Federal Communications Commission
Enforcement Bureau
Telecommunications Consumers Division
45 L Street, NE
Washington, DC 20554

August 24, 2026

VIA ELECTRONIC DELIVERY AND CERTIFIED MAIL - RETURN RECEIPT REQUESTED

To: RGTN USA Inc.
Attn: Leonardus Herps
Chief Executive Officer
244 Fifth Avenue, Suite L220
New York, NY, 10001
l.herps@rgtn.com

Re: Notification of Suspected Illegal Traffic

Dear Leonardus Herps,

RGTN USA Inc. (RGTN or Company) is transmitting apparently illegal traffic, originating from abroad, onto the U.S. telecommunications network. This traffic has taken several forms, each directed at defrauding victims: spoofed[1] calls posing as a private business to obtain internal e-mail communications from employees; spoofed calls posing as a local police department and the U.S. Customs and Border Protection (CBP); robocalls posing as a financial institution; robocalls posing as major retailers to notify consumers about nonexistent orders; and swatting[2] calls. In each of these schemes, RGTN served as the gateway provider,[3] routing calls from a foreign voice service provider, TheSwissXperts AG (TheSwissXperts),[4] to consumers' phones.

Protecting consumers nationwide from the harms of unlawful calls—including spoofed calls and robocalls—is the Commission's top consumer protection priority.[5] The Enforcement Bureau (Bureau) of the Federal Communications Commission (FCC or Commission) provides this letter as notice of important legal obligations and steps RGTN must take to address this apparently illegal traffic. Failure to comply with the steps outlined in this letter **may result in downstream providers permanently blocking *all* of RGTN's traffic.**

[1] "Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity." *Caller ID Spoofing*, Fed. Commc'ns Comm'n (Nov. 13, 2024), https://www.fcc.gov/spoofing.

[2] *See generally Threat Actors Use Swatting to Target Victims Nationwide*, Fed. Bureau of Investigation (Apr. 29, 2025), https://www.fbi.gov/investigate/cyber/alerts/2025/threat-actors-use-swatting-to-target-victims-nationwide ("Swatting is the malicious tactic of making hoax calls or reports to emergency services, typically feigning an immediate threat to life.") (FBI Swatting Alert).

[3] *See* 47 CFR § 64.6300(d) ("The term 'gateway provider' means a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider.").

[4] TheSwissXperts is registered in the Robocall Mitigation Database as a foreign voice service provider and lists its business address in Switzerland. TheSwissXperts AG (RMD0031298), Fed. Commc'ns Comm'n, Robocall Mitigation Database (filed Jan. 12, 2025), https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=4f87ecb11b6dba10dea35396624bcb6d&view=sp.

[5] *Stop Unwanted Robocalls and Texts*, Fed. Commc'ns Comm'n, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts (last visited June 9, 2026).

I. Background

A. Traffic Spoofing Caller Identification Information of a Private Business

The Bureau received a complaint through its Private Entity Robocall and Spoofing Portal alleging that on May 1, 2026, a spoofed vishing[6] campaign targeted Blue-Grace Logistics LLC (Blue-Grace).[7] Three of its employees received calls on their personal cell phones from a caller impersonating the company's Information Technology Department and attempting to obtain internal Blue-Grace e-mail communications.[8] The caller identification information made the calls appear to originate from a toll-free number assigned to Blue-Grace.[9]

Blue-Grace contacted TeleVoIPs, LLC (TeleVoIPs), which provides service to Blue-Grace's toll-free number.[10] In response, TeleVoIPs stated that the calls had not originated from its network,[11] thus confirming that the caller identification information had been spoofed.

The Bureau worked with the Industry Traceback Group (ITG)[12] to trace the source of three spoofed calls placed to Blue-Grace's employees on May 1, 2026.[13] Each call is identified in Attachment A. The ITG traces a call to its source by working upstream: starting from the terminating provider whose customer received the call, it asks each provider to identify the provider immediately upstream that handed it the call.[14] This process ideally resolves with the originating provider's identification of the end user who placed the call.[15]

The tracebacks of each of the three calls ended at GUGUcompany (GUGU), which failed to respond to ITG correspondence.[16] RGTN had received the calls from a foreign voice service provider, TheSwissXperts—which had itself received them from GUGU—and carried them onto the U.S.

---

[6] *See generally What is vishing?*, Cisco, https://www.cisco.com/site/us/en/learn/topics/security/what-is-vishing.html (last visited June 1, 2026) ("Vishing, short for voice phishing, refers to fraudulent phone calls or voice messages designed to trick victims into providing sensitive information."); *see also* Katharina Krombholz et al., *Advanced Social Engineering Attacks*, 22 J. Info. Sec. & Applications 113, 116 (2015) ("Telephone, Voice over IP are common attack channels for social engineers to make their victim deliver sensitive information.").

[7] Private Entity Portal Complaint #1437 from Blue-Grace (May 4, 2026) (on file at EB-TCD-26-00040901) (Complaint) (describing "a targeted vishing/social engineering campaign against our organization").

[8] *Id.* ("The caller impersonated our internal IT department and requested that employees search for and forward internal company emails.").

[9] *Id.* ("[B]ad actors spoofed Blue-Grace Logistics LLC's main corporate toll-free number, (800) 697-4477, to place fraudulent calls to personal cell phones belonging to three of our employees.").

[10] E-mail from {[ ]}, Info. Tech. Dir., Blue-Grace to {[ ]}, Voice Network Eng'r, TeleVoIPs (May 1, 2026, at 17:16 ET) (on file at EB-TCD-26-00040901) ({[ ]} E-mail). Material set off by double brackets {[ ]} is confidential and redacted from the public version of this document.

[11] E-mail from {[ ]}, Voice Network Eng'r, TeleVoIPs to {[ ]}, Info. Tech. Dir., Blue-Grace (May 1, 2026, at 18:21 ET) (on file at EB-TCD-26-00040901) ("[W]e have confirmed that no calls were placed to those cell phone numbers from within our system.").

[12] The ITG is the registered industry consortium selected pursuant to the TRACED Act to conduct tracebacks. *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Report and Order, 38 FCC Rcd 7561, 7561–62, para. 1 (EB 2023).

[13] *See* ITG Subpoena Response (June 4, 2026) (on file at EB-TCD-26-00040901) (ITG June Response)

[14] *Policies and Procedures*, Indus. Traceback Grp., 6 (Aug. 2025), https://tracebacks.org/wp-content/uploads/2025/09/ITG_Policies-Procedures_Aug_2025.pdf (ITG Policies and Procedures).

[15] *Id.*

[16] *See* ITG June Response, *supra* note 13.

network.[17] RGTN served as a gateway provider for the calls at issue.

B. Traffic Spoofing Caller Identification Information of Law Enforcement Agencies

During its investigation into Blue-Grace's complaint, the Bureau discovered additional spoofed calls, flagged by the ITG, that RGTN had carried onto the U.S. network for TheSwissXperts. Two of these calls impersonated local and federal law enforcement agencies.[18] Each call is identified in Attachment A.

On April 24, 2026, RGTN carried onto the U.S. network a call from TheSwissXperts with caller identification information displaying the phone number (325) 537-9311 and the caller name "HAWLEY POLICE."[19] (325) 537-9311 is a phone number assigned to and used by the Hawley, Texas Police Department.[20] The Hawley, Texas Police Department did not place the call; it was spoofed.[21] Similarly, on January 9, 2026, RGTN carried onto the U.S. network a call from TheSwissXperts with caller identification information displaying the phone number (804) 226-9675 and the caller name "C B P ASSOC INC."[22] (804) 226-9675 is a number assigned to and used by a Virginia port of entry of the CBP.[23] This call was also spoofed.[24]

C. Traffic Impersonating a Financial Institution and Major Retailers Using Artificial or Prerecorded Voices

Additionally, the ITG has received traceback requests pertaining to calls that used artificial or prerecorded voices and were carried onto the U.S. network by RGTN—the earliest placed on January 5, 2026, and the latest placed on May 24, 2026.[25] Each was received by RGTN directly from TheSwissXperts.[26] Each is identified in Attachment B.

The Bureau has reviewed available recordings of these robocalls. Several of the robocalls impersonated Coinbase, a cryptocurrency exchange, using a similar artificial or prerecorded message:

> Hello! This is an automated call from the Coinbase Security Department. We have detected an attempt to change the primary phone number assigned to your account. If

---

[17] *Id.*

[18] *See* ITG June Response, *supra* note 13; *see also Provider Summary for RGTN USA Inc.*, Indus. Traceback Grp., https://portal.tracebacks.org/providers/provider/summaries/2668 (last visited July 9, 2026) (password protected) (on file at EB-TCD-26-00040901) (RGTN Traceback Portal Summary).

[19] *See* ITG June Response, *supra* note 13 (traceback no. 38470); RGTN Traceback Portal Summary, *supra* note 18.

[20] *See Police Department*, City of Hawley, Tex., https://www.cityofhawley.com/police-dept/ (last visited June 3, 2026).

[21] *See* E-mail from Homeland Security Investigations (Chicago), Department of Homeland Security to Charles Becker, Legal Intern, Telecommunications Consumers Division, FCC Enforcement Bureau (June 3, 2026, at 17:15 ET) (on file at EB-TCD-26-00040901) (DHS E-mail) ("One of those numbers did spoof the Hawley police department.").

[22] *See* ITG June Response, *supra* note 13 (traceback no. 38955); *see also* RGTN Traceback Portal Summary, *supra* note 18.

[23] *See Richmond - Petersburg, Virginia - 1404*, U.S. Customs & Border Prot., https://www.cbp.gov/about/contact/ports/richmond-petersburg-virginia-1404 (last visited June 3, 2026).

[24] *See* E-mail from San Francisco Field Office, Federal Bureau of Investigation to Charles Becker, Legal Intern, Telecommunications Consumers Division, FCC Enforcement Bureau (June 4, 2026, at 18:04 ET) (on file at EB-TCD-26-00040901) ("Yes, a bad actor impersonated a CBP office in Virginia . . . .").

[25] *See* ITG June Response, *supra* note 13; RGTN Traceback Portal Summary, *supra* note 18. The Bureau is aware that additional such calls continue to be placed, though they are not included in this letter.

[26] *See* ITG June Response, *supra* note 13.

> this was not you, please press one. If this was you, you may hang up.[27]

Other robocalls purported to come from Amazon:

> Hello! This is an important call from Amazon Customer Support. This is to notify you regarding your today's purchase on Amazon. You have been charged $1,279.99 on your default card saved on Amazon. If you have not made any such transaction, then please press one to cancel your order. Else, if you have made this purchase on Amazon and recognize it, then please press two to confirm your order or talk to our Customer Care. Please press three to repeat this.[28]

Yet more robocalls purported to come from Walmart.[29]

D. Traffic Communicating False Emergencies

Finally, the ITG traced the source of three calls at the request of two local police departments and the Federal Bureau of Investigation in which the callers "ma[de] false claims regarding possible bomb threats, shootings[,] or other horrific events."[30] As before, the ITG identified RGTN as the gateway provider for these calls; its immediate upstream was TheSwissXperts.[31]

One of these calls had caller identification information displaying the phone number (732) 280-3000 and the caller name "INFOAGE SPACE."[32] (732) 280-3000 is a phone number assigned to and used by the InfoAge Science and History Center (InfoAge) in Wall, New Jersey.[33] This call is identified in Attachment A.

On the call, an "unidentified person" reported a "serious incident" to the Wall Township Police Department (Wall Police)'s 911 Public Safety Answering Point.[34] This "led to the evacuation of about 500 conference attendees at [InfoAge]."[35] "Following a systematic search of all structures by Wall Police and explosive detection K9 teams from Wall, Manasquan, Brick, Marlboro, and the Monmouth County Sheriff's Office, it was determined that the initial report was a swatting incident."[36] Wall Police's investigation further determined with "certain[ty] that the number calling in was a spoofed number."[37]

II. Apparent Violations

RGTN received the above-described traffic directly from TheSwissXperts and carried it onto the

---

[27] *Id.* (recording of robocall received on Jan. 5, 2026, at 20:00 UTC, traceback no. 35115).

[28] *Id.* (recording of robocall received on Feb. 6, 2026, at 15:32 UTC, traceback no. 35857); *see also id.* (traceback nos. 36110 and 37369).

[29] *Id.* (traceback no. 38383).

[30] *Id.* (traceback nos. 38103, 38337, and 38820).

[31] *Id.*

[32] *Id.* (traceback no. 38103); RGTN Traceback Portal Summary, *supra* note 18.

[33] *See Home*, Infoage Sci. & Hist. Ctr., https://www.infoage.org/ (last visited July 15, 2026).

[34] *Swatting Call Prompts Evacuation at Museum Event*, Jersey Shore Online (Apr. 20, 2026), https://www.jerseyshoreonline.com/monmouth-county/swatting-call-prompts-evacuation-at-museum-event.

[35] Ken Serrano, *Swatting Hoax Targets Three-Day Conference at Wall Museum*, AOL Media (Apr. 20, 2026), https://www.aol.com/articles/swatting-hoax-targets-three-day-201035000.html.

[36] Sara Winick, *Info Age Science & History Museum Targeted in 'Swatting' Incident, Police Say*, Patch Media (Apr. 20, 2026), https://patch.com/new-jersey/wall/info-age-science-history-museum-targeted-swatting-incident-police-say.

[37] E-mail from John Spinapont, Detective, Wall Township Police Department to Charles Becker, Legal Intern, Telecommunications Consumers Division, FCC Enforcement Bureau (July 15, 2026, at 18:50 ET) (on file at EB-TCD-26-00040901).

U.S. network.[38] That traffic was apparently illegal, for one or both of the following reasons.

A. The Traffic Apparently Violates the Truth in Caller ID Act

The Truth in Caller ID Act expressly prohibits "knowingly transmit[ting] misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value" unless an exemption applies.[39] Here, the calls placed to Blue-Grace's three employees displayed caller identification information indicating that the calling number was (800) 697-4477.[40] The Bureau verified that (800) 697-4477 is a phone number assigned to and used by Blue-Grace.[41] As discussed, the caller transmitted this number in caller identification information without authorization from Blue-Grace.[42] The use of Blue-Grace's number in the vishing campaign reveals that the caller *knew* the number did not belong to them and chose it because it would appear legitimate to Blue-Grace's employees.

The caller apparently intended to defraud. The relevant elements of common law fraud for purposes of establishing an intent to defraud are: (1) a false representation; (2) in reference to a material fact; (3) made with knowledge of its falsity; and (4) with the intent to deceive.[43] These four elements are apparently satisfied here. *First*, the caller falsely represented themself as a person in Blue-Grace's Information Technology (IT) Department. *Second*, this misrepresentation was material, providing the only pretense of authority the caller had for requesting that employees search for and forward internal e-mail communications. *Third*, the caller was aware that they did not work for Blue-Grace's IT Department. *Fourth*, the caller's intent to deceive Blue-Grace employees is demonstrated by the spoofing of Blue-Grace's toll-free number and by their pretending to be an employee of the company's IT Department, the only conceivable purpose for which was to obtain the desired communications.[44]

Additionally, the caller apparently attempted to obtain a thing of value—the company's internal e-mail communications. "Congress' frequent use of 'thing of value' in various criminal statutes has evolved the phrase into a term of art which the courts generally construe to envelope both tangibles and intangibles. This broad interpretation is based upon a recognition that monetary worth is not the sole measure of value."[45] For one perpetrating a vishing campaign, Blue-Grace's communications carry

---

[38] *See* ITG June Response, *supra* note 13.

[39] 47 U.S.C. § 227(e)(1); *see also* 47 CFR § 64.1604(a). The statute and the Commission's rules contain two narrow exemptions. *See* 47 U.S.C. § 227(e)(3)(B)(ii) (exempting spoofing in connection with "any authorized activity of a law enforcement agency" or "a court order that specifically authorizes the use of call authentication manipulation"); 47 CFR § 64.1604(b) (interpreting the two statutory exemptions).

[40] Complaint, *supra* note 7; ITG June Response, *supra* note 13.

[41] *See* TeleVoIPs Billing Name and Address (BNA) Request Response (on file at EB-TCD-26-00040901).

[42] {[} E-mail, *supra* note 10 ("At least two employees have received *fraudulent* calls, within the last hour, appearing to come from our number" (emphasis added)).

[43] *See Steve Kramer*, Forfeiture Order, 39 FCC Rcd 11229, 11239, para. 27 (2024) (citing *Pence v. United States*, 316 U.S. 332, 338 (1942) and *Hercules & Co. v. Shama Rest. Corp.*, 613 A.2d 916, 923 (D.C. 1992) for the elements of common law fraud). The Commission explained that the fifth element of common law fraud identified by the courts—an action taken in reliance upon the representation—is not necessary to establish an intent to defraud. *See id.* In other words, it is not necessary for the attempt at fraud to be successful.

[44] The Commission has accepted that intent under the Truth in Caller ID Act can be demonstrated by reference to "consequences which are desired" or "substantially certain" to result. *Affordable Enters. of Arizona, LLC*, Notice of Apparent Liability for Forfeiture, 33 FCC Rcd 9233, 9242–43, para. 26 & n.70 (2018) ("Intent is not . . . limited to consequences which are desired. If the actor knows that the consequences are certain, or substantially certain, to result from his act, and still goes ahead, he is treated by the law as if he had in fact desired to produce the result." (quoting Restatement (Second) of Torts § 8A, comment b (A.L.I. 1965))).

[45] *United States v. Nilsen*, 967 F.2d 539, 542–43 (11th Cir. 1992); *accord United States v. Schwartz*, 785 F.2d 673,

monetary value.[46] They also contain intangible trade information.[47] Courts have held that information alone can qualify as a "thing of value," as Congress has used the term in other statutes.[48]

For similar reasons, the calls impersonating law enforcement agencies also apparently violated the Truth in Caller ID Act. The caller(s) transmitted phone numbers and names associated with law enforcement agencies as caller identification information "for fraudulent means."[49]

The call communicating a false emergency also apparently violated the Truth in Caller ID Act. The caller transmitted a phone number associated with InfoAge, despite not actually calling from an InfoAge phone system, and the content of the call triggered a significant law enforcement response to the museum.[50] The only conceivable reason to carry out a swatting attack of this nature is to cause harm, including "chaos and the potential for injury or violence."[51] Accordingly, the calls identified in Attachment A apparently violated the Truth in Caller ID Act.

B. The Traffic Apparently Violates the Telephone Consumer Protection Act

The Telephone Consumer Protection Act (TCPA) expressly prohibits placing calls using an artificial or prerecorded voice to certain telephone numbers, absent an emergency purpose or the called party's prior express consent.[52] The robocalls identified in Attachment B apparently violated this prohibition. *First*, the robocalls used artificial or prerecorded voice messages[53] and were made without the prior express consent of the called parties. All of the traceback requests for these robocalls were filed by ZipDX and Verizon.[54] Robocalls reached "honeypots" operated by ZipDX and Verizon—phone numbers that are not assigned to any end user.[55] Accordingly, there was no end-user customer who could

---

680 (9th Cir. 1986) ("[I]n the ordinary sense[,] *thing of value* is not limited in meaning to tangible things with an identifiable commercial price tag." (emphasis in original)).

[46] *See Keys to the Kingdom: How Compromised Corporate Emails Have Become the Most Attractive Attack Vector for Cybercriminals*, KELA Cybercrime Intel. 30, https://www.kelacyber.com/wp-content/uploads/2022/12/KELA-RESEARCH_KEYS-TO-THE-KINGDOM_WEBMAIL-ACCOUNTS-1.pdf (last visited June 1, 2026) ("[C]ompromised corporate emails are *valuable goods* that can easily be monetized for several attacks from phishing, [business email compromise], and different malware attacks." (emphasis added)).

[47] Danny Mercer, *Your Inbox Is a Goldmine: How Email Stealers Are Quietly Looting Corporate Secrets*, Innovation Network Design (Feb. 3, 2026), https://www.innovationnetworkdesign.com/articles/cyber/email-stealers-corporate-espionage-guide-1770128596 ("Even 'boring' emails are *valuable* for reconnaissance, helping attackers learn your org structure, identify key personnel, understand ongoing projects, and craft incredibly convincing spear-phishing attacks using real conversation threads they've stolen." (emphasis added)).

[48] *See, e.g.*, *United States v. Sheker*, 618 F.2d 607, 608–09 (9th Cir. 1980) (stating that "[i]nformation can be a thing of value" and holding that the whereabouts of a witness in a criminal prosecution constitutes a "thing of value" that can support a conviction under 18 U.S.C. § 912); *United States v. Girard*, 601 F.2d 69, 71 (2d Cir. 1979) (holding that information sold from a government computer constitutes a "thing of value" that can support a conviction under 18 U.S.C. § 641).

[49] DHS E-mail, *supra* note 21 (attaching spreadsheet of traceback result).

[50] *See* ITG June Response, *supra* note 13; *supra* p. 4.

[51] FBI Swatting Alert, *supra* note 2.

[52] 47 U.S.C. § 227(b)(1)(A)(iii); *see also* 47 CFR § 64.1200(a)(1)(iii). As relevant here, the statute protects "any telephone number assigned to a . . . cellular telephone service . . . or any service for which the called party is charged for the call." *Id.*

[53] *See* ITG June Response, *supra* note 13.

[54] *Id.*

[55] *See* E-mail from Warren Currie, Robocall Traceback Fraud Specialist, ITG to Charles Becker, Legal Intern, Telecommunications Consumers Division, FCC Enforcement Bureau (July 22, 2026, at 11:35 ET) (on file at EB-

have provided consent to receive calls at these numbers. *Second*, the robocalls' content makes clear that none of the calls identified in Attachment B were made for emergency purposes. *Finally*, seven of the robocalls were made to numbers assigned to cellular service.[56] The remaining three robocalls were made to numbers assigned to a service for which the called party incurred charges for the call.[57] Accordingly, the robocalls identified in Attachment B apparently violated the TCPA.

III. Potential Consequences

As a result of transmitting apparently illegal calls, RGTN potentially faces permissive blocking under section 64.1200(k)(4)[58] of the Commission's rules, mandatory blocking under section 64.1200(n),[59] and additional consequences under section 64.6305(g) if its certification is removed from the Robocall Mitigation Database (RMD).[60]

A. RGTN Faces Permissive Blocking Under Section 64.1200(k)(4)

Under the safe harbor set forth in section 64.1200(k)(4) of the Commission's rules, any downstream provider may (without any liability under the Communications Act of 1934, as amended, or the Commission's rules) block all traffic from an upstream originating or intermediate provider that, when notified by the Commission, fails to either (a) effectively mitigate illegal traffic within 48 hours or (b) implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.[61] Prior to initiating blocking, the downstream provider shall provide the Commission with notice and a brief summary of the basis for its determination that the originating or intermediate provider meets one or more of these two conditions for blocking.[62]

This letter provides notice, pursuant to section 64.1200(k)(4), that RGTN should effectively mitigate illegal traffic within 48 hours and implement effective measures to prevent new and renewing customers from using its network to originate illegal calls within 14 days of this letter in order to avoid having its traffic blocked by downstream providers.[63] The Company should inform the Commission and the ITG, within 48 hours of the electronic delivery date of this letter, of the specific steps it has taken to mitigate illegal traffic on its network.[64]

B. RGTN Faces Mandatory Blocking Under Section 64.1200(n)(2) and (n)(3)

The Commission may order all providers that are immediately downstream to block all traffic from an upstream provider that does not comply with the obligations identified in section 64.1200(n)(2)

TCD-26-00040901) (ITG E-mail) (confirming which calls reached honeypots); *see generally What is RRAPTOR?*, ZipDX LLC, https://rraptor.org/what-is-rraptor (last visited June 8, 2026); *Honeypot Phone Numbers Collect Scam Data for AI to Analyze*, Caller ID Reputation (Oct. 18, 2023), https://calleridreputation.com/blog/honeypot-phone-numbers-collect-scam-data-for-ai-to-analyze.

[56] *See* ITG June Response, *supra* note 13.

[57] *See* E-mail from David Frankel, CEO, ZipDX LLC to Charles Becker, Legal Intern, Telecommunications Consumers Division, FCC Enforcement Bureau (July 9, 2026, at 18:41 ET) (on file at EB-TCD-26-00040901) (confirming which calls to the ZipDX honeypot resulted in charges to ZipDX).

[58] 47 CFR § 64.1200(k)(4).

[59] *Id.* § 64.1200(n).

[60] *Id.* § 64.6305(g).

[61] *Id.* § 64.1200(k)(4).

[62] *Id.*

[63] *See id.*; *see also id.* § 64.1200(n)(2)(i)(A) (requiring a minimum of 14 days to comply with the notice).

[64] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7630, para. 42 (2020).

of the Commission's rules.[65] This letter serves as a Notification of Suspected Illegal Traffic (Notice) under section 64.1200(n)(2) of the Commission's rules.[66] The Company must take the following actions in response to this Notice:

1. Promptly investigate the traffic identified in Attachment A and Attachment B for which the Company served as the originating or gateway provider;[67]
2. If the Company's investigation determines that the Company served as the originating or gateway provider for the identified traffic, block or cease accepting all of the identified traffic within 14 days of the date of this Notice and continue to block or cease accepting the identified traffic, as well as substantially similar traffic, on an ongoing basis (unless the Company determines that the identified traffic is not illegal);[68]
3. Report the results of the Company's investigation to the Bureau within 14 days of the date of this Notice.[69]

Depending on the outcome of the investigation, the report must contain certain details as described below:[70]

1. If the Company determines it is the originating or gateway provider for the identified traffic and does not conclude the traffic is legal, the report must include: (i) a certification that the Company is blocking the identified traffic and will continue to do so, and (ii) a description of the Company's plan to identify and block or cease accepting substantially similar traffic on an ongoing basis;[71]
2. If the Company determines that the identified traffic is not illegal, the report must provide: (i) an explanation as to why the Company reasonably concluded that the identified traffic is not illegal, and (ii) what steps it took to reach that conclusion;[72] and
3. If the Company determines that it did not serve as the originating or gateway provider for any of the identified traffic, the report must: (i) provide an explanation as to how the Company reached that conclusion, and (ii) if it is a non-gateway intermediate or terminating provider for the identified traffic, identify the upstream provider(s) from which the Company received the identified traffic and, if possible, take steps to mitigate the traffic.[73]

1. Initial Determination Order

The Bureau may issue an initial determination order stating the Bureau's initial determination that RGTN is not in compliance with section 64.1200 of the Commission's rules if: (a) the Company fails to respond to this Notice; (b) the Company provides an insufficient response; (c) the Company continues to originate substantially similar traffic or allow substantially similar traffic onto the U.S. network after the 14-day period identified above; or (d) the Bureau determines the traffic is illegal despite the Company's

[65] 47 CFR § 64.1200(n)(3).

[66] *Id.* § 64.1200(n)(2).

[67] *Id.* § 64.1200(n)(2)(i)(A).

[68] *See id.*

[69] *See id.*

[70] *Id.*

[71] *See id.*

[72] *Id.* § 64.1200(n)(2)(i)(B).

[73] *Id.*

assertions to the contrary.[74] If the Bureau issues an initial determination order, the Company will have an opportunity to respond.[75]

2. Final Determination Order

The Bureau may issue a final determination order in EB Docket No. 22-174 concluding that the Company is not in compliance with section 64.1200 of the Commission's rules and directing all downstream providers both to block and cease accepting all traffic from RGTN beginning 30 days from the release of the final determination order if: (a) the Company does not provide an adequate response to the initial determination order within the timeframe specified in the initial determination order; or (b) the Company continues to originate or allow substantially similar traffic onto the U.S. network.[76] A final determination order may be issued up to one year after the release date of the initial determination order.[77]

C. RGTN Faces Removal from the Robocall Mitigation Database

Pursuant to section 64.6305(g) of the Commission's rules, intermediate and voice service providers shall only accept calls directly from a domestic voice service provider, gateway provider, or non-gateway intermediate provider if that provider's certification appears in the RMD.[78] If the provider's filing is deficient in some way, the Bureau may initiate a proceeding to remove it.[79]

RGTN certified in its Robocall Mitigation Database (RMD) filing, under penalty of perjury, that it will cooperate with the Commission in investigating and stopping any illegal robocallers that use its service to originate, carry, or process calls.[80] **Failure to respond to this letter may be used as evidence that the Company's certification is deficient with respect to its commitment to cooperate with the**

---

[74] *Id.* § 64.1200(n)(2)(ii).

[75] *Id*.

[76] *Id.* § 64.1200(n)(2)(iii), (3); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404, 5417–18, para. 37 (2023).

[77] 47 CFR § 64.1200(n)(2)(iii).

[78] *See* 47 CFR § 64.6305(g)(1), (3)-(4). This requirement also extends to accepting traffic from foreign providers using "North American Number plan resources that pertain to the United States in the caller ID field to send voice traffic." *Id.* § 64.6305(g)(2).

[79] *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1903, para. 83 (2020) (*Second Caller ID Authentication Order*) (noting that if a certification "is deficient in some way," the Commission may take enforcement action as appropriate, including "removing a defective certification from the database after providing notice to the voice service provider and an opportunity to cure the filing"); *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order on Reconsideration in WC Docket No. 17-97, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, 37 FCC Rcd 6865, 6882, para. 40 (2022) (*Gateway Provider Order*) (noting that the Commission can take the same enforcement action against gateway providers); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order, 38 FCC Rcd 2573, 2603-04, paras. 57, 60 (2023) (*Sixth Caller ID Authentication Order*) (noting that the Commission can take the same enforcement action against non-gateway intermediate providers and describing the three-step removal procedure for deficient RMD filings).

[80] *See* RGTN USA Inc. Certification (RMD0015406), Fed. Commc'ns Comm'n, Robocall Mitigation Database (filed Feb. 17, 2026), https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=f6d5216c1b8e3510f9232f84604bcb05&view=sp. RGTN certified as a voice service provider, gateway provider, and non-gateway intermediate provider in its RMD certification. *Id.*

Commission.[81] If the Company's certification is removed from the RMD for any reason, all intermediate providers and terminating voice service providers must cease accepting traffic directly from the Company pursuant to section 64.6305(g) of the Commission's rules.[82] If the Bureau initiates a proceeding to remove the Company's certification from the RMD, RGTN will have an opportunity to cure the deficiency.[83]

* * *

Please direct any inquiries regarding this letter to David Konuch, Attorney Advisor, Telecommunications Consumers Division, Enforcement Bureau, FCC, at David.Konuch@fcc.gov and cc: to Daniel Stepanicich, Division Chief, Telecommunications Consumers Division, Enforcement Bureau, FCC, at Daniel.Stepanicich@fcc.gov. A copy of this letter has been sent to the ITG.

Sincerely,

Patrick Webre
Chief
Enforcement Bureau
Federal Communications Commission

[81] *See Second Caller ID Authentication Order*, 36 FCC Rcd at 1903, para. 83 (stating that deficient RMD certifications include those where the Commission finds that the provider knowingly or negligently transmits illegal robocall campaigns).

[82] *See* 47 CFR § 64.6305(g).

[83] *See Second Caller ID Authentication Order*; 36 FCC Rcd at 1903, para. 83; *Gateway Provider Order*, 37 FCC Rcd at 6882, para. 40; *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2603, para. 57.

Attachment A

Role	Call Date & Time	Calling No.	Called No.	CNAM	Description	Apparent Violations
Gateway	Jan. 09, 2026, at 18:24 UTC	+1 (804) 226-9675	{[ ]}	C B P ASSOC INC	Live calls impersonating law enforcement or government officials for fraudulent means.	47 U.S.C. § 227(e)(1) 47 CFR § 64.1604(a)
Gateway	Apr. 13, 2026, at 15:36 UTC	+1 (325) 537-9311	{[ ]}	HAWLEY POLICE	Live calls impersonating law enforcement or government officials for fraudulent means.	47 U.S.C. § 227(e)(1) 47 CFR § 64.1604(a)
Gateway	Apr. 19, 2026, at 18:12 UTC	+1 (732) 280-3000	{[ ]}	INFOAGE SPACE	Live calls making false claims regarding possible bomb threats, shootings or other horrific events.	47 U.S.C. § 227(e)(1) 47 CFR § 64.1604(a)
Gateway	May 01, 2026, at 20:32 UTC	+1 (800) 697-4477	{[ ]}	BlueGrace Logis	Live calls made to an enterprise impersonating the same enterprise for fraudulent means.	47 U.S.C. § 227(e)(1) 47 CFR § 64.1604(a)
Gateway	May 01, 2026, at 20:24 UTC	+1 (800) 697-4477	{[ ]}	BlueGrace Logis	Live calls made to an enterprise impersonating the same enterprise for fraudulent means.	47 U.S.C. § 227(e)(1) 47 CFR § 64.1604(a)

Gateway	May 01, 2026, at 21:06 UTC	+1 (800) 697-4477	{[ ]}	BlueGrace Logis	Live calls made to an enterprise impersonating the same enterprise for fraudulent means.	47 U.S.C. § 227(e)(1) 47 CFR § 64.1604(a)

Attachment B

Role	Call Date & Time	Calling No.	Called No.	Service	Description	Apparent Violations
Gateway	Jan. 05, 2026, at 20:00 UTC	+1 (800) 885-5261	{[ ]}	wireless	Prerecorded calls to recipient claiming to be some type of financial institution (e.g. bank, paypal, venmo) for fraudulent means.	47 U.S.C. § 227(b)(1)(A)(iii) 47 CFR § 64.1200(a)(1)(iii)
Gateway	Feb. 06, 2026, at 15:32 UTC	+1 (214) 588-0660	{[ ]}	wireline	Prerecorded calls to recipients impersonating Amazon for fraudulent means.	47 U.S.C. § 227(b)(1)(A)(iii) 47 CFR § 64.1200(a)(1)(iii)
Gateway	Feb. 13, 2026, at 18:58 UTC	+1 (229) 379-6939	{[ ]}	wireless	Prerecorded calls to recipient impersonating Amazon for fraudulent means.	47 U.S.C. § 227(b)(1)(A)(iii) 47 CFR § 64.1200(a)(1)(iii)
Gateway	Mar. 23, 2026, at 15:40 UTC	+1 (205) 681-6085	{[ ]}	wireline	Prerecorded calls to recipients impersonating Amazon for fraudulent means.	47 U.S.C. § 227(b)(1)(A)(iii) 47 CFR § 64.1200(a)(1)(iii)
Gateway	Apr. 27, 2026, at 15:14 UTC	+1 (812) 295-9256	{[ ]}	wireline	Prerecorded calls impersonating a store regarding an order or purchase that was made.	47 U.S.C. § 227(b)(1)(A)(iii) 47 CFR § 64.1200(a)(1)(iii)