

Voice Network Security and Robocall Mitigation Policy

TELECOM1 LTD.

Approved by: Managing Director

Document Control

Item	Value
Document Title	Telecom1 Voice Network Security and Robocall Mitigation Policy
Version	1.0
Owner	Telecom1 Ltd.
Classification	Public
Review Period	Annual
Applies To	All Telecom1 Voice Services

Purpose

This document defines the operational, administrative and technical controls implemented by Telecom1 Ltd. to protect its voice network from unauthorized use, caller identity abuse and fraudulent telecommunications activity.

The policy describes how Telecom1 authenticates subscribers, authorizes outbound calls, controls caller identification, investigates suspicious activity and cooperates with interconnected telecommunications operators.

Scope

This policy applies to every voice service operated by Telecom1, including:

- SIP voice services
- Geographic telephone numbers
- Carrier Selection services
- Access Number services

Telecom1 LTD.

- Outbound international calling
- Domestic voice services
- Customer provisioning
- Network routing
- Interconnection with other telecommunications operators

The policy applies to all Telecom1 residential and business subscribers.

Definitions

Access Number

A Telecom1 service that allows customers to access the Telecom1 voice network using designated Telecom1 access numbers.

Authentication

The process of verifying that a subscriber attempting to originate a call is a valid Telecom1 customer.

Caller ID (CLI)

The telephone number presented to the called party and to interconnected telecommunications operators.

Call Detail Record (CDR)

A record generated by the switching platform containing operational information about a telephone call.

Carrier Selection

A regulated telecommunications service allowing customers to originate calls through Telecom1 using a carrier selection prefix.

KYC (Know Your Customer)

Customer identification and verification procedures performed before activation of service.

Presented Identity

Telecom1 LTD.

The Caller ID transmitted by Telecom1 to external telecommunications operators after authorization.

Subscriber Identity

The customer record maintained within Telecom1 subscriber database.

Traceback

The process of identifying the originating customer responsible for specific telecommunications traffic following a request from another operator or regulatory authority.

Telecom1 responds promptly to legitimate traceback requests and maintains sufficient operational records to identify the authenticated subscriber responsible for originated traffic.

1. Introduction

Telecom1 Ltd. is a licensed electronic communications operator established in the Republic of Bulgaria and regulated by the Communications Regulation Commission (CRC).

The company provides fixed voice telecommunications services exclusively to its own residential and business customers.

The integrity of caller identity and the prevention of telecommunications fraud are fundamental security objectives of the Telecom1 voice network.

Telecom1 has implemented a combination of technical controls, operational procedures and customer verification processes designed to ensure that only authorized subscribers are permitted to originate calls through the Telecom1 network.

Unlike networks that provide wholesale transit services, Telecom1 operates as an originating service provider for its own customers. The company does not knowingly provide its network as a transit platform for third-party voice traffic.

Because of this architecture, every outbound call can be associated with an authenticated Telecom1 subscriber whose identity has been verified during the customer onboarding process.

2. Company Overview

Telecom1 LTD.

Telecom1 Ltd. provides electronic communications services under licenses issued by the Communications Regulation Commission of Bulgaria.

The company offers voice services to residential and business customers using its own switching infrastructure.

Telecom1 does not provide anonymous telecommunications services.

Every customer relationship is established following customer identification and service provisioning procedures.

The company maintains a central subscriber database containing customer information, assigned telephone numbers, service permissions and routing information required for voice service operation.

The Telecom1 network has been designed so that routing decisions, subscriber permissions and caller identification are centrally controlled by the switching platform rather than by customer equipment.

This architecture significantly reduces the possibility of unauthorized network access and caller identity manipulation.

3. Services

Telecom1 currently provides:

- SIP voice services
- Fixed telephone services
- Geographic numbering
- Domestic voice services
- International voice services
- Carrier Selection
- Access Number services

Telecom1 provides services only to end users.

The company does not provide wholesale voice transit.

The company does not purchase traffic from one operator for delivery to another operator through the Telecom1 network.

Incoming traffic received from interconnected carriers cannot be forwarded to other external operators.

Every outbound call processed by Telecom1 originates from an authenticated Telecom1 subscriber.

4. Customer Acceptance Policy

Telecom1 provides telecommunications services only after successful customer verification.

Residential customers are required to provide identification information necessary to establish their identity before service activation.

Business customers are required to provide company registration information together with the identity of an authorized representative.

Customer information is maintained within Telecom1 operational systems and is associated with every active voice service.

Telecom1 does not knowingly provide telecommunications services intended for:

- illegal robocalling;
- caller ID spoofing;
- traffic pumping;
- artificial traffic generation;
- unlawful telecommunications fraud;
- anonymous wholesale traffic;
- unauthorized international traffic origination.

If Telecom1 becomes aware that a customer is using its services for fraudulent or abusive purposes, the company may suspend or permanently terminate the service.

5. Customer Verification

Customer verification (Know Your Customer – KYC) forms an essential part of the Telecom1 security model.

Before any service is activated, Telecom1 verifies sufficient customer information to establish the identity of the subscriber requesting service.

For residential customers this includes personal identification and contact information.

Telecom1 LTD.

For business customers Telecom1 verifies company registration information together with the identity of the authorized representative acting on behalf of the company.

Following successful verification, the customer receives access credentials and one or more telephone numbers assigned from numbering resources allocated to Telecom1.

Only numbers officially assigned by Telecom1 may subsequently be presented as outbound caller identification.

Customer information remains associated with all services throughout the lifetime of the customer account.

Changes affecting customer identity or assigned numbering resources are performed only through authorized Telecom1 administrative procedures.

6. Network Authentication and Access Control

6.1 General Principles

The Telecom1 voice network has been designed around a simple security principle:

Every outbound call must originate from an authenticated Telecom1 subscriber.

No call is permitted to leave the Telecom1 network unless the originating subscriber has been successfully authenticated and validated by the switching platform.

Customer equipment is considered an endpoint only. It does not participate in routing decisions, caller identity authorization or interconnection control.

All security decisions are performed centrally by Telecom1 network infrastructure.

6.2 Subscriber Authentication

Every customer receives unique authentication credentials during service provisioning.

These credentials are associated with a single subscriber record maintained within the Telecom1 subscriber database.

Before a subscriber is allowed to originate calls, the switching platform verifies the authentication credentials presented by the customer device.

Telecom1 LTD.

Successful authentication confirms only the identity of the subscriber attempting to access the service.

Authentication alone does not authorize the call.

Additional validation steps are performed before the call is routed to another telecommunications operator.

6.3 Subscriber Validation

Following successful authentication, the switching platform validates the subscriber record.

At a minimum, the following information is verified:

- the subscriber exists;
- the account is active;
- voice service is enabled;
- outbound calling is permitted;
- the requested routing is allowed.

If any validation step fails, the call is rejected.

Calls originating from unknown, inactive or unauthorized subscribers are never forwarded to domestic or international interconnected operators.

Depending on the reason for rejection, the switching platform returns the appropriate signalling response.

This prevents unauthorized use of Telecom1 interconnection resources.

6.4 Centralized Routing

Routing decisions are performed exclusively by Telecom1 switching infrastructure.

Customer devices have no ability to influence:

- routing tables;
- carrier selection;
- interconnection paths;
- outbound gateway selection;
- signalling parameters used toward interconnected operators.

All routing information is maintained centrally by Telecom1 engineering personnel.

Telecom1 LTD.

Changes to routing configuration may only be performed by authorized administrators.

This architecture prevents customers from redirecting traffic through unauthorized destinations or manipulating interconnection policies.

6.5 Protection Against Unauthorized Network Use

The Telecom1 network has been designed to prevent unauthorized access to external telecommunications networks.

A subscriber who is not present in the Telecom1 subscriber database cannot originate outbound calls.

Likewise, a device possessing invalid authentication credentials cannot gain access to Telecom1 voice services.

Because subscriber authentication, subscriber validation and routing authorization are all required before call establishment, unauthorized use of Telecom1 interconnection facilities is significantly reduced.

7. Caller ID Authorization and Number Presentation

7.1 Security Objective

Telecom1 considers caller identity integrity to be a fundamental security requirement.

The company does not rely on caller identification information supplied by customer equipment when presenting calls to external telecommunications operators.

Instead, caller identity is generated by the Telecom1 switching platform using subscriber information maintained within the Telecom1 operational database.

This ensures that caller identification presented outside the Telecom1 network accurately reflects the identity of the authorized subscriber.

7.2 Customer-Supplied Caller ID

Customer equipment may transmit caller identification information during signalling.

This information is not considered authoritative.

Telecom1 does not use customer-supplied caller identity when routing calls to interconnected operators.

Instead, the switching platform retrieves the authorized outbound caller identification associated with the authenticated subscriber account.

Any caller identity supplied by the customer equipment is ignored or replaced before the call leaves the Telecom1 network.

This prevents customers from presenting arbitrary telephone numbers to external operators.

7.3 Authorized Number Assignment

Each active Telecom1 subscriber is assigned one or more telephone numbers from numbering resources allocated to Telecom1.

These assignments are maintained within the subscriber database.

Only numbers recorded within this database may be presented as outbound caller identification.

Customers cannot independently select telephone numbers that have not been assigned by Telecom1.

As a result, outbound caller identity always corresponds to numbering resources controlled by Telecom1.

7.4 Caller ID Replacement

Immediately before a call is routed to another telecommunications operator, the switching platform determines the caller identity that will be presented externally.

The presented caller identity is obtained from the Telecom1 subscriber database.

If customer equipment supplied a different caller identity during signalling, that value is replaced by the authorized Telecom1 caller identity.

Telecom1 LTD.

The replacement process is automatic and requires no customer intervention.

This mechanism provides effective protection against unauthorized caller identity presentation.

7.5 Subscriber Identity and Presented Identity

For security purposes, Telecom1 distinguishes between three separate identities:

Authentication Identity

The credentials used by the customer device to authenticate to the Telecom1 voice platform.

Subscriber Identity

The customer account maintained within the Telecom1 operational database.

Presented Identity

The telephone number transmitted by Telecom1 to interconnected telecommunications operators after authorization.

Although these identities are related, they serve different operational purposes.

The presented identity is always determined by Telecom1 network policy rather than by customer equipment.

7.6 Carrier Selection and Access Number Services

Telecom1 provides Carrier Selection and Access Number services using numbering resources assigned to Telecom1.

Customers using these services are authenticated in the same manner as all other Telecom1 subscribers.

The caller identity presented to interconnected operators is determined exclusively by Telecom1 subscriber records.

Carrier Selection and Access Number services therefore follow the same caller identity authorization policy as standard Telecom1 voice services.

Customers cannot present arbitrary caller identities through these services.

7.7 Protection Against Caller ID Spoofing

The combination of:

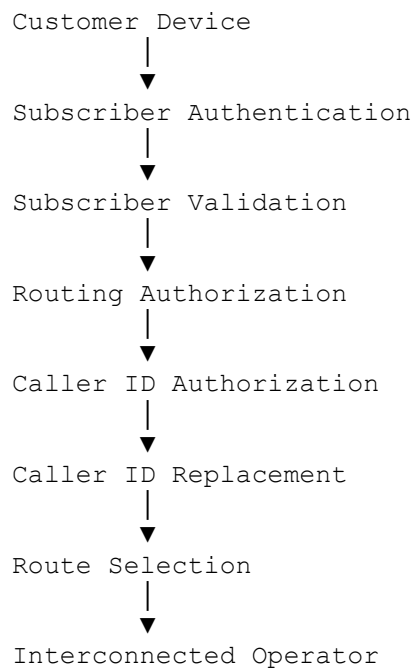
- subscriber authentication;
- subscriber validation;
- centralized routing;
- database-controlled caller identity;
- automatic caller ID replacement;

provides a layered defense against caller ID spoofing.

Because customers are unable to control the caller identity presented to interconnected operators, the possibility of unauthorized caller identity presentation originating from the Telecom1 network is significantly reduced.

7.8 Call Processing Overview

The outbound call processing sequence implemented by Telecom1 may be summarized as follows:



At no point during this process is the customer permitted to determine the caller identity presented to another telecommunications operator.

6. Network Authentication and Access Control

6.1 General Principles

The Telecom1 voice network has been designed around a simple security principle:

Every outbound call must originate from an authenticated Telecom1 subscriber.

No call is permitted to leave the Telecom1 network unless the originating subscriber has been successfully authenticated and validated by the switching platform.

Customer equipment is considered an endpoint only. It does not participate in routing decisions, caller identity authorization or interconnection control.

All security decisions are performed centrally by Telecom1 network infrastructure.

6.2 Subscriber Authentication

Every customer receives unique authentication credentials during service provisioning.

These credentials are associated with a single subscriber record maintained within the Telecom1 subscriber database.

Before a subscriber is allowed to originate calls, the switching platform verifies the authentication credentials presented by the customer device.

Successful authentication confirms only the identity of the subscriber attempting to access the service.

Authentication alone does not authorize the call.

Additional validation steps are performed before the call is routed to another telecommunications operator.

6.3 Subscriber Validation

Following successful authentication, the switching platform validates the subscriber record.

At a minimum, the following information is verified:

Telecom1 LTD.

- the subscriber exists;
- the account is active;
- voice service is enabled;
- outbound calling is permitted;
- the requested routing is allowed.

If any validation step fails, the call is rejected.

Calls originating from unknown, inactive or unauthorized subscribers are never forwarded to domestic or international interconnected operators.

Depending on the reason for rejection, the switching platform returns the appropriate signalling response.

This prevents unauthorized use of Telecom1 interconnection resources.

6.4 Centralized Routing

Routing decisions are performed exclusively by Telecom1 switching infrastructure.

Customer devices have no ability to influence:

- routing tables;
- carrier selection;
- interconnection paths;
- outbound gateway selection;
- signalling parameters used toward interconnected operators.

All routing information is maintained centrally by Telecom1 engineering personnel.

Changes to routing configuration may only be performed by authorized administrators.

This architecture prevents customers from redirecting traffic through unauthorized destinations or manipulating interconnection policies.

6.5 Protection Against Unauthorized Network Use

The Telecom1 network has been designed to prevent unauthorized access to external telecommunications networks.

A subscriber who is not present in the Telecom1 subscriber database cannot originate outbound calls.

Telecom1 LTD.

Likewise, a device possessing invalid authentication credentials cannot gain access to Telecom1 voice services.

Because subscriber authentication, subscriber validation and routing authorization are all required before call establishment, unauthorized use of Telecom1 interconnection facilities is significantly reduced.

7. Caller ID Authorization and Number Presentation

7.1 Security Objective

Telecom1 considers caller identity integrity to be a fundamental security requirement.

The company does not rely on caller identification information supplied by customer equipment when presenting calls to external telecommunications operators.

Instead, caller identity is generated by the Telecom1 switching platform using subscriber information maintained within the Telecom1 operational database.

This ensures that caller identification presented outside the Telecom1 network accurately reflects the identity of the authorized subscriber.

7.2 Customer-Supplied Caller ID

Customer equipment may transmit caller identification information during signalling.

This information is not considered authoritative.

Telecom1 does not use customer-supplied caller identity when routing calls to interconnected operators.

Instead, the switching platform retrieves the authorized outbound caller identification associated with the authenticated subscriber account.

Any caller identity supplied by the customer equipment is ignored or replaced before the call leaves the Telecom1 network.

This prevents customers from presenting arbitrary telephone numbers to external operators.

7.3 Authorized Number Assignment

Each active Telecom1 subscriber is assigned one or more telephone numbers from numbering resources allocated to Telecom1.

These assignments are maintained within the subscriber database.

Only telephone numbers recorded and authorized within the Telecom1 subscriber database may be presented as outbound caller identification.

These numbers may be assigned directly by Telecom1 or may represent customer telephone numbers from interconnected operators that have been verified and associated with the authenticated subscriber account.

Customers cannot independently select arbitrary caller identities. The presented caller identity is always determined by Telecom1 authorization policies.

7.4 Caller ID Replacement

Immediately before a call is routed to another telecommunications operator, the switching platform determines the caller identity that will be presented externally.

The presented caller identity is obtained from the Telecom1 subscriber database.

If customer equipment supplied a different caller identity during signalling, that value is replaced by the authorized Telecom1 caller identity.

The replacement process is automatic and requires no customer intervention.

This mechanism provides effective protection against unauthorized caller identity presentation.

7.5 Subscriber Identity and Presented Identity

For security purposes, Telecom1 distinguishes between three separate identities:

Authentication Identity

The credentials used by the customer device to authenticate to the Telecom1 voice platform.

Subscriber Identity

Telecom1 LTD.

The customer account maintained within the Telecom1 operational database.

Presented Identity

The telephone number transmitted by Telecom1 to interconnected telecommunications operators after authorization.

Although these identities are related, they serve different operational purposes.

The presented identity is always determined by Telecom1 network policy rather than by customer equipment.

7.6 Carrier Selection and Access Number Services

Telecom1 provides Carrier Selection and Access Number services to authenticated subscribers.

Customers may be identified either by a verified calling line associated with their subscriber account or, where such verification is not possible, by customer account credentials.

The caller identity presented to interconnected operators is determined exclusively from Telecom1 subscriber records and only authorized caller identities may be used.

Customers using these services are authenticated in the same manner as all other Telecom1 subscribers.

The caller identity presented to interconnected operators is determined exclusively by Telecom1 subscriber records.

Carrier Selection and Access Number services therefore follow the same caller identity authorization policy as standard Telecom1 voice services.

Customers cannot present arbitrary caller identities through these services.

7.7 Protection Against Caller ID Spoofing

The combination of:

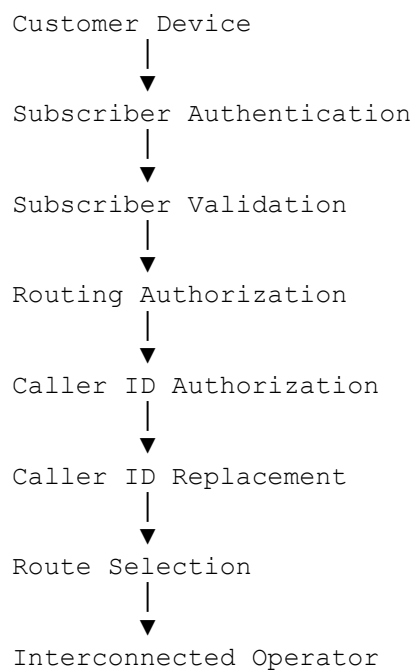
- subscriber authentication;
- subscriber validation;
- centralized routing;
- database-controlled caller identity;
- automatic caller ID replacement;

provides a layered defense against caller ID spoofing.

Because customers are unable to control the caller identity presented to interconnected operators, the possibility of unauthorized caller identity presentation originating from the Telecom1 network is significantly reduced.

7.8 Call Processing Overview

The outbound call processing sequence implemented by Telecom1 may be summarized as follows:



At no point during this process is the customer permitted to determine the caller identity presented to another telecommunications operator.

8. Traffic Monitoring and Fraud Prevention

8.1 Operational Monitoring

The Telecom1 voice network is continuously monitored to ensure the reliable operation of telecommunications services and to identify abnormal traffic conditions that may indicate fraud, unauthorized network use or service misuse.

Monitoring activities are performed using operational data generated by the switching platform and associated management systems.

Telecom1 LTD.

These activities support:

- service availability;
- operational troubleshooting;
- fraud investigation;
- customer support;
- regulatory compliance.

Operational monitoring forms an integral part of the Telecom1 network security model.

8.2 Call Detail Records

Telecom1 generates Call Detail Records (CDRs) for voice traffic processed by its switching platform.

Depending on the nature of the call, CDRs may contain operational information including:

- originating subscriber;
- called number;
- call start time;
- call end time;
- call duration;
- routing information;
- call completion status;
- signalling cause codes.

CDRs are used for:

- customer billing;
- dispute resolution;
- operational analysis;
- fraud investigation;
- traceback requests;
- regulatory obligations.

The company considers CDRs one of the primary sources of operational information when investigating network incidents.

8.3 Operational Logs

In addition to Call Detail Records, Telecom1 maintains operational logs generated by network equipment and supporting systems.

These logs assist engineering personnel in identifying:

- authentication failures;
- signalling errors;
- routing failures;
- abnormal call attempts;
- operational anomalies.

Operational logs are used exclusively for network administration, troubleshooting and security investigations.

8.4 Detection of Suspicious Activity

Telecom1 periodically reviews operational information to identify traffic that differs significantly from the expected behaviour of an individual subscriber.

Examples include:

- unusually high outbound call volumes;
- unexpected calling destinations;
- repeated unsuccessful call attempts;
- indications of unauthorized account use;
- behaviour inconsistent with the subscriber's normal service profile.

The presence of unusual traffic does not automatically indicate fraudulent activity.

Where necessary, Telecom1 performs additional investigation before determining the appropriate response.

9. Fraud Prevention and Incident Response

9.1 Security Principles

Telecom1 employs multiple independent controls designed to reduce the risk of telecommunications fraud.

These controls include both administrative procedures and technical safeguards.

No single security mechanism is relied upon in isolation.

Instead, fraud prevention is achieved through a layered security approach.

9.2 Preventive Controls

The principal controls implemented by Telecom1 include:

- customer identity verification before service activation;
- subscriber authentication;
- subscriber database validation;
- centralized routing;
- database-controlled caller identification;
- automatic caller ID replacement;
- prepaid service model;
- operational monitoring;
- Call Detail Record analysis;
- immediate administrative suspension when required.

The combination of these controls substantially reduces opportunities for unauthorized network use.

9.3 Service Suspension

Where Telecom1 determines that a service is being used in a manner inconsistent with applicable laws, contractual obligations or network security requirements, the company may immediately restrict or suspend the affected service.

Examples include:

- suspected caller ID spoofing;
- fraudulent telecommunications activity;
- unauthorized use of subscriber credentials;
- attempts to abuse Telecom1 interconnection facilities.

Depending on the circumstances, service may remain suspended until the matter has been resolved or may be permanently terminated.

9.4 Incident Investigation

When suspicious activity is identified, Telecom1 performs an internal investigation using available operational records.

Depending on the circumstances, this investigation may include review of:

Telecom1 LTD.

- customer information;
- subscriber configuration;
- authentication records;
- routing information;
- Call Detail Records;
- operational logs.

The objective of the investigation is to determine whether the activity resulted from:

- normal customer behaviour;
- customer misconfiguration;
- unauthorized access;
- attempted fraud;
- other operational causes.

10. Complaint Handling and Traceback

10.1 Complaint Handling

Telecom1 investigates reports of suspected network abuse received from:

- customers;
- interconnected telecommunications operators;
- regulatory authorities;
- law enforcement authorities.

Each report is evaluated using available operational information.

Where additional information is required, Telecom1 may contact the customer before reaching a final conclusion.

10.2 Traceback Requests

Telecom1 supports legitimate traceback requests relating to voice traffic that originated from the Telecom1 network.

Upon receipt of a valid request, Telecom1 may review:

- subscriber records;
- assigned telephone numbers;
- Call Detail Records;
- routing information;

Telecom1 LTD.

- authentication records.

Where permitted by applicable law, this information is used to identify the subscriber responsible for the reported traffic.

10.3 Cooperation with Other Operators

Telecom1 cooperates with interconnected telecommunications operators in the investigation of suspected fraudulent telecommunications traffic.

Where appropriate, relevant operational information may be exchanged in accordance with applicable legal and regulatory requirements.

Telecom1 recognizes that cooperation between originating and terminating operators is an important component of effective robocall mitigation.

11. Technical Controls Summary

Risk	Telecom1 Control
Anonymous customer	Customer verification (KYC)
Unauthorized network access	SIP subscriber authentication
Unknown subscriber	Database validation before every outbound call
Invalid account	Call rejected
Unauthorized routing	Centralized routing controlled by Telecom1
Caller ID spoofing	Caller ID replaced from Telecom1 subscriber database
Customer-controlled routing	Not permitted
Wholesale transit abuse	Network architecture does not provide transit services
Service misuse	Operational monitoring and investigation
Fraud	Immediate administrative suspension
Traceback request	CDR and subscriber record investigation

12. Compliance Statement

Telecom1 is committed to operating a secure voice network that prevents unauthorized use of its telecommunications services.

The company combines customer verification, subscriber authentication, centralized routing, caller identity authorization and operational monitoring to reduce the risk of robocalling, caller ID spoofing and telecommunications fraud.

Telecom1 continuously reviews its operational procedures and technical controls to ensure that they remain appropriate for the services provided and consistent with applicable regulatory requirements.

This policy is reviewed periodically and updated whenever operational, technical or regulatory changes require modification.

13. Contact Information

Telecom1 Ltd.

For regulatory, traceback and abuse-related matters:

Email: **abuse@telecom1.bg**

Website: <https://telecom1.bg>

Registered Office:

*105 Tsarigradsko Shose Blvd.
1113 Sofia, Bulgaria*

This document also serves as Telecom1's Robocall Mitigation Program for the purposes of the FCC Robocall Mitigation Database (RMD).