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

September 10, 2025

VIA ELECTRONIC DELIVERY AND CERTIFIED MAIL - RETURN RECEIPT REQUESTED

To: Brisa Cruz
Belthrough, LLC
1942 Broadway, Ste 314C
Denver, CO 80302
brisa@belthrough.com

Re: Notification of Suspected Illegal Traffic

Dear Brisa Cruz,

Belthrough, LLC (Belthrough or Company) is apparently transmitting illegal robocall traffic onto the U.S. network as an originating and gateway provider. The Enforcement Bureau (Bureau) of the Federal Communications Commission (FCC or Commission) provides this letter as notice of important legal obligations and steps that the Company 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 the Company's traffic.**

I. Background

In August 2024, YouMail, Inc. (YouMail)[1] reported a significant volume of robocalls impersonating major Internet Service Providers (ISPs) and purporting to offer a discounted price for "service."[2] The impersonated ISPs included Spectrum, Comcast/Xfinity, AT&T, and DirecTV.[3] Some of these robocalls included prerecorded messages requesting that recipients call back on toll-free numbers identified in the message; subsequent variations included prerecorded messages requesting that recipients call the callers back on the number displayed on the recipient's caller ID. Many of the prerecorded messages were as follows: "This call is about an important upgrade for your Spectrum services. Dear customer, this is to inform you that Spectrum is removing the 40% discount offer on your monthly bill. To reactivate this please press 1.[4]"

The FCC estimates receiving approximately 1,200 consumer complaints relating to ISP impersonation in 2024 and the first half of 2025. In one such complaint, a consumer described receiving ISP impersonation calls and her interactions with the scam call centers: "I called the number back . . . to find out more about the Spectrum promotion . . . . They described the promotion this way: I can get my internet, TV and phone bill cut in half if I paid 9 months in advance. So by paying Spectrum $1440 now would lock in the discounted rate.[5]"

---

[1] YouMail is a third-party robocall identification and blocking service. *See About Us*, YouMail, https://www.youmail.com/home/corp/about (last visited Oct. 23, 2024).

[2] Email from {[ ]}, YouMail, to David Konuch, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Aug. 16, 2024, 19:55 EDT).

[3] *Id.*

[4] *See* ITG Subpoena Response (Sept. 19, 2024) at Traceback 18759 (on file at EB-TCD-24-00037445) (ITG Sept. 2024 Response).

[5] FCC Complaint # 7455461 (Nov. 12, 2024) (on file at EB-TCD-24-00037445).

She was sometimes instructed to pay the caller with gift cards to obtain the discount: "Ma'am, in order for this to work, Spectrum has partnered with Target stores to bring this promotion to you. Do you shop at Target? . . . . Then what you can do is purchase 4 gift cards in the amount of $360 each.[6]"

In another instance, a consumer complained that she sent $770 in gift cards to a caller impersonating her ISP, for a discount her actual ISP was not offering.[7] The complainant only realized that the purported offer was a scam through online research after sending the gift cards.[8]

YouMail estimates that callers impersonating ISPs placed approximately 97 million robocalls in 2024, an average of more than 8 million calls per month. In the first quarter of 2025 alone there were nearly 28 million ISP impersonation robocalls.[9] Affected ISPs have warned consumers about these deceptive impersonation calls.[10] The calls have generated hundreds of complaints to the Commission and also caught the attention of news organizations, [11] and the Federal Trade Commission.[12]

USTelecom's Industry Traceback Group (ITG)[13] receives "tracebacks," formal requests to trace an alleged illegal robocall to its source, from law enforcement entities and government agencies on behalf of consumers. The ITG investigated the calls identified in Attachment A (the "identified calls" or "identified traffic"), and determined that Belthrough served as either the originating or gateway provider transmitting these calls.[14]

The ITG notified Belthrough of these calls and provided it with supporting data identifying each call.[15] Belthrough confirmed that it had transmitted the identified calls and identified its upstream

---

[6] *Id.*

[7] *See id*.

[8] *Id.*

[9] Email from {[ ]}, YouMail, to David Konuch, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau, Attachment "Spectrum Est Calls - 2025-04-18" (Apr. 18, 2025, 16:43 EDT).

[10] *See, e.g.*, Scam and Fraud Alerts, Spectrum, https://www.spectrum.net/support/general/scam-and-fraud-alerts (last visited Aug. 14, 2024) ("Scammers posing as Spectrum are targeting customers with a significant discount on their monthly bill for cable services over an extended period, which can only be activated by purchasing retailer gift cards, such as those from CVS, Target, etc. This is part of a known fraud scam that targets customers of Spectrum as well as of other companies.").

[11] *See*, *e.g.*, FCC Complaint # 7629898 (Feb. 5, 2025) (on file at EB-TCD-24-00037445)("Recorded message call claiming to be from Spectrum" then transferred to live telemarketer allegedly offering "discount"); Tanya Rivers, *Spectrum call about a 50% off discount is a 'Known Scam'*, WFMY News 2 (Updated Dec. 6, 2023, 9:38 AM EST), https://www.wfmynews2.com/article/news/local/spectrum-50-percent-off-monthly-bill-call-is-a-scam-fraud-alert-website/83-f8cfa8ea-3123-4f97-a517-422be79ce33a; *Scammers pose as Spectrum Cable promising discount*, 2 First Alert WBAY.com (Mar. 1, 2024, 12:54 PM EST), https://www.wbay.com/video/2024/03/01/scammers-pose-spectrum-cable-promising-discount/.

[12] *See Discounted phone, TV, or internet services if you pay with a gift card? No, it's a scam*, Federal Trade Commission Consumer Alert, April 28, 2028, https://consumer.ftc.gov/consumer-alerts/2025/04/discounted-phone-tv-or-internet-services-if-you-pay-gift-card-no-its-scam, last visited June 24, 2025.

[13] The ITG is the registered industry consortium selected pursuant to the TRACED Act to conduct tracebacks. *See Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order, 38 FCC Rcd 7561, 7561-62, para. 1 (EB 2023).

[14] *See* ITG Sept. 2024 Response, *supra* note 4; 47 CFR § 64.1200(f)(19) (defining "gateway provider" as "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").

[15] *See id.*

provider for each call as a foreign provider.[16] In two other instances, Belthrough identified itself as the "calling party," although the Company noted under "steps taken" that it had "blocked that user from our network" and that the customer was on a trial account.[17]

II. Apparent Violations

A. The Identified Traffic Was Apparently Illegal

It is unlawful to make calls to cellphones or residential landlines using an artificial or prerecorded voice message absent an emergency purpose, prior express consent of the called party, or an exemption in the Commission's rules.[18] Furthermore, artificial or prerecorded voice message calls to cellphones or residential landlines that introduce an advertisement or constitute telemarketing[19] are illegal absent prior express *written* consent.[20] Here, the identified calls all featured prerecorded voice messages and were placed to cellphones or a residential landline.[21] The identified calls were made without the prior express consent, written or otherwise, of the call recipient, were not made for an emergency purpose, and did not fall under an exemption in the Commission's rules.[22] Accordingly, the identified calls were apparently illegal.[23]

B. Belthrough Apparently Transmitted the Identified Traffic

A provider's failure to protect its network can ultimately result in downstream providers permanently blocking all of the provider's traffic.[24] Here, Belthrough did not dispute that it transmitted the identified calls, or that the calls were illegal.[25]

III. Potential Consequences

As a result of serving as the gateway provider for apparently illegal calls, Belthrough potentially faces permissive blocking under section 64.1200(k)(4)[26] of the Commission's rules, mandatory blocking under section 64.1200(n)(3)[27] of the Commission's rules, and additional consequences under section 64.6305(g)[28] of the Commission's rules.

---

[16] *See id*.

[17] ITG Subpoena Response (June 23, 2025) (on file at EB-TCD-24-00037445) (ITG June 2025 Response).

[18] *See* 47 U.S.C. § 227(b)(1)(A); 47 CFR § 64.1200(a)(1), (9).

[19] *See* 47 CFR § 64.1200(f)(1) ("The term 'advertisement' means any material advertising the commercial availability or quality of any property, goods, or services."); *id.* § 64.1200(f)(13) ("The term 'telemarketing' means the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person.").

[20] *See id*. § 64.1200(a)(2).

[21] *See* ITG Sept. 2024 Response, *supra* note 4.

[22] *See id*. The ITG categorized these calls as "ISP/Cable/Wireless-Impers-P1," referring to the campaign of robocalls apparently impersonating ISPs. *See*, *e.g.*, *id.* at Traceback 18759. None of the identified calls fall within the narrow exemptions identified in section 64.1200(a)(9) of our rules. *See* 47 CFR § 64.1200(a)(9).

[23] *See* 47 U.S.C. § 227(b)(1)(A); 47 CFR § 64.1200(a)(1)-(2).

[24] *See* 47 CFR § 64.1200(n)(2)-(3).

[25] *See* ITG Sept. 2024 Response, *supra* note 4.

[26] *See* 47 CFR § 64.1200(k)(4).

[27] *See id.* § 64.1200(n)(3).

[28] *See id.* § 64.6305(g).

A. Belthrough 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 (including a gateway 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.[29] 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.[30]

This letter provides notice, pursuant to section 64.1200(k)(4), that Belthrough 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 pursuant to section 64.1200(k)(4).[31] Belthrough should inform the Commission and the ITG, within 48 hours of the electronic delivery of this letter, of the specific steps it has taken to mitigate illegal traffic on its network.[32]

B. Belthrough 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) of the Commission's rules.[33]

This letter serves as a Notification of Suspected Illegal Traffic (Notice) to the Company under section 64.1200(n)(2) of the Commission's rules.[34] The Company must take the following actions in response to this Notice:

1. Promptly investigate the calls identified in Attachment A for which the Company served as the originating or gateway provider;[35]
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;[36] and
3. Report the results of the Company's investigation to the Bureau within 14 days of the date of this Notice.[37] The Company should copy the ITG on communications to the Bureau.

---

[29] *See id.* § 64.1200(k)(4).

[30] *See id.*

[31] *See id.*

[32] *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).

[33] *See* 47 CFR § 64.1200(n)(2)-(3).

[34] *See id.* § 64.1200(n)(2).

[35] *See id.* § 64.1200(n)(2)(i)(A).

[36] *See id.*

[37] *See id.*

Depending on the outcome of the investigation, the report must contain certain details as described below:[38]

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;[39]
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;[40] 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.[41]

1. Initial Determination Order

The Bureau may issue an initial determination order stating the Bureau's initial determination that the Company 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 assertions to the contrary.[42] If the Bureau issues an initial determination order, the Company will have an opportunity to respond.[43]

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 the Company 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.[44] A final determination order may be issued up to one year after the release date of the initial determination order.[45]

---

[38] *See id.*

[39] *See id.*

[40] *See id.* § 64.1200(n)(2)(i)(B).

[41] *See id.*

[42] *See id.* § 64.1200(n)(2)(ii).

[43] *See id*.

[44] *See 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) (*Seventh Call Blocking Order*).

[45] *See* 47 CFR § 64.1200(n)(2)(iii).

C. Belthrough Faces Removal from the Robocall Mitigation Database and Mandatory Blocking Under Section 64.6305(g)

Pursuant to section 64.6305(g) of the Commission's rules, intermediate and voice service providers shall only accept traffic from a domestic voice service provider or gateway provider if that provider's certification appears in the RMD.[46] Such filings must include the specific reasonable steps the provider has taken to avoid originating, carrying, or processing illegal robocall traffic as part of its robocall mitigation program.[47] If a company's filing is deficient in some way, the Bureau may initiate a proceeding to remove it.[48]

Belthrough certified in its RMD filing, under penalty of perjury, that it will cooperate with the FCC in investigating and stopping any illegal robocallers that use its service to carry or process calls.[49] **Failure to respond to this letter as described above may be used as evidence that the Company's certification is deficient with respect to its commitment to cooperate.[50] The Bureau may initiate proceedings to remove a deficient filing from the database.** If the Company's certification is removed from the RMD for any reason, all intermediate providers and terminating voice service providers must cease accepting all of the Company's calls.[51] If the Bureau initiates a proceeding to remove the Company's certification from the Robocall Mitigation Database, the Company will have an opportunity to cure the deficiency.[52]

---

[46] *See id.* § 64.6305(g)(1), (3). 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).

[47] *See id.* § 64.6305(d)(2)(ii), (e)(2)(ii).

[48] *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, Order, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and 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 rule applies to gateway providers as well as voice service providers); *see also Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2590, para. 31 (2023) (*Sixth Caller ID Authentication Order*) ("[A] provider's program is 'sufficient if it includes detailed practices that can reasonably be expected to significantly reduce' the carrying or processing (for intermediate providers) or origination (for voice service providers) of illegal robocalls. Each provider 'must comply with the practices' that its program requires, and its program is insufficient if the provider 'knowingly or through negligence' carries or processes calls (for intermediate providers) or originates (for voice service providers) unlawful robocall campaigns." (citations omitted)).

[49] *See* Belthrough (No. RMD0015088), Fed. Commc'ns Comm'n, Robocall Mitigation Database (filed March 11, 2025), https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=b058b2201b30b5103c7943bae54bcb27&view=sp.

[50] *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).

[51] *See* 47 CFR § 64.6305(g).

[52] *Second Caller ID Authentication Order*, 36 FCC Rcd at 1903, para. 83; *Gateway Provider Order*, 37 FCC Rcd at 6882, para. 40.

Please direct any inquiries regarding this letter to David Konuch, Attorney Advisor, Telecommunications Consumers Division, Enforcement Bureau, at david.konuch@fcc.gov and cc: to Daniel Stepanicich, Deputy 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
Acting Chief
Enforcement Bureau
Federal Communications Commission

Attachment A

Belthrough Tracebacks

Role	Customer	Call Date & Time	Calling No.	Called No.	Description	Apparent Violations
POE[53]	CSC Telecom Ltd.	Jul 17, 2024 18:43 UTC	{[ ]}	{[ ]}	ISP/Cable/Wireless Impersonation	47 U.S.C. § 227(b); 47 CFR § 64.1200(a)
POE	CSC Telecom Ltd.	Jul 17, 2024 18:45 UTC	{[ ]}	{[ ]}	ISP/Cable/Wireless Impersonation	47 U.S.C. § 227(b); 47 CFR § 64.1200(a)
POE	CSC Telecom Ltd.	Jul 17, 2024 19:04 UTC	{[ ]}	{[ ]}	ISP/Cable/Wireless Impersonation	47 U.S.C. § 227(b); 47 CFR § 64.1200(a)
POE	CSC Telecom Ltd.	Jul 17, 2024 19:12 UTC	{[ ]}	{[ ]}	ISP/Cable/Wireless Impersonation	47 U.S.C. § 227(b); 47 CFR § 64.1200(a)
POE	CSC Telecom Ltd.	Jul 17, 2024 20:26 UTC	{[ ]}	{[ ]}	ISP/Cable/Wireless Impersonation	47 U.S.C. § 227(b); 47 CFR § 64.1200(a)
ORG[54]	Belthrough	Apr 09, 2025 18:40 UTC	{[ ]}	{[ ]}	ISP/Cable/Wireless Impersonation	47 U.S.C. § 227(b); 47 CFR § 64.1200(a)
ORG	Belthrough	Apr 23, 2025 18:04 UTC	{[ ]}	{[ ]}	ISP/Cable/Wireless Impersonation	47 U.S.C. § 227(b); 47 CFR § 64.1200(a)

[53] "POE" denotes that the Company was identified as the gateway provider or point of entry for the call.

[54] "ORG" denotes that the Company was identified as the Originating Voice Service Provider.