ANI/DNIS blocking capabilities
 - b. Entry and programming of targeted blocking and alert protection for individual account requirements
 - c. Entry of localized control over account while maintaining system-wide protection
- iii. **Alert-based Watchdog Systems and passive monitoring software for Metric Monitoring and Response**
 - a. Running of Automated processes monitor various traffic metrics.
 - b. Configurable criteria trigger temporary or permanent blocking actions.
 - c. Pre-programmed Auto Detection and alert of unusual patterns such as high volumes of short-duration calls
 - d. A system-wide and an account-specific watchdog functionality for suspicious activity
- iv. **Advanced AI-Based Fraud Detection with Smart Shield™ Technology**
 - a. Passive call analysis and metrics using artificial intelligence.

- b. Behavioral, contextual, and intent analysis for fraud probability assessment based upon traffic patterns.
- c. Detection analytics for previously unknown scam types

v. Generation of Comprehensive Reporting and Analysis

- a. Detailed reports on all flagged calls with actionable intelligence
- b. Report analysis includes scam type identification and threat assessment.
- c. Sample detection categories include:
 - 1. Known Multi-language promotional scams.
 - 2. Known Technical support impersonation.
 - 3. Known Prize and giveaway fraud schemes.

vi. On-demand Multi-Vector Blocking Capabilities

Following AI analysis, blocking actions through manual operation of the software may further target on-demand:

- a. Originating ANI (caller ID)
- b. Originating media IP addresses
- c. Originating Operating Company Number (OCN) when STIR/SHAKEN authenticated.

vii. Generation of Traffic Quality Assessment Reports for periodic or event review

- a. Summary reports that provide overall customer traffic analysis
- b. Reports on fraud rate detection and trunk-level service suspension

Continuous Monitoring. The automated systems and software used by Dorial allow 24/7 automated monitoring of all traffic filtering systems to ensure regular policy compliance audits and system performance reviews. The software has ongoing updates to detect new algorithms and blocking criteria to allow staff to monitor as well as intervene when necessary.

Customer Communication. The software also allows transparent reporting on fraud prevention activities to customers through ticketing systems and tracking. This allows Dorial reasonable coordination with customers on account-specific protection needs when identified by ITG or otherwise be the FCC.

14. DID/ANI NUMBERING RESALE COMPLIANCE PROGRAM. Effective with this Rev. 4.0 policy, Dorial has commenced a DID/ANI numbering resale line of business, acquiring U.S. Direct Inward Dialing numbers and associated Automatic Number Identification resources from regional CLECs, I-VoIP providers, and major carriers, for resale with U.S. termination to other communications and telecommunications providers and to end users. This Section 14 governs that line of business and supplements, and where in conflict controls over, the general provisions of this policy as applied to numbering resale activity.

- A. **Regulatory Classification.** Dorial's intermediate call-routing line of business, described in Sections 1 through 13 above, remains that of a pure intermediate provider that does not originate or terminate calls. Dorial's DID/ANI numbering resale line places Dorial in an origination-adjacent role: while Dorial does not itself originate the calls its resold numbers are used to make, Dorial is responsible, as the entity assigning or reassigning numbering resources to its customers, for the sourcing verification, KYC, and attestation methodology obligations described below. Dorial acquires numbering resources exclusively through licensed upstream CLECs, I-VoIP providers, and major carriers holding valid FCC numbering authorizations, and does not, as of this policy date, seek direct access to numbering resources from NANPA. Should Dorial's numbering resale volume warrant seeking direct access authorization from the FCC in the future, this policy will be revised to incorporate the certification requirements applicable to direct access authorization holders under the Third VoIP Direct Access Report and Order (Dec. 19, 2025).
- B. **Numbering Source Verification.** Before reselling any DID/ANI number, Dorial verifies that its upstream source (CLEC, I-VoIP provider, or major carrier) holds current, valid numbering authorization and is registered and current on the FCC Robocall Mitigation Database. For Native Numbers, Dorial confirms the source

- carrier's Operating Carrier Number assignment. For Ported Numbers, Dorial obtains and retains a Letter of Authorization or equivalent porting record establishing chain of custody. This documentation is retained for the duration of the customer relationship plus twenty-four (24) months following termination or number disconnection, whichever is later.
- C. Downstream Right-of-Use Verification (Offnet Numbers). Dorial will not activate, and will not extend Level A STIR/SHAKEN attestation to, any number a downstream customer seeks to port in or otherwise associate with Dorial's numbering resale service (an "Offnet Number") unless that customer first furnishes equivalent right-of-use documentation to that described in subsection B above. This requirement applies regardless of whether the customer is itself a communications provider or an end user.
 - D. Enhanced KYC for Numbering Resale Customers. In addition to the KYC information described in Section 6 of this policy, and consistent with Section 6(a) of the TRACED Act as implemented in WC Docket No. 20-67, Dorial collects the following from every DID/ANI numbering resale customer prior to activation: (i) the customer's intended use case for the requested numbers, including whether the numbers will be used for outbound calling, inbound termination only, or further resale; (ii) disclosure of whether the customer services any call centers, telemarketers, or SMS/text campaign originators; and (iii) if the customer intends to further resell numbering resources to its own downstream customers, the flow-down certification described in subsection F below.
 - E. Attestation Methodology for Resold DID/ANI Traffic. Dorial's assignment of STIR/SHAKEN attestation level to traffic associated with resold DID/ANI numbers follows a documented methodology: (i) Level A attestation is extended only where Dorial can confirm both the identity of the customer and the customer's verified right of use of the specific calling number under subsections B and C above; (ii) Level B attestation is used where the customer's identity is confirmed but the specific right of use of the calling number cannot be verified to the Level A standard; and (iii) Level C attestation is used for traffic entering Dorial's network from outside the STIR/SHAKEN-enabled chain of trust. Dorial will not extend

Level A attestation to any Offnet Number lacking the documentation required under subsection C.

- F. Reseller Certification and Flow-Down (WC Docket No. 26-49). Dorial requires every DID/ANI numbering resale customer to certify that it will not use, and will contractually prohibit its own downstream customers from using, numbers obtained from Dorial to knowingly transmit, encourage, assist, or facilitate illegal robocalls, illegal spoofing, or fraud. Where a customer further resells DID/ANI resources obtained from Dorial, that customer must obtain equivalent certifications, and equivalent KYC and right-of-use verification under subsections C and D, from its own downstream customers, and must make such certifications available to Dorial upon request. Dorial monitors WC Docket No. 26-49 (Combating Illegal Robocalls Through FCC Numbering Policies, FCC 26-17, adopted March 26, 2026), including its proposed one-time reseller certification requirement, proposed reseller identification to wholesale providers and NANPA, and proposed limitation of numbering resale to a single level, and will update this policy and Dorial's numbering resale customer agreements upon adoption of a final rule in that proceeding.
- G. Trust Anchor and SPC Token Considerations. Dorial's numbering resale line of business does not, as of this policy date, alter Dorial's Trust Anchor posture described in Sections 7 through 11 of this policy. Dorial continues to hold and sign traffic directly with its own SPC token and Certificate Authority credentials as described therein. Should Dorial's numbering resale activity require Dorial to assume originating-provider STIR/SHAKEN obligations for specific traffic (as opposed to the origination-adjacent role described in subsection A), Dorial will evaluate and, if necessary, expand its Trust Anchor registration accordingly, and will update this policy to reflect that change.
- H. Traceback and Record Retention for Numbering Resale Customers. Dorial's numbering resale customers are subject to the same Industry Traceback Group cooperation and 24-hour target response expectations, and the same tolerance levels for Fraudulent Robocall traceback requests, described in Sections 3 and 4 of this policy. Dorial additionally retains call detail records and number-assignment

documentation associated with numbering resale customers for not less than eighteen (18) months following the relevant call or number assignment, to support traceback and audit requests.

- I. 911, CALEA, and CPNI Flow-Down. Dorial's numbering resale customers are required to acknowledge, in Dorial's standard numbering resale service agreement, that they are not relying on Dorial to provide 911 or E911 service in connection with resold numbers, and to provide CALEA inquiry contact information consistent with applicable law. Customers that further resell DID/ANI resources must flow down equivalent 911 and CALEA disclosures to their own downstream customers.
- J. Annual Recertification and Monitoring List. Dorial's numbering resale line of business is subject to the same annual RMD recertification cycle (March 1) described elsewhere in this policy. Dorial additionally maintains an active monitoring list for the following proceedings bearing on the numbering resale line: WC Docket No. 26-49 (reseller certification and single-level resale cap, FCC 26-17); WC Docket No. 20-67 (TRACED Act Section 6(a) Know Your Customer requirements for entities with access to numbering resources); and the Call Authentication Trust Anchor Know-Your-Upstream-Provider proceeding, WC Docket No. 17-97, FCC 26-32 (May 21, 2026), which addresses interconnected VoIP resellers and MVNOs specifically.

These Robocall policies ensure Dorial maintains the highest standards of network security based upon its role in the telecom ecosystem and regulatory compliance with robocall mitigation Rules while providing reliable telecommunications services to all customers.