PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov

DA 26-72
Released: January 22, 2026

WIRELINE COMPETITION BUREAU ANNOUNCES OMB APPROVAL AND EFFECTIVE DATES FOR ROBOCALL MITIGATION DATABASE (RMD) RULES, PROVIDES GUIDANCE FOR FILING IN THE RMD, REMINDS RMD FILERS OF THEIR MARCH 1, 2026, ANNUAL RECERTIFICATION REQUIREMENT, AND ESTABLISHES A REPORTING MECHANISM FOR RMD DEFICIENCIES

WC Docket No. 24-213, MD Docket No. 10-234

In this Public Notice, the Wireline Competition Bureau (Bureau) announces Office of Management and Budget (OMB) approval of and the effective dates for revised Robocall Mitigation Database (RMD) filing requirements and related rules adopted in the *Robocall Mitigation Database Report and Order*, including increased base forfeiture amounts for submission of false or inaccurate information into the RMD and for failure to update information in the RMD.[1] The Bureau also announces its implementation of certain Commission directives in the *Robocall Mitigation Database Report and Order*. Additionally, the Bureau reminds RMD filers of their requirement under the new rules to recertify their RMD filings by **March 1, 2026**, and announces that the recertification filing window will open on February 1, 2026. Further information on each of these actions is described herein.

Guidance and Filer Education. The Bureau has attached to this Public Notice additional guidance in the form of a "Frequently Asked Questions" document to assist RMD filers with their robocall mitigation compliance obligations. In the *Robocall Mitigation Database Report and Order*, the Commission directed the Bureau to issue such guidance, agreeing with commenters that such guidance may assist providers in interpreting the Commission's requirements and improve the accuracy of the RMD, decrease filing deficiencies, and save the Commission's and providers' time and resources.[2] The Commission specifically instructed the Bureau to address requests in the record to provide filers that meet the definition of "foreign voice service providers" with interpretive guidance as to how to complete the RMD certification form so that such filers can consistently identify themselves as foreign providers in their RMD filings.[3] The Commission also directed the Bureau to clarify how providers' obligation to certify whether they have been the subject of a previous robocall investigation or enforcement action applies to affiliates and principals.[4] To fulfill its obligation, the Bureau developed a "Frequently Asked Questions" document, which is attached as Appendix A and available at

[1] *Improving the Effectiveness of the Robocall Mitigation Database, Amendment of Part I of the Commission's Rules Concerning Practice and Procedure, Amendment of CORES Registration System*, WC Docket No. 24-213, MD Docket No. 10-234, Report and Order, 40 FCC Rcd 599 (2025) (*Robocall Mitigation Database Report and Order*).

[2] *Id*. at 611, para. 27.

[3] *Id*. at 611-12, para. 29.

[4] *Id*. at 612, para. 30.

https://www.fcc.gov/sites/default/files/rmd-faq.pdf.[5]

Reporting Mechanism for Deficient Filings. The Bureau has established a mechanism stakeholders can use to report to the Commission deficient filings in the RMD in the form of an email address, which will be monitored by FCC staff. In the *Robocall Mitigation Database Report and Order*, the Commission directed the Bureau to establish a dedicated reporting mechanism for deficient filings in order to enhance the integrity and usefulness of the RMD.[6] The Commission further directed the Bureau, in consultation with the Office of the Managing Director and the Enforcement Bureau, to determine the appropriate mechanism for the Commission to receive reports of deficient filings.[7] Additionally, the Commission delegated to the Bureau the authority, in consultation with the Office of the Chief Information Officer and the Senior Agency Official for Privacy, to specify the form and format of any such submissions and to make any necessary changes to the RMD portal and interface in connection with the reporting mechanism.[8] In accordance with these directives, the Bureau created an email address to which parties can submit information regarding deficient robocall mitigation database filings. Such information can be sent to **RMD-Reporting@fcc.gov**. While the Bureau has not established specific reporting content and format requirements at this time, submissions will be most helpful if they include the business name, FRN, and RMD number associated with a filing, and a brief description of the alleged deficiency.

Multi-Factor Authentication. The Bureau announces that multi-factor authentication has been established for RMD access. In the *Robocall Mitigation Database Report and Order*, the Commission directed the Bureau and OMD "to develop a two-factor (or more) authentication solution for accessing the Database" to better secure the RMD.[9] The Commission further directed that such solution offer users the option of using phishing-resistant authentication (*i.e.*, provide support for Web-Authentication-based approaches, such as security keys).[10] Filers must now use multi-factor authentication to access the RMD and have the option of using phishing resistant authentication. Instructions for logging into the RMD are available in the RMD filing instructions at https://www.fcc.gov/sites/default/files/rmd-instructions.pdf.

Annual Recertification. The Bureau announces that the effective date of 47 CFR § 64.6305(h) is February 5, 2026, reminds filers of their obligation under the rule to recertify their RMD filings by **March 1, 2026**, and announces the recertification window will open on February 1, 2026. Section 64.6305(h) requires providers to certify annually, on or before March 1, that any information submitted to the RMD is true and correct.[11] Section 64.6305(h) becomes effective 30 days after Federal Register publication, which occurred on January 6, 2026, making the effective date February 5, 2026.[12] The filing

[5] Although the Commission delegated to the Bureau authority to determine the form of the guidance, it referenced that in other contexts, such guidance has been provided through Frequently Asked Questions and other similar documents posted to the Commission's website. *Id*. at 611, para. 28. The RMD "Frequently Asked Questions" document may be updated at the Bureau's discretion.

[6] *Id.* at 609, para. 24.

[7] *Id.* at 610, para. 26.

[8] *Id.*

[9] *Id.* at 616, para. 39.

[10] *Id.*

[11] 47 CFR § 64.6305(h); *see also Robocall Mitigation Database Report and Order*, 40 FCC Rcd at 615-16, paras. 37-38 and Appx. A. We remind filers that they also must update their RMD filings within 10 business days of any change. *See* 47 CFR § 64.6305(d)(5), (e)(5), (f)(5); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2595-96, para. 42 (2023) (*Sixth Caller ID Authentication Report and Order*).

[12] The Commission stated in the *Robocall Mitigation Database Report and Order* that the rules it adopted would become effective 30 days after publication in the Federal Register, except for section 64.6305(h), as it may contain

(continued….)

window for the first annual recertification will open on February 1, 2026, and RMD filers must complete their annual recertifications by **March 1, 2026**. Instructions for completing the annual certification requirement are available in the RMD filing instructions at https://www.fcc.gov/sites/default/files/rmd-instructions.pdf.

When completing their recertifications, providers must ensure that the information contained in their RMD filings is accurate and truthful, including with respect to the certifications required by the Commission's rules. Notably, the certification options relating to complete and partial STIR/SHAKEN implementation contain recent modifications adopted in the *Eighth Caller ID Authentication Report and Order* that became effective on September 18, 2025.[13] Providers must make the required STIR/SHAKEN implementation certification selection(s) for each role they play in the call path and should carefully review the certification option(s) they have selected to ensure they correctly certify to compliance with the modified Commission rules.

Application Fee. The Bureau notes that the requirement to submit an application fee as required by the amendment to 47 CFR § 1.1105 is not yet effective. The amendment to section 1.1105 requires filers to submit a $100 application fee for initial submissions and required annual recertifications in the RMD.[14] The Commission stated in the *Robocall Mitigation Database Report and Order* that the rules it adopted would become effective 30 days after publication in the Federal Register, except for section 1.1105, "which requires notice to Congress pursuant to section 9A(b)(2) of the Communications Act, 47 U.S.C. § 159A(b)(2), and also requires certain updates to the FCC's information technology systems and internal procedures . . . ."[15] The Commission will publish a notice announcing when it has completed these steps and when the application fee requirement will become effective.

Base Forfeiture Amount for False or Inaccurate RMD Filing Information. The Bureau announces that the effective date of the amendment to 47 CFR § 1.80 is February 5, 2026. This amendment increases the base forfeiture amount to $10,000 for each violation for filers that submit false or inaccurate information to the RMD and sets a base forfeiture amount of $1,000 for failure to update the RMD within 10 business days for information that has changed.[16] The amendment also provides that these violations continue until cured; accordingly, forfeitures shall be assessed on a daily basis up to the

---

modifications to existing information collection requirements that require review by OMB under the Paperwork Reduction Act. *Robocall Mitigation Database Report and Order*, 40 FCC Rcd at 624, para. 58. OMB completed its review on August 11, 2025, prior to Federal Register publication, so the effective date for the new rule defaults to 30 days after Federal Register publication. *See* Notice of OMB Action, OMB Control No. 3060-1285 (August 11, 2025), https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202505-3060-029#. The annual recertification requirement was submitted to and approved by OMB as a substantive information collection modification even though the *Robocall Mitigation Database Report and Order* stated that it may only contain non-substantive modifications and did not contain new or substantively modified information collection requirements. *See id.*; *Robocall Mitigation Database Report and Order*, 40 FCC Rcd at 623-24, para. 54.

[13] *See* FCC, Call Authentication Trust Anchor, Eighth Report and Order, 90 Fed. Reg. 40241 (Aug. 19, 2025); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Eighth Report and Order, 39 FCC Rcd 12894 (2024) (*Eighth Caller ID Authentication Report and Order*). Among other things, the *Eighth Caller ID Authentication Report and Order* adopted modifications to the caller ID authentication requirements for voice service providers and intermediate providers contained in 47 CFR § 64.6301 and 47 CFR § 64.6302, respectively. *See id.* at 12927-28, App. A.

[14] *See Robocall Mitigation Database Report and Order*, 40 FCC Rcd at 612-15, paras. 32-36. There is no application fee associated with routine updates to filings to reflect changes to the underlying information pursuant to 47 CFR § 64.6305(d)(5), (e)(f), and (f)(5).

[15] *See Robocall Mitigation Database Report and Order*, 40 FCC Rcd at 624, para. 58.

[16] *See id*. at 605, para. 14.

statutory maximum for continuing violations.[17] The Commission stated in the *Robocall Mitigation Database Report and Order* that this rule amendment would become effective 30 days after publication in the Federal Register.[18] The *Robocall Mitigation Database Report and Order* was published in the Federal Register on January 6, 2026, making the effective date February 5, 2026.

CORES Information Updates. The Bureau announces that the effective date of the amendment to 47 CFR § 1.8002(b)(2) is February 5, 2026. This amendment requires that all entities and individuals that register with the Commission to obtain an FCC Registration Number (FRN) in the Commission Registration System (CORES), which is required in order to submit filings to the RMD, or for any other purpose related to their FRN registration, update any information submitted to CORES within 10 business days of any change to that information.[19] The amendment to section 1.8002(b)(2) becomes effective 30 days after Federal Register publication, which occurred on January 6, 2026, making the effective date February 5, 2026.[20]

For further information regarding the RMD rules, please contact Merry Wulff, Wireline Competition Bureau, Competition Policy Division, at (202) 418-1084 or by email at Merry.Wulff@fcc.gov.

[17] *See id*. at 605, para. 14; *see also* 47 U.S.C. § 503(b) (setting statutory maximums for violations of the Act and Commission rules).

[18] *See Robocall Mitigation Database Report and Order*, 40 FCC Rcd at 624, para. 58.

[19] *See id*. at 604, para. 13. Although, in general, a CORES user may register for an individual or business-type FRN, only a business-type FRN can be used to submit a filing in the RMD.

[20] The Commission stated in the *Robocall Mitigation Database Report and Order* that the rules it adopted would become effective 30 days after publication in the Federal Register, except for the amendment to section 1.8002(b)(2), as it may contain modifications to existing information collection requirements that require review by OMB under the Paperwork Reduction Act. *Robocall Mitigation Database Report and Order*, 40 FCC Rcd at 624, para. 58. OMB completed its review and granted approval of the information collection on May 27, 2025, prior to Federal Register publication, so the effective date for the rule amendment defaults to 30 days after Federal Register publication. *See* Notice of OMB Action, OMB Control No. 3060-0918 (May 27, 2025), https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202505-3060-034#.

APPENDIX A

Robocall Mitigation Database
Frequently Asked Questions For Filers

Last updated January 20, 2026

Robocall Mitigation Database
Frequently Asked Questions For Filers

1) Who must file?

- All voice service providers and intermediate providers, including gateway providers, are required to file in the Robocall Mitigation Database (RMD).
- An affiliate or subsidiary of a filing entity that independently meets the definition of a voice service provider or intermediate provider should submit its own RMD filing. An affiliate is an individual or entity that directly or indirectly owns or controls, is owned or controlled by, or is under common ownership or control with, another individual or entity. *See* 47 U.S.C § 153(2).
- To submit a filing in the RMD, a provider must have its own FCC Registration Number (FRN)—a 10-digit unique identifying number that is assigned to entities doing business with the FCC. An FRN can be registered and managed using the COmmission REgistration System (CORES). For more information regarding CORES, visit https://www.fcc.gov/licensing-databases/commission-registration-system-fcc.
- For the purposes of the RMD, a **voice service provider** is any entity that provides any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end-user using resources from the North American Numbering Plan (NANP) or any successor. An **intermediate provider** is any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point insofar as that entity neither originates nor terminates that traffic, and includes gateway providers. A **gateway provider** is any U.S.-based intermediate provider that receives a call directly from a foreign provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider. *See* 47 CFR § 64.6300. A **non-gateway intermediate provider** is any entity that is an intermediate provider that is not a gateway provider.
- Any provider that meets these definitions, including voice over Internet protocol (VoIP) resellers and mobile virtual network operators (MVNOs), must file in the RMD.

2) Do foreign providers need to file?

- Intermediate providers and voice service providers can only accept calls that use U.S. NANP resources in the caller ID field directly from a foreign voice service provider or foreign intermediate provider if the foreign provider's filing appears in the RMD and has not been removed from the RMD pursuant to an enforcement action. *See* 47 CFR § 64.6305(g)(2). Accordingly, although foreign providers may, but are not required to, implement STIR/SHAKEN in their networks, foreign providers that send calls using U.S.

NANP numbers to U.S. providers must submit a filing in the RMD in order for their traffic to be accepted by domestic intermediate and voice service providers.

- When completing the RMD submission form, foreign providers can certify to "Option 3 – No STIR/SHAKEN Implementation" and in the exemption field indicate that it is a foreign provider.

3) Who should identify as a "foreign voice service provider" on the RMD submission form?

- A "foreign voice service provider" is any entity providing voice service outside the United States that has the ability to originate voice service that terminates in a point outside that foreign country or terminate voice service that originates from points outside that foreign country. *See* 47 CFR § 64.6300(c). This definition applies to an entity based on the **voice service it provides**, not on its ownership or country of incorporation.
- If a foreign-based provider provides voice service outside the United States that has the ability to terminate within the United States, it must identify itself as a foreign voice service provider on the RMD submission form, regardless of whether it has a domestic office or operation.
- If a U.S.-based provider has a foreign affiliate that provides voice service outside the United States that has the ability to terminate within the United States, the foreign affiliate must file in the RMD and identify itself as a foreign voice service provider on the RMD submission form. As noted above, if foreign voice service providers (including foreign affiliates) do not take these steps, their traffic must not be accepted by domestic U.S. providers (including domestic affiliates). The U.S.-based provider **should not** identify itself as a foreign voice service provider on its RMD submission form **unless** it provides voice service outside the United States that terminates within the United States.

4) What should be included in the "Principals, Affiliates, Subsidiaries, and Parent Companies" section of the RMD submission form?

- The Commission's rules require each filer, including those that file because they are affiliates or subsidiaries of a filing entity and independently meet the definition of a voice service provider or intermediate provider, to provide information regarding their principals, affiliates, subsidiaries, and parent companies on the RMD submission form.
- While a filer may not have any affiliates, subsidiaries, or parent companies, every RMD filer must identify at least one principal, who must be an individual, on the RMD submission form to provide the Commission with sufficient detail regarding the filer's ownership and management.

- A principal is any individual who exercises influence, management, or supervisory responsibility for the entity filing in the RMD, whether or not they have ownership or control of the entity. *See* *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2609, para. 71 n.256 (2023). Common examples of principals include, but are not limited to, owners, directors, officers, and managers of the entity.

5) What is an Operating Company Number (OCN), and is each filer required to have one?

- An Operating Company Number (OCN) is the 4-place alphanumeric code that uniquely identifies a local exchange carrier. *See* 47 CFR § 64.2101.
- A filer is only required to provide an OCN on the RMD submission form **if the filer possesses one**. Filers who do not possess an OCN are not required to obtain one prior to submitting their RMD filing, and should select "No" when prompted on the RMD submission form to disclose whether or not they possess an OCN.

6) When should a provider certify that it has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation?

- A provider must certify on its RMD submission form whether, at any time in the prior two years, the provider (*i.e.*, the filing entity) "and/or any entity for which the filing entity shares common ownership, management, directors, or control[] has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing" related to illegal robocalling or spoofing or a deficient RMD filing, and to provide certain details about any such action or investigation. *See* 47 CFR § 64.6305(d)(2)(iv), (e)(2)(iv), (f)(2)(iv).
- Such actions or investigations necessarily include, but are not limited to: (1) Notices of Apparent Liability and Show Cause Orders issued to a provider by the FCC Enforcement Bureau related to illegal robocalling or a deficient RMD filing, and (2) FCC Enforcement Bureau Orders removing a provider's filing or the filing of a principal or affiliate of the provider from the RMD. Each of these actions should be disclosed in the provider's filing as well as in the filings of the provider's principals and affiliates, to the extent any such principals or affiliates are independently required to file in the RMD. *See* *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2597-99, para. 47 (2023).
- The description of any such action or investigation must include: (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.

7) **What are the proper procedures for requesting confidential treatment of robocall mitigation plans submitted in the RMD?**

- Filers seeking confidential treatment of a robocall mitigation plan should follow the procedures set forth and described in detail in the Protective Order adopted by the Commission on October 14, 2021.
- Pursuant to the Protective Order, filers seeking confidential treatment of their robocall mitigation plans **must** submit a confidentiality request in WC Docket No. 17-97 through the FCC's Electronic Comment Filing System (ECFS) that complies with the requirements set forth in 47 CFR § 0.459. Filers must also submit **both** a redacted and unredacted copy of their robocall mitigation plan directly through the RMD portal.
    - Initial requests for confidential treatment should be submitted in WC Docket No. 17-97 through ECFS, and not via the RMD portal. Filers **should not** file copies of their confidential, unredacted mitigation plans through ECFS.
    - A filer wishing to designate a **portion** of its mitigation plan as confidential should check the applicable box in the "Uploads" section of the RMD submission form stating that it requests that some of the filing's contents be kept confidential. Once checked, the filer must upload both confidential (i.e., unredacted) and non-confidential (i.e., redacted) versions of their mitigation plan. All documents must be uploaded in PDF format. Redacted plans will be published in the RMD. Additional information is available in the RMD filing instructions.
- As stated in the Protective Order, filings which are overly-redacted are not appropriate and the Commission may, on its own or based on a third-party challenge, review and take action on any improper requests. Accordingly, filers seeking confidential treatment **should not redact their entire mitigation plans**, including any information that is specifically required to be included in their mitigation plans under the Commission's rules, unless such information meets the definition of confidential or highly confidential as defined in the Protective Order and the filer has followed all procedures for requesting confidentiality, including filing a confidentiality request in WC Docket No. 17-97 through ECFS.

8) **What if a filer requires more space to submit an answer than is allowed on the RMD submission form?**

- If a filer requires more space to submit a response than is provided in any text box fields on the RMD submission form in the RMD portal, the filer may include the required information in the filer's robocall mitigation plan instead.

- Filers should indicate on the RMD submission form where they have opted to provide the required information in their robocall mitigation plan and clearly identify the section of the robocall mitigation plan that contains the responsive information.

9) When should a provider certify to complete STIR/SHAKEN implementation?

- A provider that selects "Option 1 – Complete STIR/SHAKEN Implementation" on the RMD submission form certifies that the filer has fully implemented STIR/SHAKEN on its **entire** network. This should be selected only when the provider's entire network is Internet Protocol (IP)-based.
- "Option 1 – Complete STIR/SHAKEN Implementation" is not appropriate when a portion of the provider's network is non-IP, even if the provider has fully implemented STIR/SHAKEN on the IP portion of its network. In this circumstance, the provider should select "Option 2 – Partial STIR/SHAKEN Implementation."
- Any provider certifying to complete STIR/SHAKEN implementation in the RMD must be registered with the STIR/SHAKEN Policy Administrator, obtain its own SPC token from the Policy Administrator, use that token to generate a certificate with the Certificate Authority, and authenticate all its calls with that certificate, whether directly or through a third party.

10) What is required of providers who certify to less than complete STIR/SHAKEN implementation?

- A provider that selects "Option 2 – Partial STIR/SHAKEN Implementation" or "Option 3 – No STIR/SHAKEN Implementation" must identify an **applicable** extension or exemption under the FCC's rules and Orders and explain the bases for why the extension or exemption applies to the filer.
- Filers should consult 47 CFR § 64.6304 and the RMD Instructions and Deadlines Public Notice, including all Orders referenced therein, for more information regarding extensions and exemptions from the STIR/SHAKEN implementation requirements, including what extensions and exemptions are currently in effect.
- We note, specifically, that as of June 30, 2022, and June 30, 2023, the extensions for non-facilities-based and facilities-based small voice service providers, respectively, have expired, and therefore **cannot** be relied upon by filers to comply with the requirement to identify an applicable extension on the RMD submission form.
- Any provider certifying to partial STIR/SHAKEN implementation in the RMD must be registered with the STIR/SHAKEN Policy Administrator, obtain its own SPC token from the Policy Administrator, use that token to generate a certificate with the Certificate

Authority, and authenticate all calls on the IP portions of its network with that certificate, whether directly or through a third party.

11) How should a provider certify its STIR/SHAKEN implementation when it uses a third party to authenticate its calls?

- A provider with a STIR/SHAKEN implementation obligation may fulfill that obligation by entering into an agreement with a third party to perform the technological act of authenticating calls so long as the provider: (1) makes all attestation level decisions, consistent with the STIR/SHAKEN technical standards; and (2) ensures that all calls are signed using its own certificate obtained from a STIR/SHAKEN Certificate Authority—not the certificate of a third party. *See* 47 CFR § 64.6301(b) and § 64.6302(f).
- When a provider has a STIR/SHAKEN implementation obligation and it is not otherwise exempt, it should certify to the level of STIR/SHAKEN implementation across its network **irrespective** of whether it has contracted with a third party to perform the technological act of authenticating calls on its behalf.
- A provider's decision to enter into a third-party authentication arrangement does not affect whether the provider has a STIR/SHAKEN implementation obligation or whether it is eligible to claim a valid extension or exemption under our rules.

12) Are providers required to use data analytics as part of their robocall mitigation programs?

- A provider is **not** required to use data analytics as part of its robocall mitigation program, **but if it does**, the provider must describe in its robocall mitigation plan the analytics system it is using, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s). A provider should state whether or not it uses data analytics as part of its robocall mitigation program.
- If a provider is relying on its underlying provider(s) for data analytics, it should provide the name(s) of its underlying provider(s) in its robocall mitigation plan, though the provider may request confidential treatment of this information pursuant to the procedures described in the Protective Order.

13) Are providers required to have know-your-customer (KYC) procedures in place as part of their robocall mitigation programs?

- All voice service providers are required to know their end user customers pursuant to 47 CFR § 64.1200(n)(4), and must describe in their robocall mitigation plans how they comply with this obligation. Voice service providers must also describe any procedures they have in place to know their upstream providers. *See* 47 CFR § 64.6305(d)(2)(ii).

- Intermediate providers are required to know their upstream providers pursuant to 47 CFR § 64.1200(n)(5), and must describe in their robocall mitigation plans how they comply with this obligation. *See* 47 CFR § 64.6305(e)(2)(ii), (f)(2)(ii).

14) When must filers update their RMD filings?

- All filers are required to update their filings within 10 business days of any change to the information provided in their filings. This includes, but is not limited to, changes in ownership or control of the filing entity due to a merger, acquisition, or other company change. *See* 47 CFR § 64.6305(d)(5), (e)(5), (f)(5). The Commission has established a base forfeiture amount of $1000 for failure to update information that has changed within 10 business days. *See* 47 CFR § 1.80.
- All filers are also required to recertify their filings annually on or before March 1. *See* 47 CFR § 64.6305(h).
- If an entity believes that it is no longer required to have a filing in the RMD because it is no longer operating as a voice service, gateway, or non-gateway intermediate provider (such as due to a merger or the entity ceasing operations), that entity should either delete its RMD filing or update the filing to indicate that the entity is no longer operating as a voice service, gateway, or non-gateway intermediate provider. Detailed instructions for deleting and updating an RMD filing are available in the RMD filing instructions.

15) When and how must filers submit their annual recertifications?

- Each provider with an existing RMD filing must recertify and resubmit their filing each year by March 1. *See* 47 CFR § 64.6305(h). When completing their recertifications, providers must ensure that the information contained in their RMD filings is accurate and truthful, including with respect to the certifications required by the Commission's rules. In the future, providers will also be required to pay a $100 annual recertification fee, and the Commission will announce when this requirement becomes effective. Detailed instructions for submitting an annual recertification are available in the RMD filing instructions.

16) How can a filer access the RMD if they've forgotten their password or if their RMD filing was created by an employee that has since left the company?

- Filers login to the RMD using their CORES username and password. The username is the email address associated with the company's FCC Registration Number (FRN) in CORES. If a filer has forgotten the password associated with their CORES username, they may follow instructions to reset their password here.

- If a filer has forgotten their CORES username or is still having trouble logging in after visiting the password reset link above, they may contact the CORES help desk by calling 877-480-3201 (Mon.-Fri. 8 a.m.-6 p.m. ET).
- If the CORES user that created the RMD filing has since left the company, the filer may associate a new CORES username with the company's FRN in order to login and access the company's RMD filing. The CORES help desk can assist with this and can be reached by calling 877-480-3201 (Mon.-Fri. 8 a.m.-6 p.m. ET).
- All entities that register in CORES to obtain an FRN must update any information submitted to CORES within 10 business days of any change to that information. *See* 47 CFR § 1.8002(b)(2).