



Robocall Mitigation Database External Filing Instructions

Version: January 2026

Contents

I.	INTRODUCTION	2
II.	VIEW DATABASE	2
a.	Downloading a .CSV File of the Database	2
b.	Viewing the Database Online	3
c.	Searching the Online Database	4
d.	Accessing the Database via API	4
III.	SUBMIT AND MANAGE FILINGS WITHIN THE DATABASE	5
a.	Submitting a Filing	5
b.	Revising a Filing	23
c.	Submitting an Annual Recertification	26
d.	Deleting a Filing	29

I. INTRODUCTION

The Robocall Mitigation Database can be found at <https://fccprod.servicenowservices.com/rmd>.

Upon arriving at the Robocall Mitigation Database Welcome Page, you will see four options: “Download,” “View Database,” “Log In,” and “Create Account.”

Registration is not required to download or view the Database—any member of the public can download a .CSV file of the Database or view and search the Database online at any time. The Database can also be accessed via API.

When accessing the Robocall Mitigation Database, if you believe there are errors with the content or function of the Database, or if you require special assistance with submitting a filing, please email FCC staff at RobocallMitigationDatabase@FCC.gov.

II. VIEW DATABASE

a. Downloading a .CSV File of the Database

- i. To download the Robocall Mitigation Database, visit <https://fccprod.servicenowservices.com/rmd> and click on the “Download” button (see Figure 1).

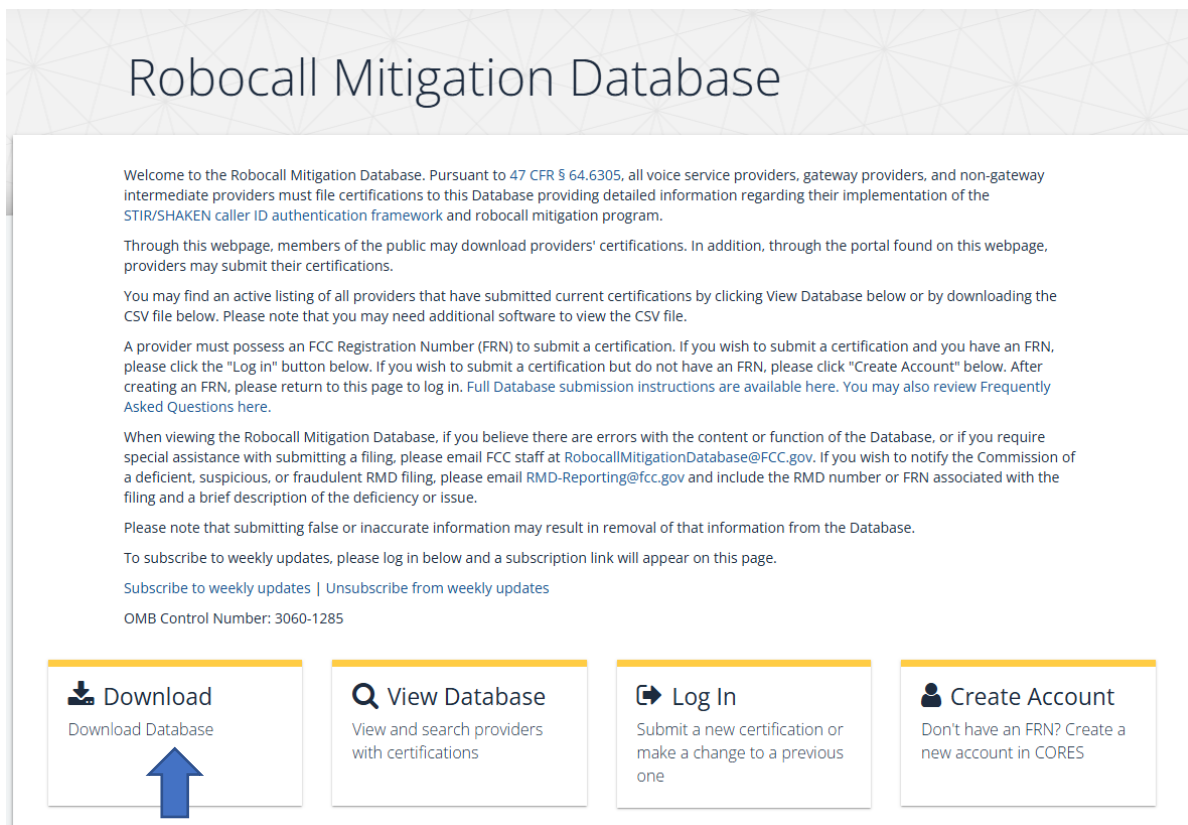


Figure 1 – Welcome Page, click “Download” to download the Database.

Robocall Mitigation Database External Filing Instructions

January 2026

- ii. After you click “Download,” your browser may prompt you to choose an application to view the .CSV file. Please note that you may need additional software to view the Database file.

b. Viewing the Database Online

- i. To view the Robocall Mitigation Database, visit <https://fccprod.servicenowservices.com/rmd> and click on the “View Database” button (see Figure 2).

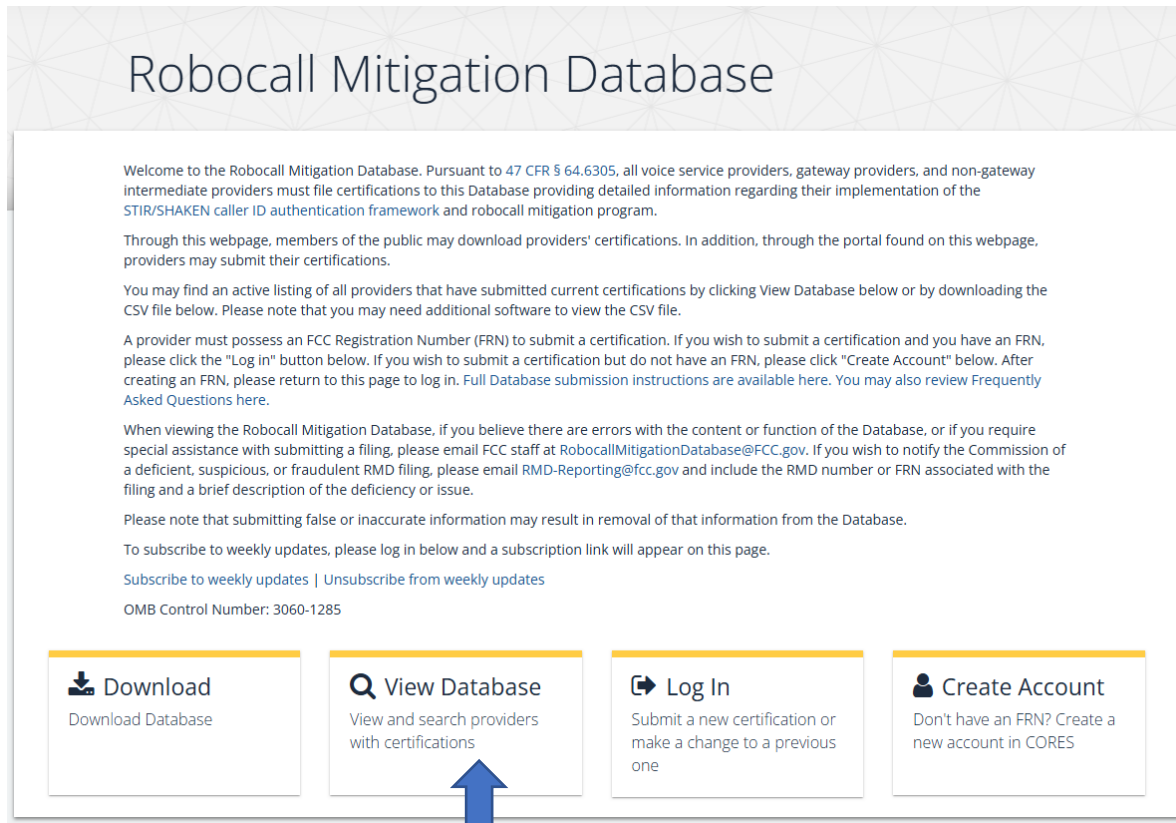


Figure 2 – Welcome Page, click “View Database” to view the Database.

- ii. To subscribe to weekly updates, you must first log in with a CORES account. Once logged in, a “Subscribe to weekly updates” link will appear.

c. Searching the Online Database

- i. To conduct a text search within the Database, after clicking the “View Database” button, you will arrive at the Public Listings Page and a “Keyword Search” box will be located in the top right of the screen (see Figure 3).

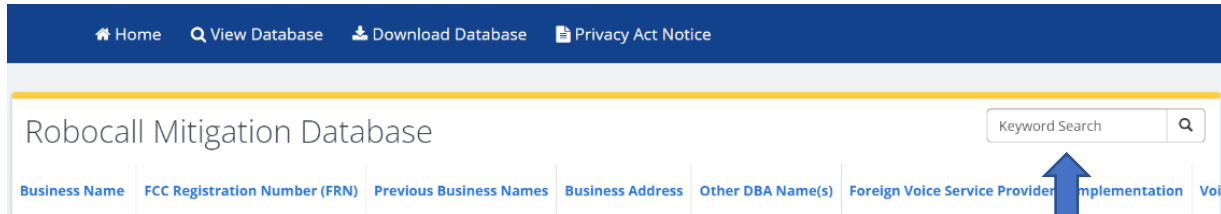


Figure 3 – Public Listings Page, use the “Keyword Search” box to search the Database.

- ii. To view all columns of the Database, use the horizontal scroll bar located at the bottom of the screen (see Figure 4).

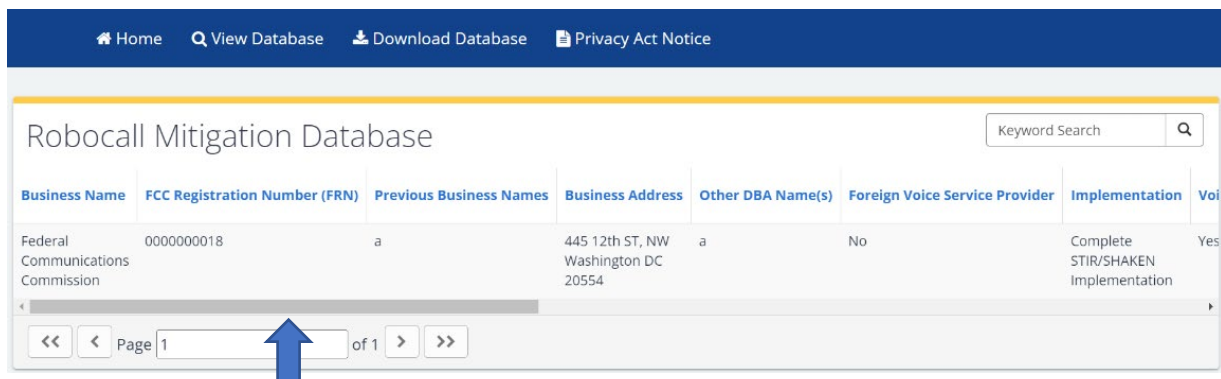


Figure 4 – Public Listings Page, use the horizontal scroll bar to view all columns.

d. Accessing the Database via API

- i. The API provides programmatic read access to the Database dataset, including the ability to filter and query data.
- ii. Detailed instructions on how to access the Database via API are available at the following link:
www.fcc.gov/files/robocall-mitigation-database-api-documentation.

III. SUBMIT AND MANAGE FILINGS WITHIN THE DATABASE

a. Submitting a Filing

- i. A Commission Registration System (CORES) account and an FCC Registration Number (FRN) are needed to submit a Robocall Mitigation Database filing.
 - If you need a CORES account or an FRN, please click the “Create Account” button (see Figure 5) or visit <https://apps.fcc.gov/core/userLogin.do> to begin the CORES account creation process.
 - The CORES welcome page has a link to CORES Tutorial Videos that provide guidance on the account creation process.
 - Please note that the Robocall Mitigation Database form cannot be submitted with an individual-type FRN. Please contact CORES if you need assistance registering a business-type FRN.

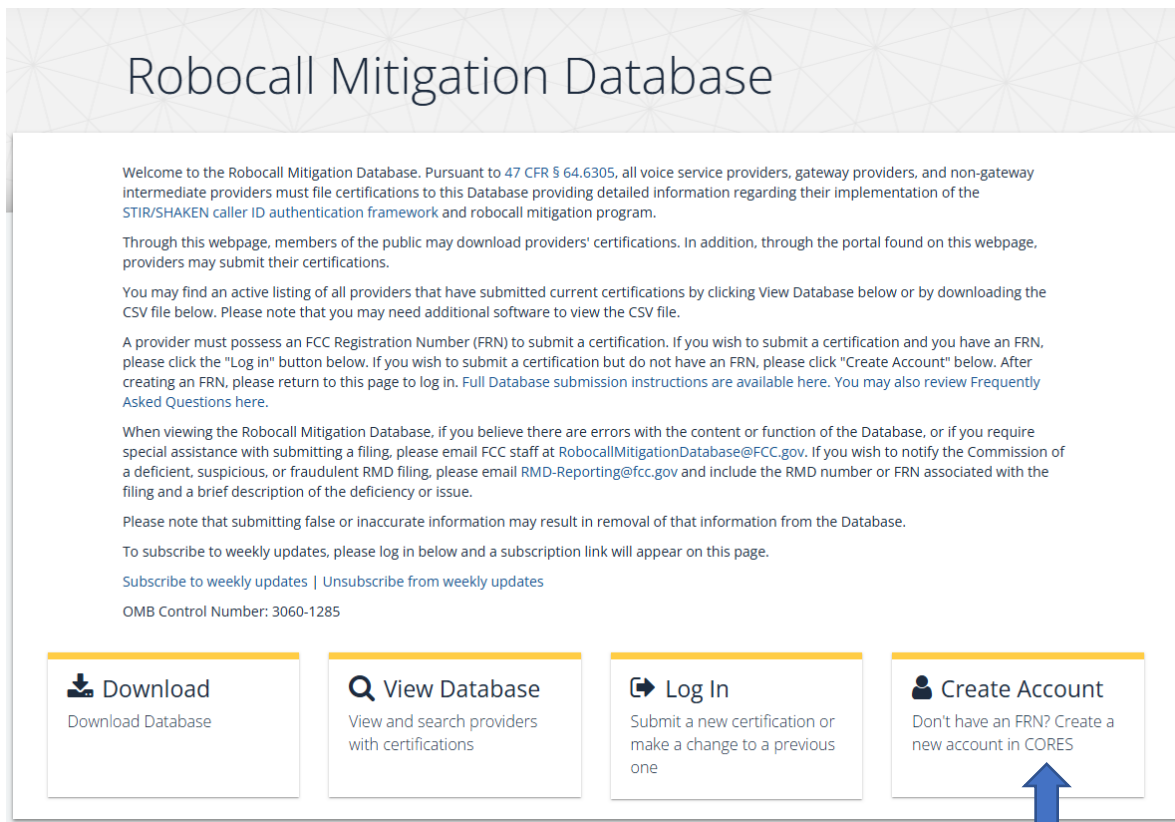


Figure 5 – Welcome Page, click “Create Account” to create a CORES account.

- ii. Providers with a CORES account and an FRN can log in and submit a Robocall Mitigation Database filing by clicking the “Log In” button on the Robocall Mitigation Database Welcome Page (See Figure 6).

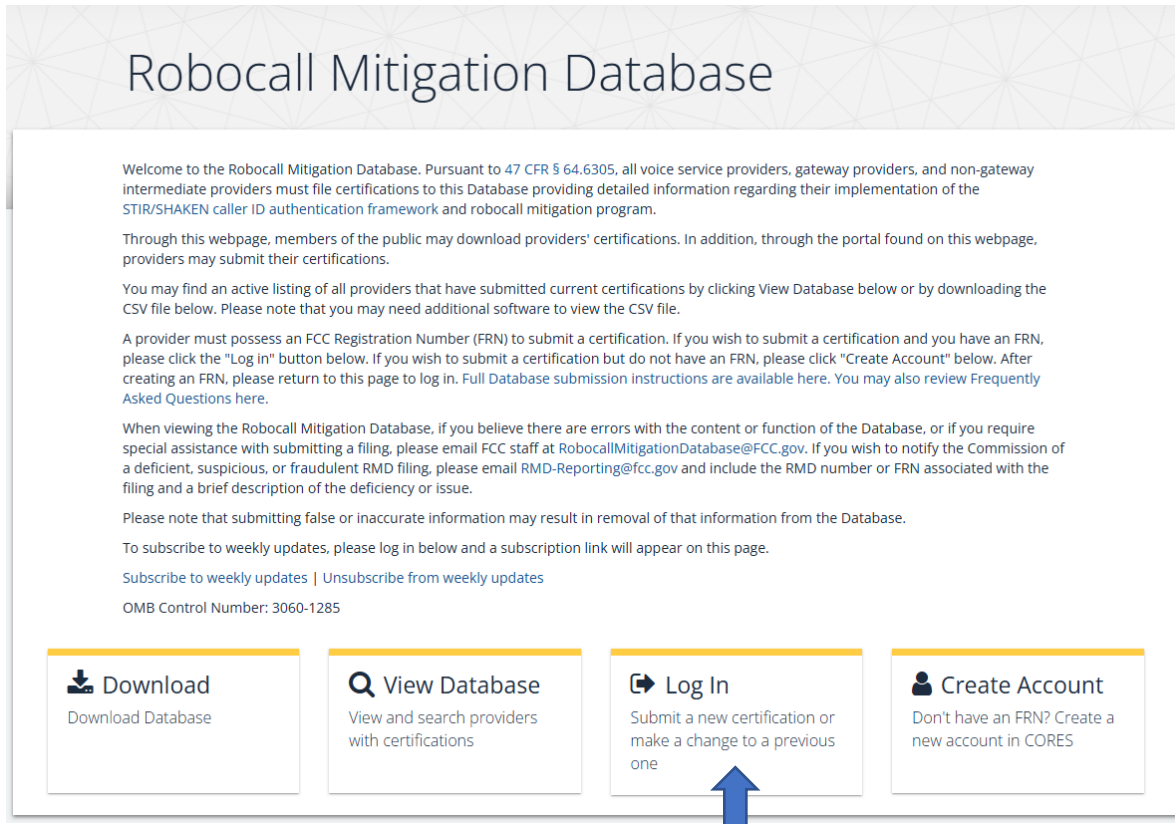


Figure 6 – Welcome Page, click “Log In” to log into the Database.

- iii. Once you are logged in, you will arrive at the Robocall Mitigation Database Landing Page. Click the “Start a New Filing” button to begin the filing process (see Figure 7).

When viewing the Robocall Mitigation Database, if you believe there are errors with the content or function of the database, or if you require special assistance with submitting a filing, please email FCC staff at RobocallMitigationDatabase@FCC.gov.

To subscribe to weekly updates, please log in below and a subscription link will appear on this page.

[Subscribe to weekly updates](#) | [Unsubscribe from weekly updates](#)

OMB Control Number: 3060-1285

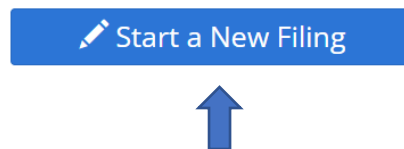


Figure 7 – Landing Page, click “Start a New Filing” to start a filing.

- iv. Once you click “Start a New Filing,” you will arrive at a new screen prompting you for your FRN (see Figure 8). Note that only business-type FRNs that are associated with the user and not already selected in the “FCC Registration Number (FRN)” field for another filing will be available for selection in the FRN drop-down box located at the top of the form. If no FRNs are available to select in the “FCC Registration Number (FRN)” field, the form cannot be completed.

New Filing

* FCC Registration Number (FRN)

Business Name

Business Address

* Type of Provider Filing

- ☐ Voice Service Provider Filing
☐ Gateway Provider Filing
☐ Non-Gateway Intermediate Provider Filing

Please separate entered values with a semicolon

* Other FRNs (enter 'None' if you have none)

* Foreign Voice Service Provider

* Other DBA Name(s) (enter 'None' if you have none)

* Principals, Affiliates, Subsidiaries, and Parent Companies (if you require more space, please provide this information in your robocall mitigation program description)

* Previous Business Names (enter 'None' if you have none)

Figure 8 – New Filing Form, Provider Details

- v. Once an FRN has been selected, the “Business Name” and “Business Address” fields will automatically populate with the business name and address associated with the selected business-type FRN in CORES. Please note that the “Business Name” and “Business Address” fields are read only. If any changes need to be made to the “Business Name” or “Business Address” fields, you must make the edits directly in CORES.
- vi. Next, you must indicate whether the filing entity is a Voice Service Provider, Gateway Provider, and/or Non-Gateway Intermediate Provider. If the provider serves more than one role in the call chain, please select all options that apply.
- vii. Foreign Voice Service Providers, including Gateway and Non-Gateway Intermediate Providers that are also Foreign Voice Service Providers, must select “Yes” from the drop-down menu in the “Foreign Voice Service Provider” field, and domestic U.S. providers must select “No.” Foreign Voice Service Providers must then select the country associated with their “Business Address” from the drop-down list found in the “Country for Business Address” field. For domestic providers, this field will auto-populate with “United States of America.”

Robocall Mitigation Database External Filing Instructions
January 2026

- viii. Please list any Principals, Affiliates, Subsidiaries, and Parent Companies in the corresponding textbox. If you require additional space, please provide this information in your robocall mitigation program description attachment (see paragraph III.a.xvi below).
- ix. Please list any other FRNs, DBA names, or previous business names associated with the filing entity in the “Other FRNs,” “Other DBA Names,” and “Previous Business Names” fields, as appropriate. When inputting multiple values into any of these fields, please separate the entered values with a semicolon. If you have none, please enter “None.”
- x. Once you enter the initial business information, scroll to the “Contact Information” section, and enter the information for your robocall mitigation point of contact (see Figure 9). These fields will ask for information including contact name, title, department, address, telephone number, and email. You can also copy the information found in the “Business Address” and “Country for Business Address” fields into the relevant contact address fields by clicking the “Contact Address Same as Business Address” box. The relevant contact address fields will then auto-populate with the information from the “Business Address” and “Country for Business Address” fields.

Contact Information

* Robocall Mitigation Contact Name

* Contact Title

* Contact Department

☐ Contact Address Same as Business Address

* Contact Street

Contact Street Continued

* Contact City

* Contact Zip Code

* Contact Telephone Number

* Contact Country

Contact State, Province, County, District, Region, etc.

Contact Phone Extension

* Contact Email

Figure 9 – New Filing Form, Contact Information Section

- xi. Once you enter the robocall mitigation contact information, scroll to the “Additional Information” section. In this section, you are required to provide information regarding the provider’s role in the call chain, information on whether the provider has been the subject of a robocall-related government action or investigation, and the provider’s Operating Company Number (OCN), if it has one.
- xii. If you checked the “Voice Service Provider Filing” checkbox, a field labeled “Voice Service Provider Role in the Call Chain” will appear (see Figure 10). You must indicate the voice service provider’s role in the call chain by selecting one (and only one) of the following four options from the drop-down menu:
 - Voice Service Provider with a STIR/SHAKEN implementation obligation serving end-users;
 - Voice Service Provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls;
 - Voice Service Provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls and serving end-users; or
 - Voice Service Provider without a STIR/SHAKEN obligation

Additional Information

*Voice Service Provider Role in the Call Chain

-- None --

-- None --

Voice Service Provider with a STIR/SHAKEN implementation obligation serving end-users

Voice Service Provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls

Voice Service Provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls and serving end-users

Voice Service Provider without a STIR/SHAKEN obligation

Figure 10 – Additional Information Section, Voice Service Provider Role in the Call Chain

If you checked the “Gateway Provider Filing” checkbox, then a field labeled “Gateway Provider Role in the Call Chain” will appear (see Figure 11). You must indicate the gateway provider’s role in the call chain by selecting one (and only one) of the following two options from the drop-down menu:

- Gateway Provider with a STIR/SHAKEN obligation; or

- Gateway Provider without a STIR/SHAKEN obligation

Additional Information

* Gateway Provider Role in the Call Chain

-- None --

-- None --

Gateway Provider with a STIR/SHAKEN obligation

Gateway Provider without a STIR/SHAKEN obligation

* Operating Company Number (OCN)

-- None --

Figure 11 – Additional Information Section, Gateway Provider Role in the Call Chain

If you checked the “Non-Gateway Intermediate Provider Filing” checkbox, then a field labeled “Non-Gateway Intermediate Provider Role in the Call Chain” will appear (see Figure 12). You must indicate the non-gateway intermediate provider’s role in the call chain by selecting one (and only one) of the following two options from the drop-down menu:

- Non-Gateway Intermediate Provider with a STIR/SHAKEN obligation; or
- Non-Gateway Intermediate Provider without a STIR/SHAKEN obligation

Additional Information

* Non-Gateway Intermediate Provider Role in the Call Chain

-- None --

-- None --

Non-Gateway Intermediate Provider with a STIR/SHAKEN obligation

Non-Gateway Intermediate Provider without a STIR/SHAKEN obligation

* Operating Company Number (OCN)

-- None --

Figure 12 – Additional Information Section, Non-Gateway Intermediate Provider Role in the Call Chain

Please note that if you checked more than one provider filing-type checkbox at the beginning of the form, then multiple dropdown menus will appear in this section for each provider-type's role in the call chain. You must select one (and only one) option from each of the drop-down menus to complete the form.

- xiii. Below the role in the call chain field(s), you will find a statement regarding the filing entity's involvement in a formal Commission, law enforcement, or regulatory agency action or investigation (see Figure 13). Please read this statement carefully. If the statement is true regarding the filing entity, you must select "Yes" from the drop-down menu. If the statement is false regarding the filing entity, you must select "No" from the drop-down menu.

Additional Information

* The filing entity has, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

-- None --

▼

Figure 13 – Additional Information Section, Prior Action or Investigation

If you select "Yes" from the drop-down menu, a textbox will appear prompting you to describe the action or investigation (see Figure 14), including (1) all law enforcement or regulatory agencies involved, (2) the date that any action or investigation was commenced, (3) the current status of the action or investigation, (4) a summary of the findings of wrongdoing made in connection with the action or investigation, and (5) whether any final determinations have been issued. You must complete this field. If you require additional space, please provide this information in your robocall mitigation program description attachment (see paragraph III.a.xvi below).

Additional Information

*The filing entity has, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

*Provide a description of any such action or investigation, including (1) all law enforcement or regulatory agencies involved, (2) the date that any action or investigation was commenced, (3) the current status of the action or investigation, (4) a summary of the findings of wrongdoing made in connection with the action or investigation, and (5) whether any final determinations have been issued (if you require more space, please provide this information in your robocall mitigation program description).

Figure 14 – Additional Information Section, Description of Prior Action or Investigation

- xiv. In the drop-down menu labeled “Operating Company Number (OCN)”, please indicate if the provider has an OCN by selecting either “Yes” or “No” (see Figure 15).

Additional Information

*The filing entity has, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

*Operating Company Number (OCN)

Yes

-- None --

Yes

No

Figure 15 – Additional Information Section, Operating Company Number

If you select “Yes” from the drop-down menu, a textbox will appear prompting you to manually enter the provider’s OCN (see Figure 16).

Additional Information

*The filing entity has, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

*Operating Company Number (OCN)

*OCN

Figure 16 – Additional Information Section, Enter Operating Company Number

- xv. Once you have completed the additional information section, scroll to the “Certifications” section. Here you will be required to select a certification option corresponding to the provider’s level of STIR/SHAKEN implementation. If you checked more than one provider filing-type checkbox at the beginning of the form, you must select one certification option from each set of options for the provider filing-type(s) you selected. Please read the certification language carefully for each option you select.

Voice Service Providers – Please select one of the three Voice Service Provider certification options from the “Voice Service Provider Certification” section of the form (see Figure 17).

Certification

***Voice Service Provider Certification (Choose one)**

- ☒ Option 1: Complete STIR/SHAKEN Implementation. The filer certifies that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with 47 CFR § 64.6301.
- ☐ Option 2: Partial STIR/SHAKEN Implementation. The filer certifies that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it originates on that portion of its network are compliant with 47 CFR § 64.6301(a) and (b).
- ☐ Option 3: No STIR/SHAKEN Implementation. The filer certifies that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

Figure 17 – Certification Section, Voice Service Provider Certification

Note that if you select “Option 2” or “Option 3,” a textbox will appear requiring you to state the rule that exempts the filer from compliance and explain in detail why this exemption applies to the filer (see Figure 18). If you require additional space, please provide this information in your robocall mitigation program description attachment (see paragraph III.a.xvi below).

Certification

*Voice Service Provider Certification (Choose one)

- ☐ Option 1: Complete STIR/SHAKEN Implementation. The filer certifies that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with 47 CFR § 64.6301.
- ☒ Option 2: Partial STIR/SHAKEN Implementation. The filer certifies that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it originates on that portion of its network are compliant with 47 CFR § 64.6301(a) and (b).
- ☐ Option 3: No STIR/SHAKEN Implementation. The filer certifies that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

*State the rule that exempts the filer from compliance and explain in detail why that exemption applies to the filer (if you require more space, please provide this information in your robocall mitigation program description).

Figure 18 – Certification Section, Voice Service Provider Certification, State Rule Exemption

Gateway Providers – Please select one of the three Gateway Provider certification options from the “Gateway Provider Certification” section of the form (see Figure 19).

Certification

* Gateway Provider Certification (Choose one)

- ☐ Option 1: Complete STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(b), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with 47 CFR § 64.6302.
- ☐ Option 2: Partial STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(b), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it carries or processes on that portion of its network are compliant with 47 CFR § 64.6302.
- ☐ Option 3: No STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(b), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls.

Figure 19 – Certification Section, Gateway Provider Certification

Note that if you select “Option 2” or “Option 3,” a textbox will appear requiring you to state the rule that exempts the filer from compliance and explain in detail why this exemption applies to the filer (see Figure 20). If you require additional space, please provide this information in your robocall mitigation program description attachment (see paragraph III.a.xvi below).

Certification

*** Gateway Provider Certification (Choose one)**

- ☐ Option 1: Complete STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(b), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with 47 CFR § 64.6302.
- ☐ Option 2: Partial STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(b), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it carries or processes on that portion of its network are compliant with 47 CFR § 64.6302.
- ☒ Option 3: No STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(b), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls.

*** State the rule that exempts the filer from compliance and explain in detail why that exemption applies to the filer (if you require more space, please provide this information in your robocall mitigation program description).**

Figure 20 – Certification Section, Gateway Provider Certification, State Rule Exemption

Non-Gateway Intermediate Providers – Please select one of the three Non-Gateway Intermediate Provider certification options from the “Non-Gateway Intermediate Provider Certification” section of the form (see Figure 21).

Certification

*** Non-Gateway Intermediate Provider Certification (Choose one)**

- ☐ Option 1: Complete STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(c), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with 47 CFR § 64.6302.
- ☐ Option 2: Partial STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(c), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it carries or processes on that portion of its network are compliant with 47 CFR § 64.6302.
- ☐ Option 3: No STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(c), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls.

Figure 21 – Certification Section, Non-Gateway Intermediate Provider Certification

Note that if you select “Option 2” or “Option 3,” a textbox will appear requiring you to state the rule that exempts the filer from compliance and explain in detail why this exemption applies to the filer (see Figure 22). If you require additional space, please provide this information in your robocall mitigation program description attachment (see paragraph III.a.xvi below).

Certification

* Non-Gateway Intermediate Provider Certification (Choose one)

- ☐ Option 1: Complete STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(c), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with 47 CFR § 64.6302.
- ☒ Option 2: Partial STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(c), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it carries or processes on that portion of its network are compliant with 47 CFR § 64.6302.
- ☐ Option 3: No STIR/SHAKEN Implementation. The filer certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(c), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. The filer also certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls.

* State the rule that exempts the filer from compliance and explain in detail why that exemption applies to the filer (if you require more space, please provide this information in your robocall mitigation program description).

Figure 22 – Certification Section, Non-Gateway Intermediate Provider Certification, State Rule Exemption

- xvi. All providers are required to upload a robocall mitigation program description (see Figure 23).
- The robocall mitigation program description must meet the requirements of 47 CFR § 64.6305(d)(ii)-(iii) (for voice service providers), (e)(ii)-(iii) (for gateway providers), and/or (f)(ii)-(iii) (for non-gateway intermediate providers). More information regarding the required contents of the robocall mitigation plan is available in DA 24-73 ([Filing Instructions Public Notice](#)).
 - If you would like to designate a portion of your mitigation plan as confidential and you have filed such a request in WC Docket No. 17-97 of the Electronic Comment Filing System (ECFS), you can check the box stating that you request that some of the filing's contents be

kept confidential. Once checked, you must upload both confidential (i.e., unredacted) and non-confidential (i.e., redacted) versions of your mitigation plan into the Database. Confidential (i.e., unredacted) plans are not published to the Database and are only viewable by FCC staff. Non-confidential (i.e., redacted) plans are published to the Database and are viewable by the public.

- All documents must be uploaded in PDF format.

Upload Robocall Mitigation Program Description

- ☐ The filer requests that some of the filing's contents be kept confidential and has filed such a request in the Electronic Comment Filing System (ECFS)

Document must be in PDF format. For further information regarding the required contents of the robocall mitigation program description, please refer to the Robocall Mitigation Database filing instructions, available at <https://www.fcc.gov/sites/default/files/rmd-instructions.pdf>.

*PDF

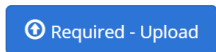


Figure 23 – Upload Robocall Mitigation Program Description Section

- xvii. To submit a filing, the declaration statement must be checked and the “Officer e-Signature” box must be signed (see Figure 24).

Declaration

- ☐ * I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on 1/16/2024.

*Officer e-Signature

Figure 24 – Declaration Section

- xviii. Once all required fields have been completed, click the “Submit” button to submit your filing (see Figure 25).

Declaration

☒ * I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on 1/16/2024.

*Officer e-Signature

Jane Doe

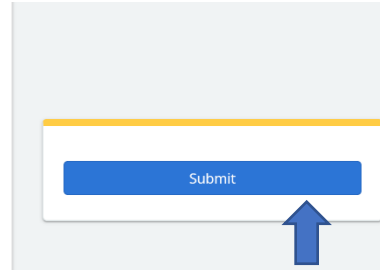


Figure 25 – Click “Submit” to submit your filing

- xix. Once you click “Submit,” you will be directed to a page confirming your submission (see Figure 26).

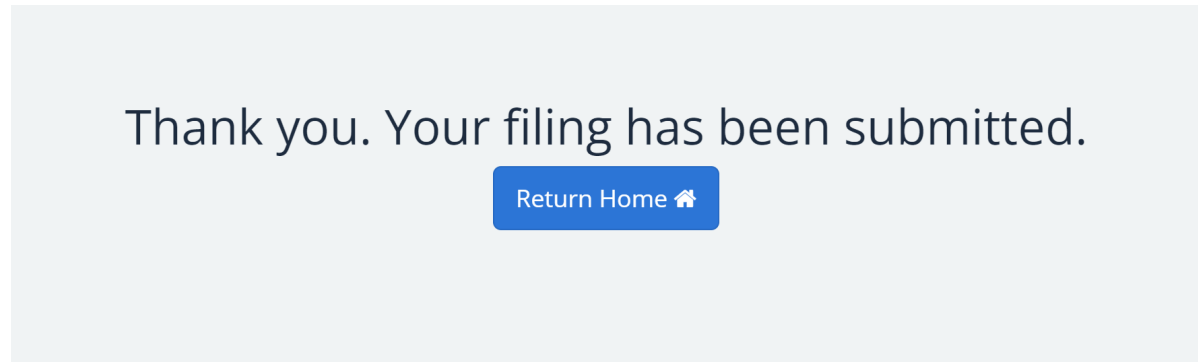


Figure 26 – Confirmation Page

- xx. Click the “Return Home” button to go back to the Landing Page. Once you are back on the Landing Page, you can view, revise, or delete your submitted filing (see Figure 27).

My Filings				
Number	FCC Registration Number (FRN)	Business Name ^	Business Address	Robocall Mitigation Contact Name
	0003770732	Gulf Coast Broadcasting Co. Inc.	26946 Martinique Drive PO Box 679 Orange...	ff
< > Rows 1 - 1 of 1				

Figure 27 – Landing Page Displaying Submitted Filings

- xxi. To view the details of a previously submitted filing, click the filing listed on the Landing Page to open the submission form. This will display a read-only view of the information that was submitted, along with options to delete or revise the filing in the top right corner of the form (see Figure 28). The revise and delete options are addressed in Sections III.b and III.c, below.

Robocall Mitigation Database External Filing Instructions
January 2026

Delete

Revise

Attachments

Download PDF

Federal Communications Commission

Attachments

Test PDF.pdf

Robocall Mitigation Database

Number

RMD0010585

Provider Details

* FCC Registration Number (FRN)

0000000018

* Business Name

Federal Communications Commission

Business Address

445 12th ST, NW
Washington DC 20554

Figure 28 – Click a filing to display a detailed view of what was submitted

b. Revising a Filing

- i. To revise a submitted filing, visit <https://fccprod.servicenowservices.com/rmd> and click on the “Log In” button (see Figure 29).

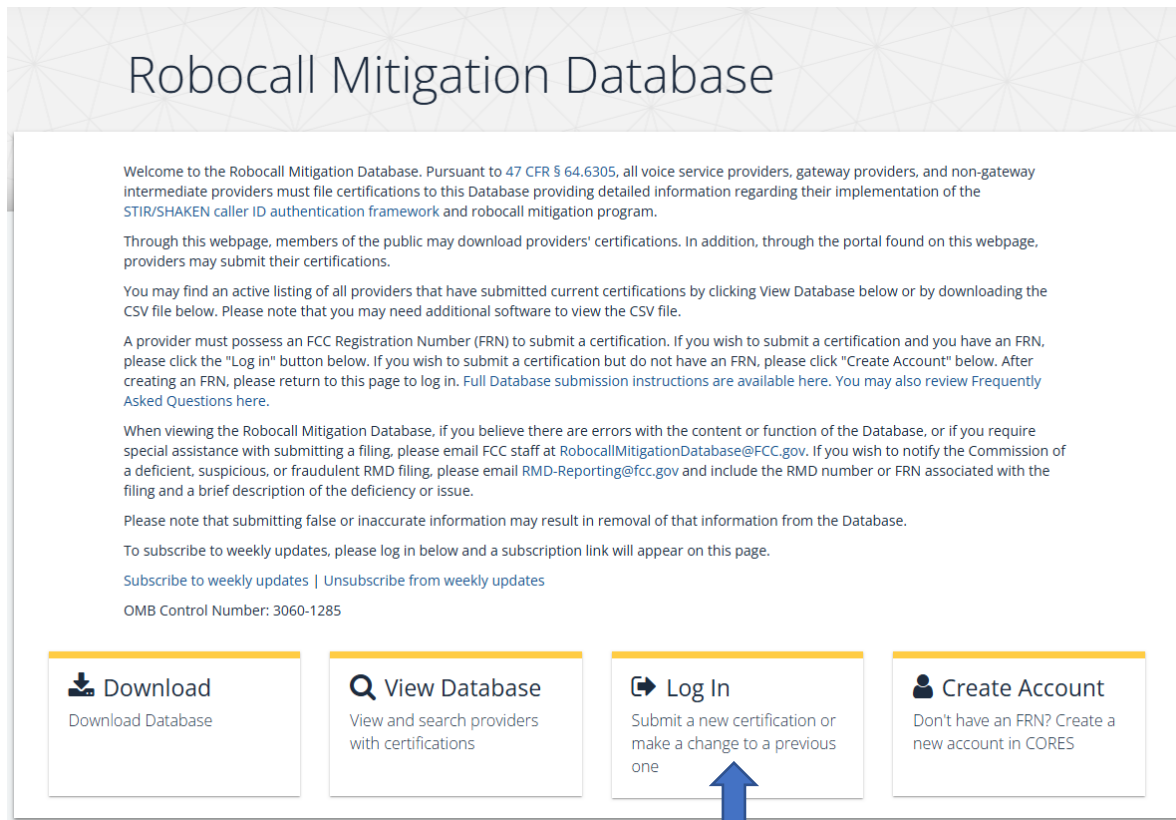


Figure 29 – Welcome Page, click “Log In” to log into the Database

- ii. Once you are logged in, you will see a list of your submitted filings. Click the filing you want to revise, then click the “Revise” button at the top right of the form (see Figure 30).

Robocall Mitigation Database External Filing Instructions
January 2026

Robocall Mitigation Database External Filing form. The form includes fields for Attachments (Test PDF.pdf), Robocall Mitigation Database Number (RMD0010585), Provider Details (FCC Registration Number (FRN) 0000000018, Business Name Federal Communications Commission, Business Address 445 12th ST, NW Washington DC 20554), and buttons for Delete, Revise, Attachments, and Download PDF.

Figure 30 – Submitted Filing, click the “Revise” button to revise the filing

- iii. Once you click the “Revise” button, you can make changes to the editable fields on the form and upload a revised robocall mitigation program description.
- iv. Note that you will not be able to edit the “FRN,” “Business Name,” or “Business Address” fields. If any changes need to be made to the “Business Name” or “Business Address” fields, please make those edits directly in CORES. In order for the Database to update with any changes made in CORES, first log out of the Database and then log back in. Once logged in, select the submitted filing from the Landing Page, click “Revise” and the changes will be reflected.
- v. Once all revisions have been made, you will need to re-certify and re-submit the filing. This means the “Declaration” section must be completed again in order to submit the revised filing (see Figure 31).

Declaration

☒ * I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on 1/16/2024.

* Officer e-Signature

Jane Doe

Submit

Figure 31 – Declaration Section must be completed before submitting a revised filing

- vi. Once you click “Submit,” you will be directed to the Confirmation Page (see Figure 32).

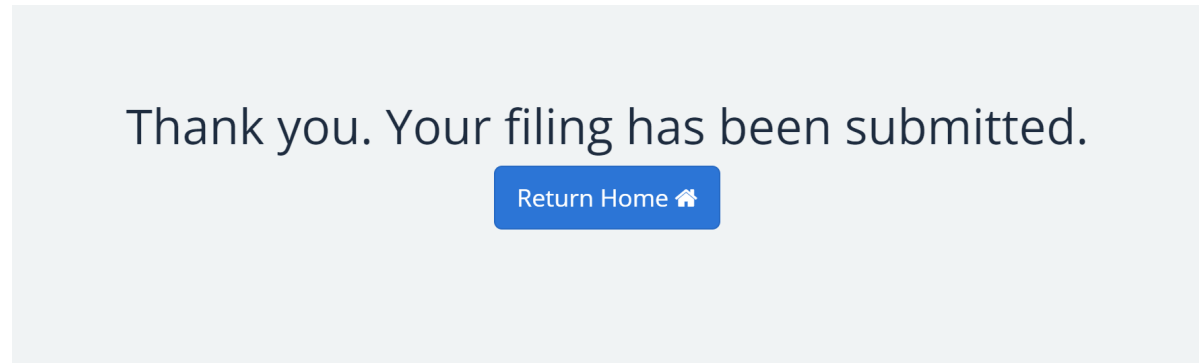


Figure 32 – Confirmation Page

- vii. Click the “Return Home” button to go back to the Landing Page. Once you are back on the Landing Page, you can view, revise, or delete your submitted filing(s).

c. Submitting an Annual Recertification

- i. Existing filers are required to recertify their filings each year by March 1. Annual Recertifications can only be completed during the Annual Recertification filing window, which opens each year on February 1.
- ii. To submit the required Annual Recertification during the filing window, visit <https://fccprod.servicenowservices.com/rmd> and click on the “Log In” button (see Figure 33).

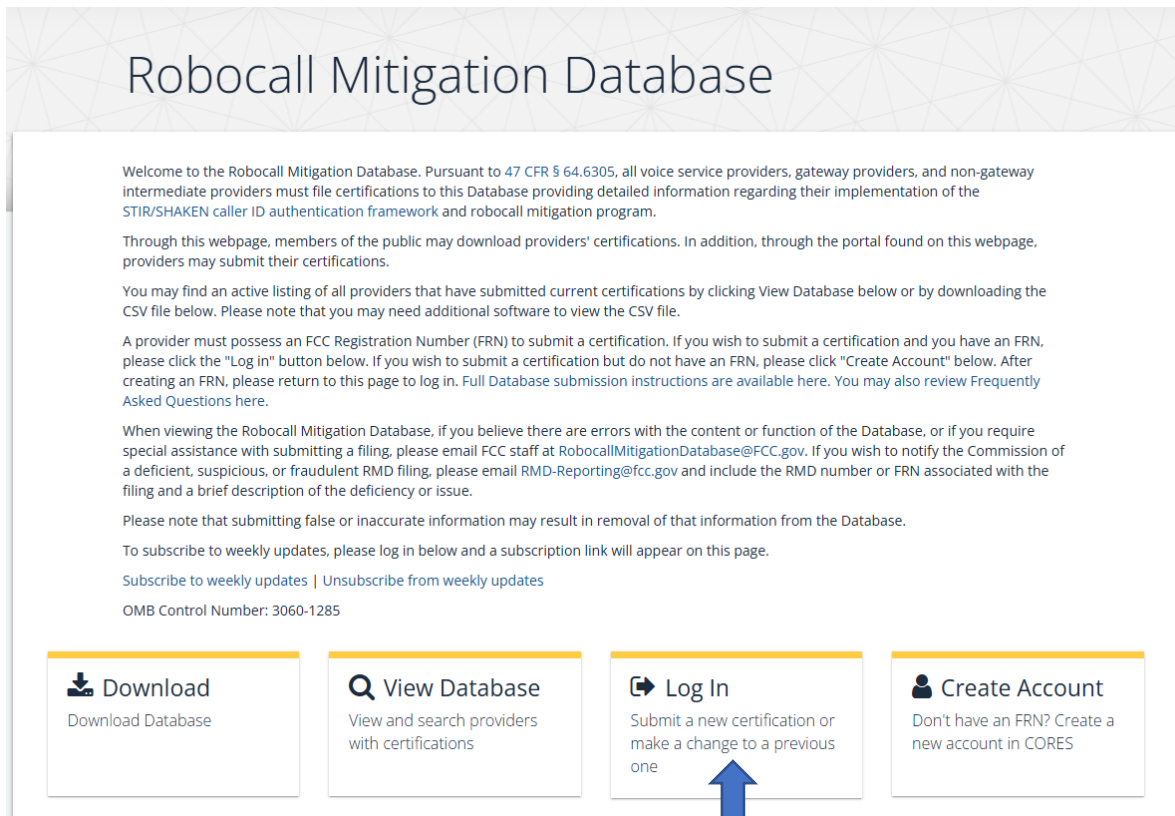


Figure 33 – Welcome Page, click “Log In” to log into the Database

- viii. Once you are logged in, you will see a list of your submitted filings. Click the filing you want to recertify from the list of submitted filings, then click the “Recertify” button at the top right of the form (see Figure 34). *Please note – the “Recertify” button will only appear during the Annual Recertification filing window beginning on February 1 each year.

The screenshot shows a web form for filing a Robocall Mitigation Database entry. At the top right, there are three buttons: "Delete", "Revise", and "Recertify". Below these, there is a "Download PDF" button with a download icon. The form itself is titled "Federal Communications Commission" and "Robocall Mitigation Database Filings". It includes an "Attachments" section with a link to "Robocall Mitigation Program Description.pdf". The "Number" field contains "RMD0022167". The "Provider Details" section includes an "FCC Registration Number (FRN)" field with "0031022809" and a "Business Name" field with "Federal Communications Commission".

Figure 34 – Submitted Filing, click the “Recertify” button to revise the filing

- ix. Once you click the “Recertify” button, you may make any necessary changes to the editable fields on the form and upload a revised robocall mitigation program description (see Section III.b above).
- x. To complete the recertification, fill out the “Declaration” section and click “Submit” (see Figure 35).

Declaration

☒ * I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on 1/16/2024.

* Officer e-Signature

Jane Doe

The screenshot shows a blue button with the text "Submit" in white, centered on a light gray background.

Figure 35 – Declaration Section must be completed before submitting an Annual Recertification.

- xi. Once you click “Submit,” you will be directed to the Confirmation Page (see Figure 36).

Thank you. Your filing has been submitted.

[Return Home](#)

Figure 36 – Confirmation Page

Robocall Mitigation Database External Filing Instructions
January 2026

- xii. Click the “Return Home” button to go back to the Landing Page. Once you are back on the Landing Page, you can view, revise, or delete your submitted filing(s).
- xiii. To view the date a submitted filing was last recertified, click on the filing you wish to view from the list of submitted filings. The “Last Recertified” date will appear at the top right of the form (see Figure 37). *Please note – a filing can only be recertified once during the Annual Recertification filing window.

The screenshot displays a web form for the Robocall Mitigation Database. At the top right, there are two buttons: 'Delete' and 'Revise'. Below these, the text 'Last Recertified: 2026-01-14' is shown. A blue arrow points upwards towards this date. To the right of the date is the text 'Attachments' and a 'Download PDF' button. The main body of the form contains the following sections:

- Federal Communications Commission**
- Attachments**
 - Robocall Mitigation Program Description.pdf
- Robocall Mitigation Database Filings**
- Number**
 - RMD0022164
- Provider Details**
 - *FCC Registration Number (FRN)
 - 0031022809
 - *Business Name
 - Federal Communications Commission

Figure 37 – Submitted Filing, view the “Last Recertified” date

d. Deleting a Filing

- i. To delete a submitted filing, visit: <https://fccprod.servicenowservices.com/rmd> and click on the “Log In” button (see Figure 38).

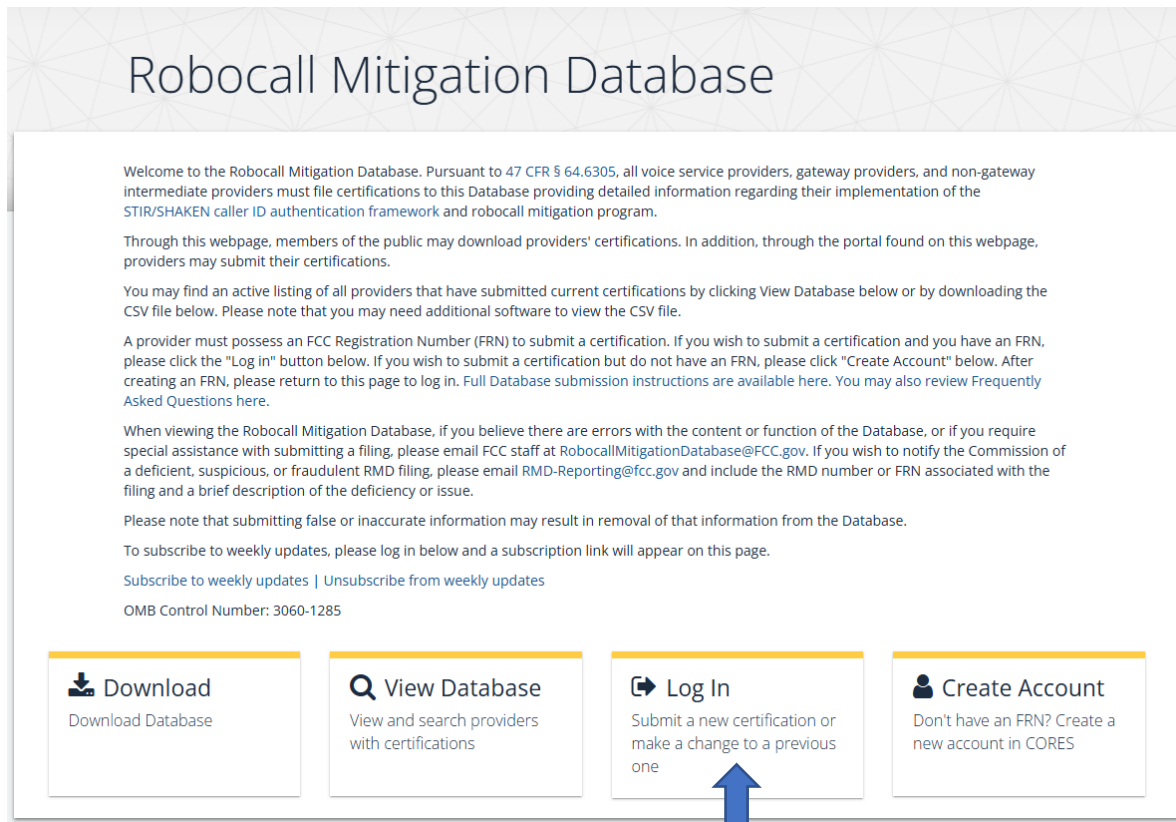
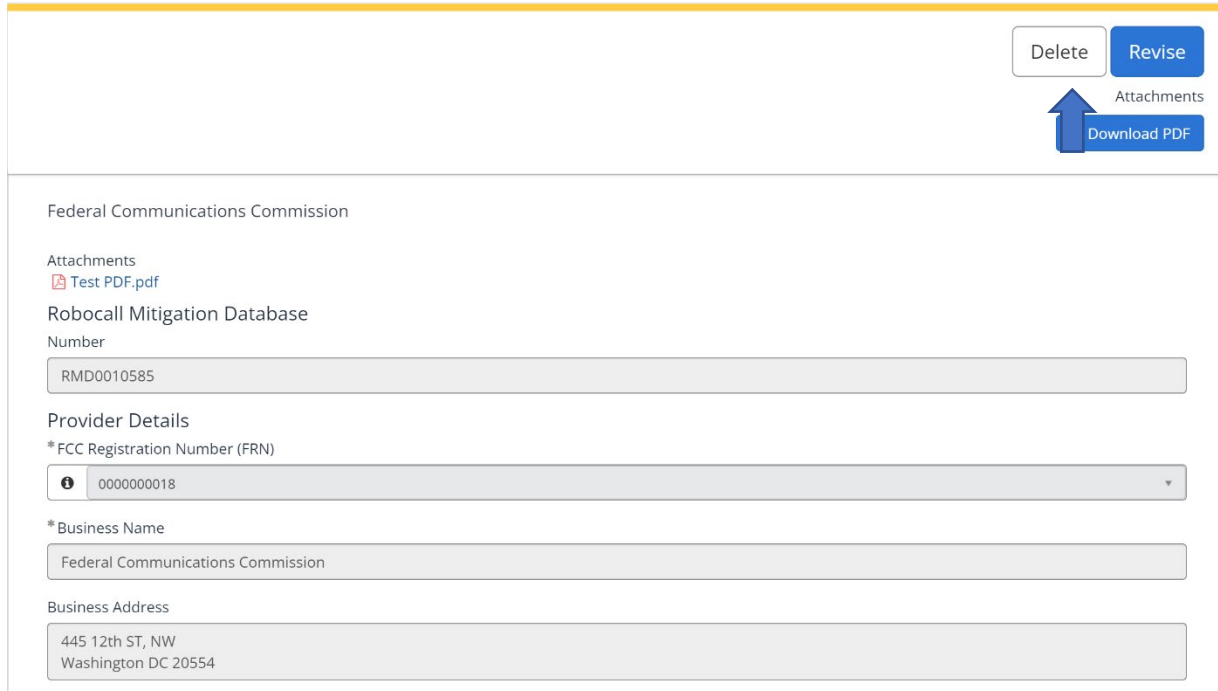


Figure 38 – Welcome Page, click “Log In” to log into the Database

- ii. Once you are logged in, you will see a list of your submitted filings. Click the filing you want to delete from the list of submitted filings, then click the “Delete” button at the top right of the form (see Figure 39).

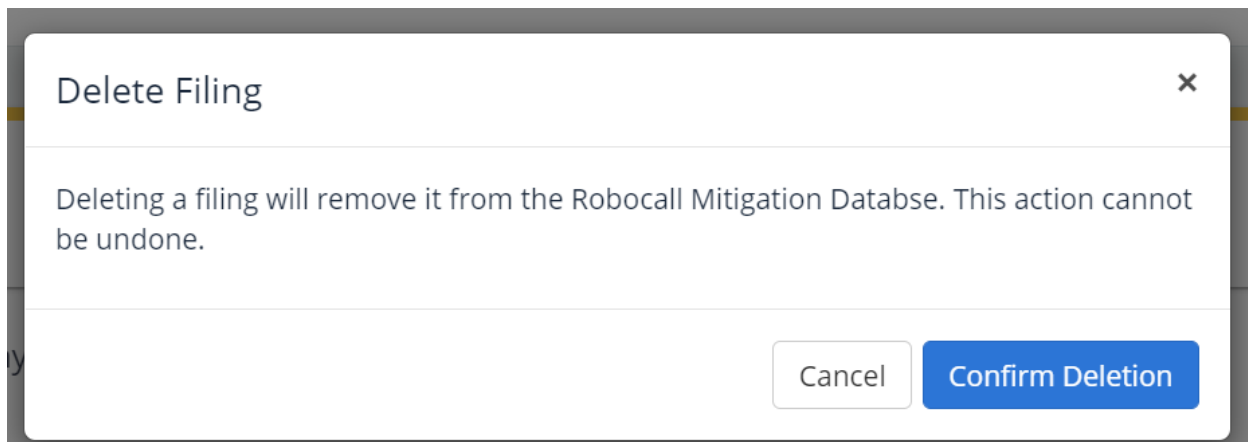


The screenshot shows a web form for submitting a filing to the Robocall Mitigation Database. At the top right, there are buttons for "Delete" and "Revise". Below these is an "Attachments" section with a blue arrow icon and a "Download PDF" button. The form fields are as follows:

- Federal Communications Commission**
- Attachments**
 - Test PDF.pdf
- Robocall Mitigation Database**
- Number**
 - RMD0010585
- Provider Details**
 - *FCC Registration Number (FRN)**
 - 0000000018
 - *Business Name**
 - Federal Communications Commission
 - Business Address**
 - 445 12th ST, NW
 - Washington DC 20554

Figure 39 – Submitted Filing, click “Delete” to delete the filing

- iii. Once you click the “Delete” button, a pop-up window will appear giving you the option to cancel or confirm the deletion (see Figure 40).



The screenshot shows a pop-up window titled "Delete Filing" with a close button (X) in the top right corner. The text inside the window reads: "Deleting a filing will remove it from the Robocall Mitigation Databse. This action cannot be undone." At the bottom right, there are two buttons: "Cancel" and "Confirm Deletion".

Figure 40 – Deletion Pop-Up Window, click “Confirm Deletion” to delete the filing

- iv. Once you click “Confirm Deletion,” the filing will be removed from the Robocall Mitigation Database and you will be directed back to the Landing Page. If you click “Cancel,” the pop-up window will disappear, the filing will not be removed from the Robocall Mitigation Database, and you will return to the submitted filing.