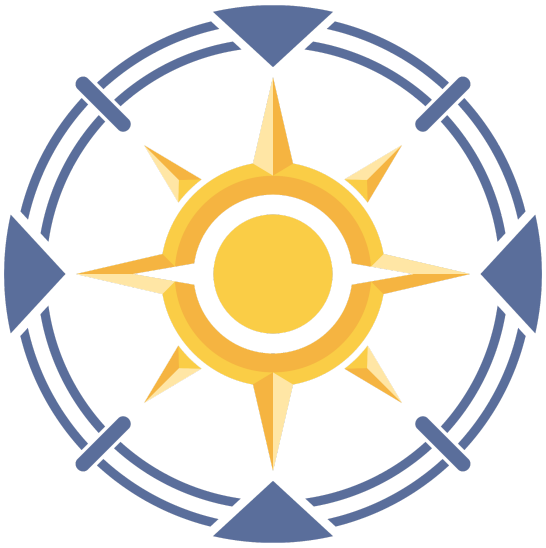


The Fight Against Scammers On Telecom Networks

Why America’s Telecoms Are Losing the War On Scams

September 13, 2026

By the Demurrage Team

Contents

Contents **2**
Disclaimer **2**
Introduction **3**
Background: How The U.S. VoIP Industry Works 4
A “Mark” Controlled Business 6
Where To Find A Mark If You’re A Scammer 8
Consumers Lack The Tools To Fight Back 12
What’s Not Working: Bandwidth and the Wholesale Runaround **14**
Google Voice Numbers 15
The Infrastructure Used to Defeat KYC Controls 25
What Is Not Working: Sinch and Its Refusal to Communicate **32**
Problems with Sinch’s webform 35
Notable Cases 39
Notable cases 57
What Works: Telecom Action That Actually Stops Fraud **66**
Statistics: Lumen 67
Notable Cases 68
Statistics: IP Horizon 73
Notable Cases 74
Closing Statements **80**
Email Records: Sinch **83**
Email Records: Bandwidth **83**
Email Records: Lumen **83**
Email Records: IP Horizon **83**

Disclaimer

Demurrage is an independent, self-funded collective specializing in detailed investigations into how scammers exploit American communications networks and consumers. Demurrage has not received payment from any outside entity or organization, for or against any party. Its work focuses on reporting numbers used in tech support fraud to the appropriate carriers, tracking carrier response times, and documenting outcomes without bias.

Introduction

With 2026 now entering its final three months, scam related abuse of VoIP telecommunications providers shows no signs of slowing down. The responses of such providers to scammers abusing their services can be grouped into two categories: meaningful action taken, and a lack thereof. **There is no middle ground.**

While Demurrage has previously published detailed reports on individual telecom responses to fraud and the abuse patterns those telecoms have often ignored, no report has yet compared one telecom's response directly against another's. This report aims to provide that information, offering consumers and governing bodies an understanding of how complicated the problem has become. There is currently no universal standard for addressing fraud beyond the common advice to block the phone number or report it to the FCC or FTC, neither of which addresses the issue at its source, the actual toll-free or tolled number used by scammers to commit tech support fraud, which requires the provider itself to terminate the number for fraudulent use.

While scammer activity continues to rise, the methods by which scammers acquire U.S. toll-free and tolled numbers have changed dramatically, and not for the better.

Robust KYC policies adopted by many telecoms to prevent scammers from acquiring such numbers have already been defeated, and were being defeated even before widespread adoption. With governing bodies still focused primarily on stopping robocalls, many telecoms and regulators remain either unaware of the actual source of the problem or have little interest in addressing it. While robocalls remain a concern, existing policies still fail to address the tech support scam side of the industry, in which a consumer receives a fraudulent email, invoice, or pop-up designed to resemble a virus warning and instructs them to call a toll-free or tolled number for fraudulent technical support, under the threat that failure to do so will result in the loss of personal or sensitive data.

Many in the industry are quick to dismiss claims that they are not doing enough to stop such scams. However, Demurrage has observed a disturbing trend over the last three years strongly suggesting that many telecoms have little interest in addressing this

issue. As Demurrage's data grows, the evidence consistently points back to the same telecoms being repeatedly abused by scammers, and the actions, or lack thereof, taken by these telecoms reinforce the central finding of this report, either action is taken, or none is taken at all.

This report examines 4 telecoms and documents the responses received when fraud cases involving their VoIP numbers used in tech support scams were submitted.

These 4 telecoms were selected based on the volume and consistency of data collected, both positive and negative, and on the degree to which a clear pattern of action or inaction could be observed for each.

The telecoms featured in this report are Lumen, IP Horizon, Sinch and Bandwidth.

Background: How The U.S. VoIP Industry Works

When Demurrage states that robust KYC policies have already been defeated by scammers, this conclusion is based on evidence gathered and continuously observed in the field. While many telecoms assert that they maintain strict KYC policies and are fully compliant with STIR/SHAKEN rules, these policies are not bulletproof.

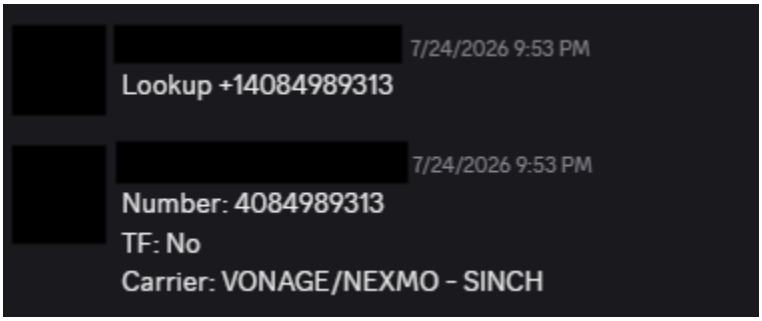
In fact, many of the telecoms that champion these policies are among the most frequently abused when it comes to numbers being used in tech support fraud. A common misconception is that telecoms are complicit with scammers and therefore have an incentive to overlook such activity.

Demurrage does not hold this view.

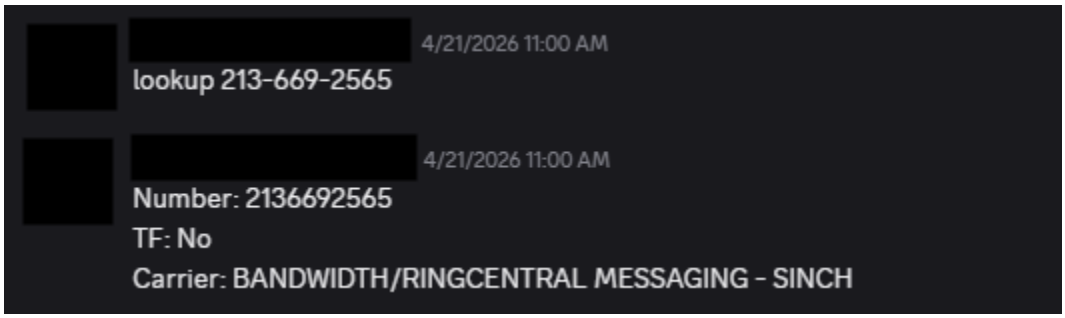
To understand why overseas scammers continue to abuse the same telecoms, it is necessary to first understand how the U.S. telecom industry operates and why it remains so easy for scammers to exploit the system without ever setting foot on U.S. soil.

When a VoIP number, whether toll-free or tolled, is sold to a consumer, it is not purchased directly from the telecom, even when registered through that provider's own website. The number is typically sold by a third party, commonly referred to as a wholesale provider, operating within the telecom's network and infrastructure. So while a consumer may pay the VoIP provider for the number, it is effectively purchased from one of that provider's wholesale partners, who receive a percentage of the sale with the remainder going to the VoIP provider.

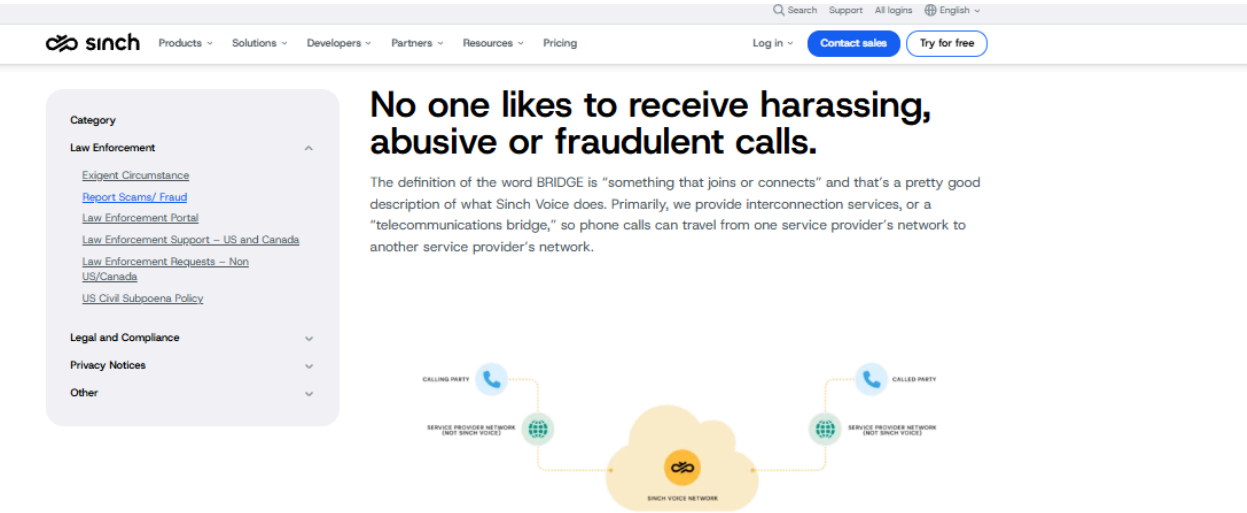
This can be verified by using a carrier lookup service to identify who actually sold the number, or by reporting a number to a VoIP provider and receiving a response indicating that while the number traces back to them, it is managed by one of their wholesale partners.



For example, toll-free providers such as RingCentral offer tolled numbers for sale but do not own those numbers directly. Instead, such numbers are supplied by one of three companies: Sinch, Bandwidth, and Level 3 via Lumen. The same applies to other major VoIP providers offering both toll-free and tolled numbers. In these cases, a fraud report could in theory be submitted to all three underlying providers if a number is found to be used in a tech support scam.



Notably, Sinch's designated robocall reporting web form illustrates this dynamic clearly and provides a useful summary of how U.S. VoIP providers operate within this framework.



In some cases, certain VoIP providers act as sellers to other companies that distribute these numbers to consumers. While this structure has a certain internal logic, this is precisely where both the confusion and the problems begin.

A “Mark” Controlled Business

Demurrage defines a "mark" as a complicit wholesale provider that willingly and knowingly sells accounts and toll-free numbers to overseas scammers for the sole purpose of facilitating tech support fraud.

A mark is not the telecom itself, but a customer of the telecom operating within its network. Marks exist within nearly every major U.S. VoIP provider's network, a conclusion based on extensive email evidence and other verified sources confirmed by Demurrage prior to publication.

Marks have become the primary means by which scammers defeat KYC policies and acquire U.S. toll-free and tolled numbers for use in tech support fraud. Evidence consistently indicates that nearly every number used in a tech support scam was either sourced or controlled by a mark operating within that provider's network.

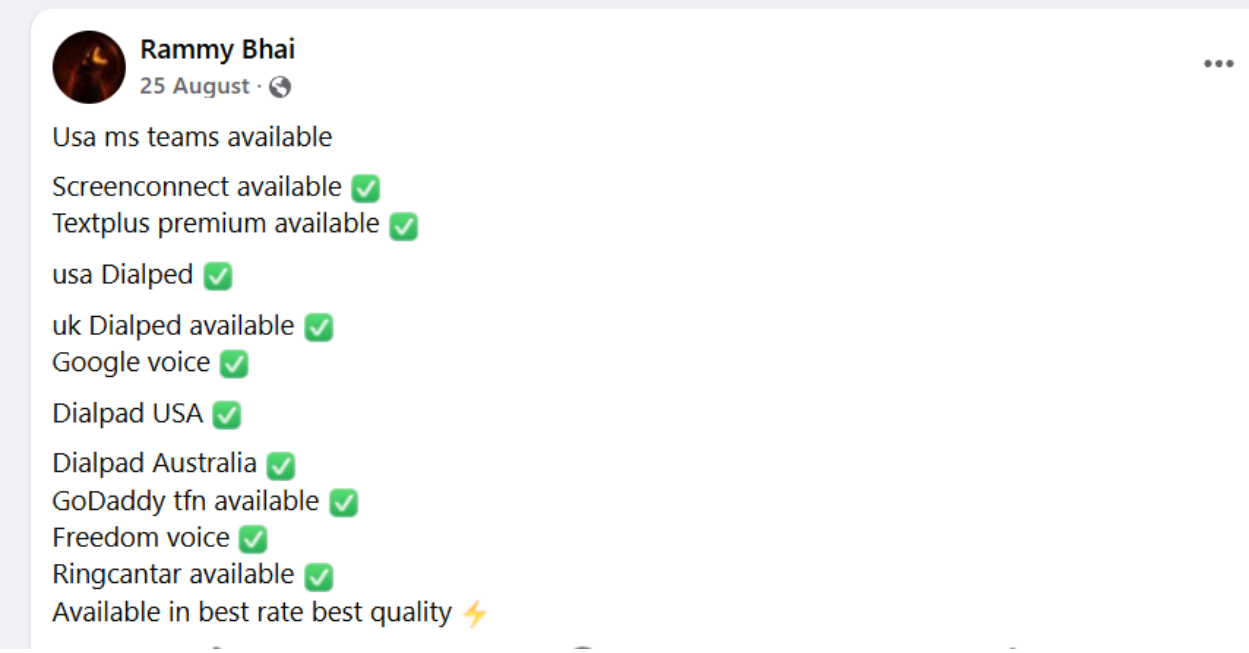
While some believe that telecoms deliberately overlook complicit wholesale providers because it is profitable for both parties, it is highly unlikely that marks are accurately reporting or passing back the correct percentage of their sales to the telecom. Evidence suggests that scammers pay significantly more than the standard market rate, particularly when entire accounts are sold. If telecoms are either unaware of this or unwilling to acknowledge that their wholesale providers are the source of the problem, it is unreasonable to expect that a mark is accurately declaring sales at standard market price, as reporting the true sale amount would raise immediate red flags and risk removal from the network, the very outcome marks seek to avoid, as it would disrupt their ability to sell to and profit from scammer clients.

This is why Demurrage firmly believes that the claim that scammers are in bed with major U.S. VoIP telecoms is false.

It is the marks who generate the greatest profit from these transactions, charging scammers a premium precisely because the scammers are not required to submit their own KYC documentation. It is unlikely that major U.S. VoIP providers are receiving an accurate percentage of such inflated sales, and if any revenue is being reported, it is most likely declared at standard market price by the mark.

Where To Find A Mark If You’re A Scammer

Defeating KYC is often the primary selling point advertised by both marks and scammers, as demand for pre-verified accounts is extremely high. Such sales and advertisements originate within social media groups on platforms including Facebook, Twitter, WhatsApp, and Telegram, and no telecom is off limits, which is perhaps the most concerning aspect of this trend.



High -**quality USA CLI routes** with **full passability**

We've got you covered with **Tier-1 Bandwidth Routes** — optimized for **manual** and **VICIdial traffic**.

✔️**All ANI Pass**

✔️ **18xx / TFN / Local – All Pass**

✔️**Stable for Manual** & **Vici Traffic**

✔️ **Tier-1 Bandwidth Routes**

✔️ **24/7 Technical Support**

✔️ **Instant Testing Available**

💰 **Rate: Just $0.*095* per minute**

🚀 **Test** & **Start Your Traffic Today**!

If you have active traffic, **connect with us now**.

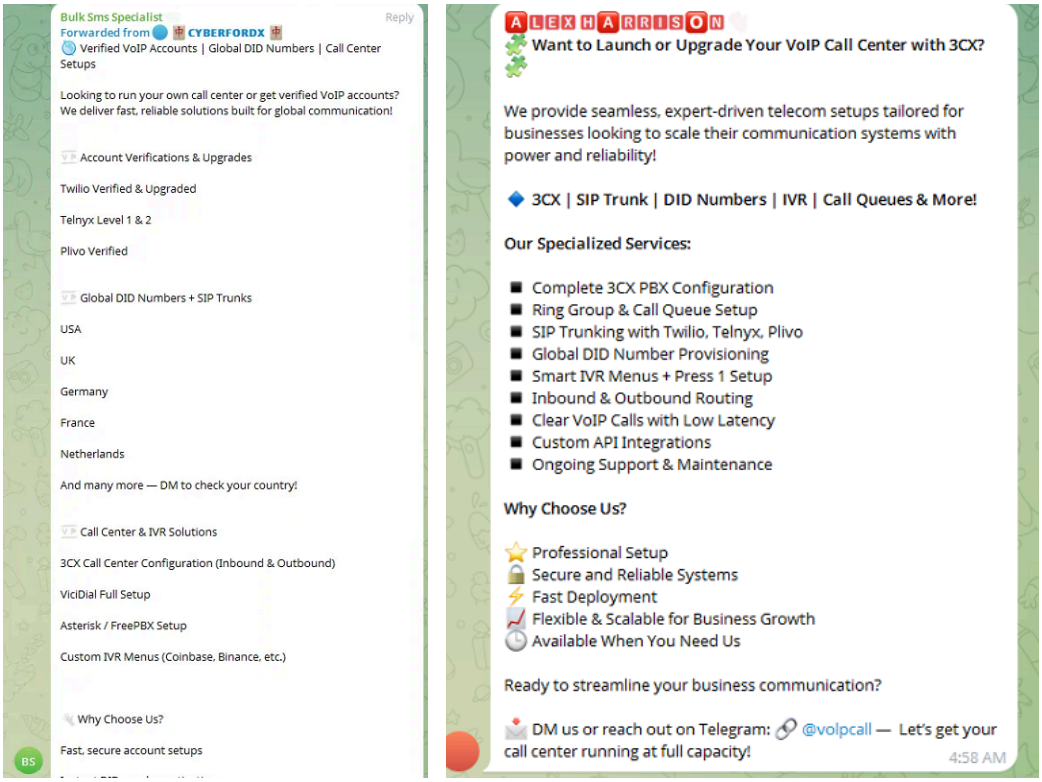
📩 **Send your IP for testing** and experience **premium route quality**.

👉 **Let's build long-term business together**!

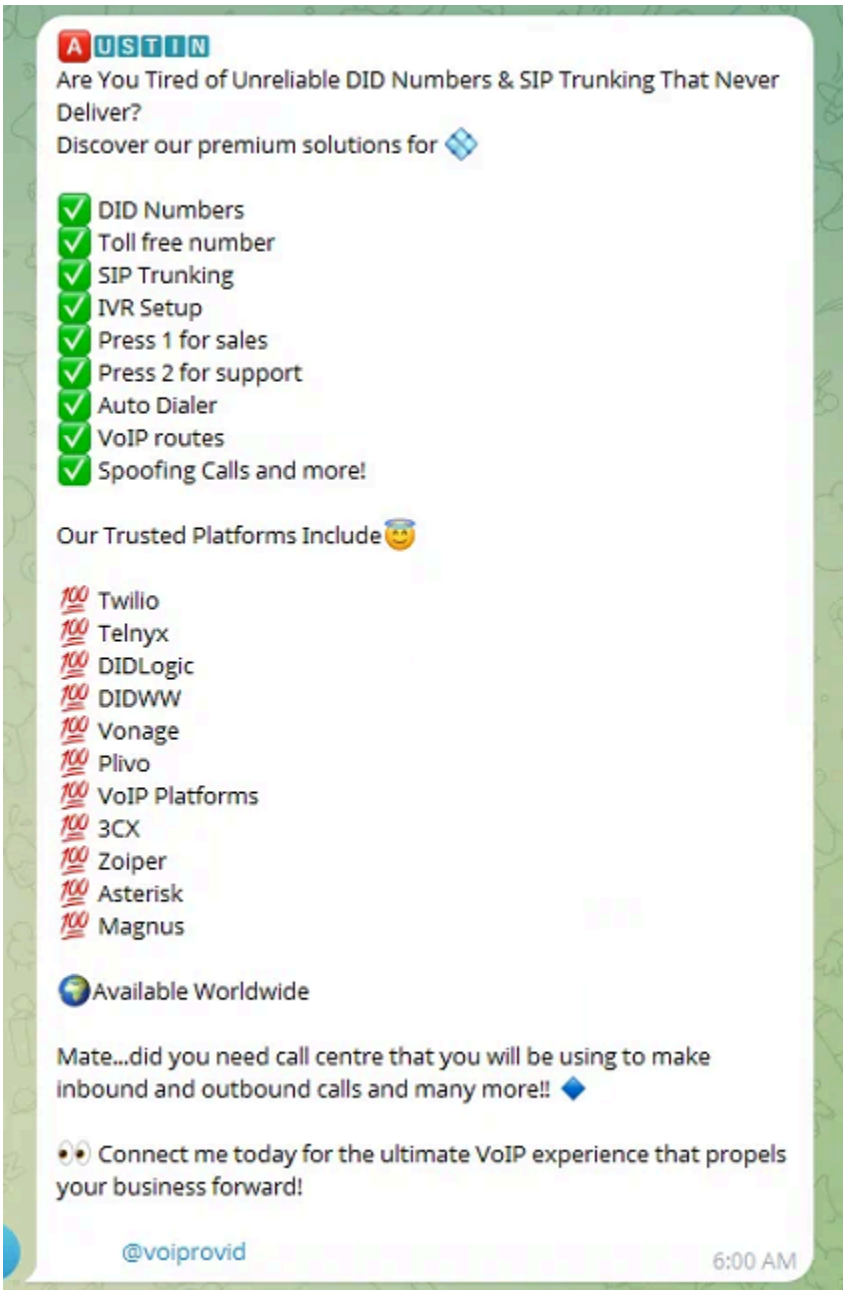
📲**WhatsApp**: +447367068224



18009505114	4456162		00:02:43	00:55:47
18005284800	4456120		00:04:17	00:54:12
18005284800	4456131		00:33:43	00:24:46
18009505114	4456163		00:41:57	00:16:32
18009564442	4456164		00:49:41	00:08:49



STIR/SHAKEN has also been defeated, as marks advertise their ability to sell accounts capable of spoofing numbers openly, the very activity STIR/SHAKEN was designed to prevent. Demurrage has observed this firsthand on numerous occasions, as scammers frequently acquire separate tolled VoIP numbers, commonly referred to as callback numbers, to contact victims directly. In approximately half of the callback instances documented, the numbers were spoofed, indicating that scammers deliberately avoid using their primary numbers to reduce the risk of those numbers being reported for fraud.



Marks are the primary mechanism by which scammers have defeated KYC policies, and this is no longer a matter of dispute. Serious regulation and accountability must be enforced by both the VoIP provider industry and the governing bodies associated with it.

More concerning still, while telecoms are quick to announce robust KYC enforcement for direct sales, the same scrutiny does not appear to extend to their wholesale partners. No telecom, based on current U.S. law, appears to have ever been required to disclose the identities of its wholesale providers, whether a mark or a smaller company operating within the VoIP provider's infrastructure. The requirements for becoming a wholesale provider within these networks remain unclear. What is clear, however, is that just as the scammers purchasing these numbers are based overseas, primarily in India and Pakistan, the marks themselves appear to be as well.

This raises serious concerns about how unregulated the U.S. VoIP industry has become and how slow the industry and its governing bodies have been to address the issues currently affecting both consumers and providers.

Consumers Lack The Tools To Fight Back

While Demurrage's work may appear straightforward, it is anything but simple. The most common guidance issued by the FTC and FCC is to block the number, label it as spam, or submit a report. However, this does little to address the underlying issue or meaningfully protect consumers.

When a number is blocked or labeled as spam on a cell phone, it may be flagged within that carrier's network, but this does not prevent scammers from reaching consumers on other networks. For example, if a number is labeled as spam on the Boost Mobile network, it will not carry any such label on the AT&T network, and the call will still connect. This makes the current system fundamentally flawed.

Reporting to the FTC or FCC is equally flawed. The reporting web form itself states that no direct action will be taken and that the report will be forwarded to local law enforcement, which is useless given that the vast majority of tech support scams originate from illegal call centers in India.

Neither resource addresses the actual phone number. The FTC and FCC do not contact the telecom responsible for the number to request its termination, and blocking a number on a cell phone does not produce that outcome either. In fact, some telecoms that refuse to act on fraud reports will direct complainants to block the number or report it to the FTC or FCC instead, further undermining confidence in the system.

Simply put, the average consumer lacks the tools to report a phone number for fraud or to identify which telecom is responsible for it. This is a significant problem in the United States, a country that regularly issues public statements about robocalls and efforts to address them, yet rarely provides consumers with the means to look up a phone number or contact the relevant telecom directly. While some telecoms publish contact information on their websites, most do not provide a dedicated contact listing or web form for anything beyond sales inquiries.

The process Demurrage uses to perform number lookups and trace them back to their respective telecoms requires substantial knowledge of programming and carrier infrastructure, and is only made possible by Demurrage's team of developers. It is not a matter of simply downloading an application.

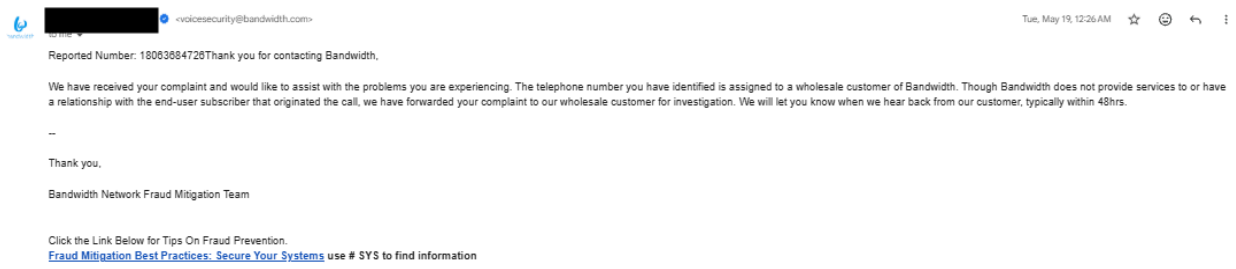
Consumers should have accessible tools to look up phone numbers and report them directly to the telecom on which those numbers are hosted. Such tools should be standard features of all cell and landline services, particularly as an increasing number of consumers are put off by the idea of answering their phones due to the persistent volume of robocalls and tech support scam voicemails.

That this capability is not yet a standard offering in the United States or internationally is a step in the wrong direction.

What's Not Working: Bandwidth and the Wholesale Runaround

The most common approach adopted by major U.S. VoIP providers upon receiving a fraud complaint about one of their numbers is to forward the complaint to their wholesale provider for investigation. In an ideal scenario, one would expect those wholesale providers to respond honestly and take action when presented with a complaint supported by evidence of fraudulent use. However, as discussed earlier, the numbers scammers acquire are sourced from and controlled by marks, and it is here that the first and most fundamental problem arises.

Bandwidth is one of the major players in the VoIP industry with considerable influence, yet its approach to fraud reports has gotten worse over time. Despite periodic updates to its robocall reporting web form, Bandwidth places complete trust in its wholesale providers whenever a number is reported for fraud. At no point during an initial report has Bandwidth directly taken a number offline in response to a fraud complaint. Every report submitted to Bandwidth has been forwarded to a wholesale provider for investigation, regardless of how much evidence of fraud is presented in the email.


[redacted] <voicesecurity@bandwidth.com> Tue, May 19, 12:26 AM

Reported Number: 18063684726Thank you for contacting Bandwidth,

We have received your complaint and would like to assist with the problems you are experiencing. The telephone number you have identified is assigned to a wholesale customer of Bandwidth. Though Bandwidth does not provide services to or have a relationship with the end-user subscriber that originated the call, we have forwarded your complaint to our wholesale customer for investigation. We will let you know when we hear back from our customer, typically within 48hrs.

--

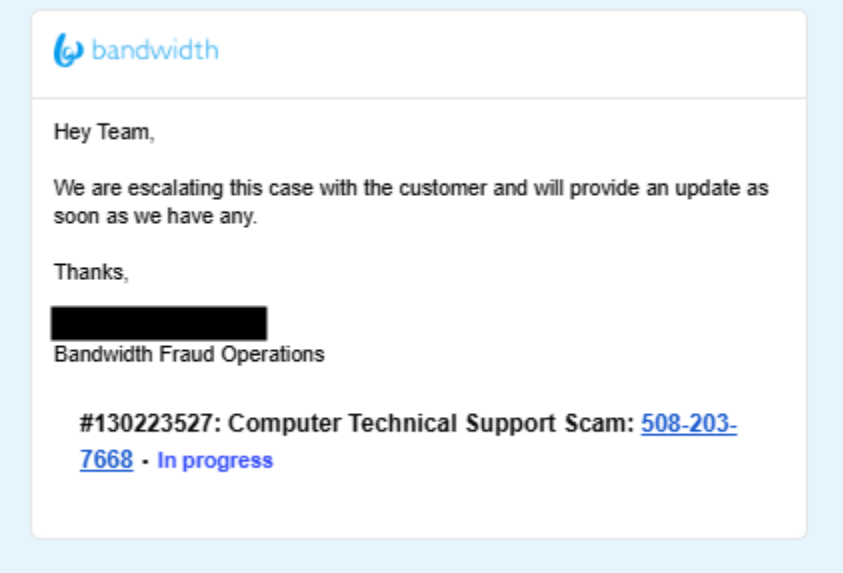
Thank you,

Bandwidth Network Fraud Mitigation Team

Click the Link Below for Tips On Fraud Prevention.
Fraud Mitigation Best Practices: Secure Your Systems use # SYS to find information

Bandwidth states that wholesale providers are given 48 hours to respond to a fraud report, a window that is excessive given the urgency of such complaints. Demurrage has repeatedly observed that many of Bandwidth's wholesale providers routinely allow this period to lapse without responding or updating the status of the case, and Bandwidth makes no attempt to hold them accountable. If the person who submitted the complaint does not manually follow up, no response is ever received from Bandwidth or the wholesale provider. Even when a ticket is updated, several wholesale providers will

still refuse to respond, even after Bandwidth claims to have escalated the issue and requested a reply.


bandwidth

Hey Team,

We are escalating this case with the customer and will provide an update as soon as we have any.

Thanks,

[redacted]
Bandwidth Fraud Operations

#130223527: Computer Technical Support Scam: 508-203-7668 · In progress

RingCentral and Google Voice, both customers of Bandwidth on the tolled number side, routinely allow the 48-hour response window to lapse without responding to fraud complaints, and at no point does Bandwidth hold them accountable.

Google Voice Numbers

Google Voice is by far the most exploited wholesale provider on Bandwidth's network, and every Google Voice number reported to Bandwidth has proven to be an account set up and controlled by a mark.

Google Voice is not available outside of the United States, yet these numbers consistently reach scammers in India. They are also among the most sought-after numbers in the scammer community and are advertised widely across social media platforms.

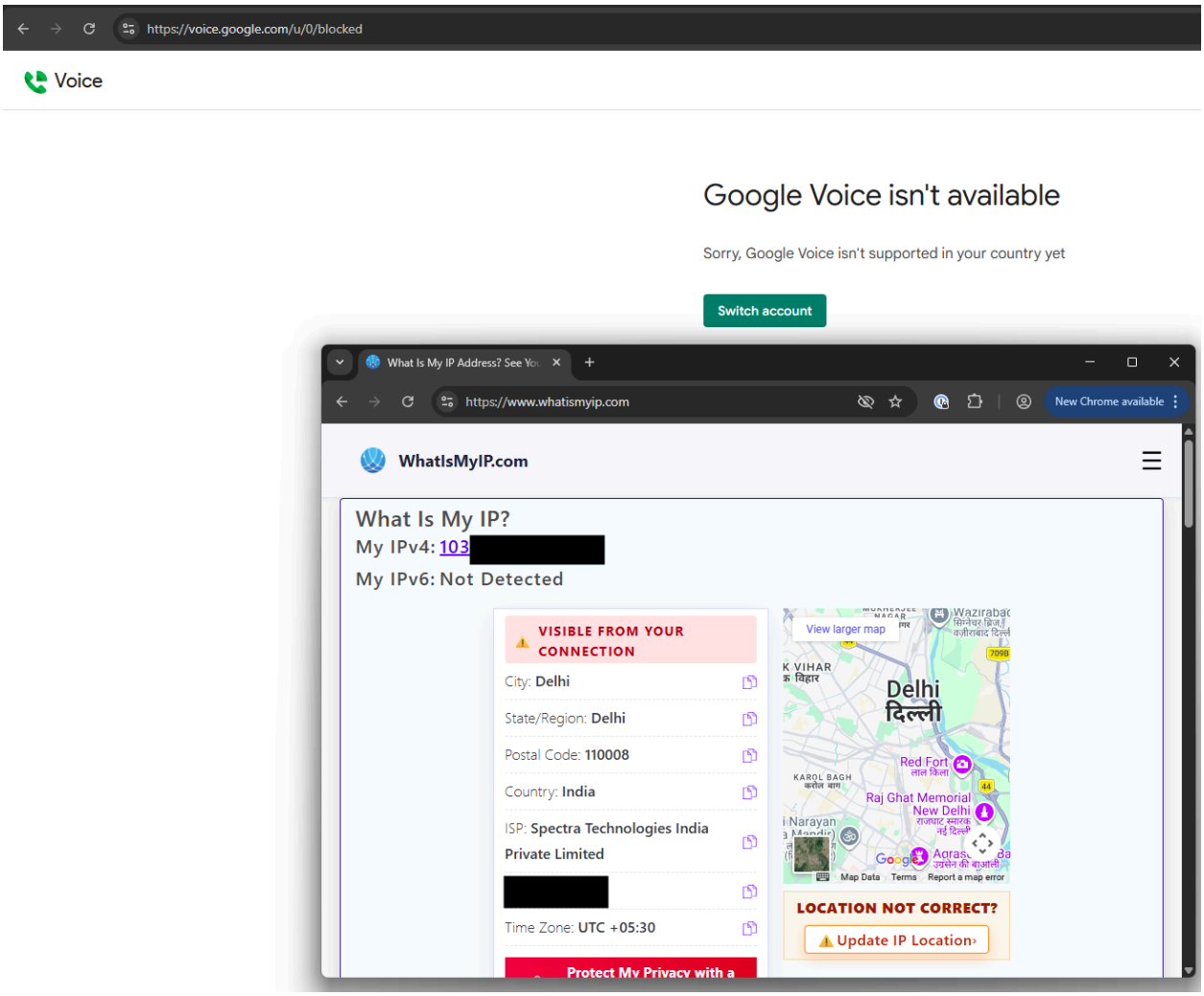

Global Voice Solutions
Global Voice Solutions
GOOGLE VOICE
Dialers
Business Accounts
Unlimited Calling
30 Days Replacement Guarantee
USA, UK, Canada, Australia, Ireland & EUROPE
First Login Then Pay

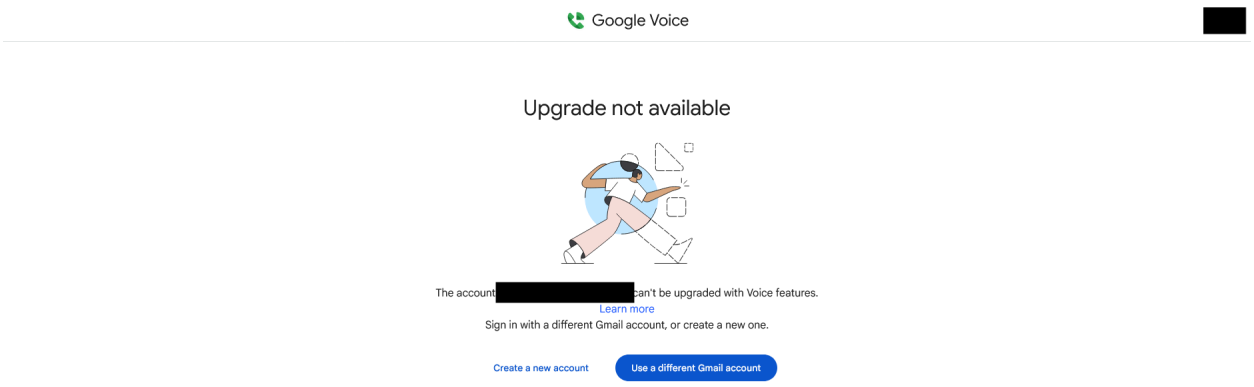

Google
Voice Accounts
Why Choose Us ?
Best Quality Accounts
24/7 Customer Support
Fast Delivery
Real Ip Created Accounts
4-5 hr Warranty
Instant Start your Work
Cheapest On Online
100% Customers Satisfaction
Get Them Below Market Price
Don't Hesitate to Contact me Directly.
Telegram
(Only Text)
+91 9674017637

Data Dialer Voip
21 hours ago ·

Dedicated to delivering transparent, high-quality audio across every network.

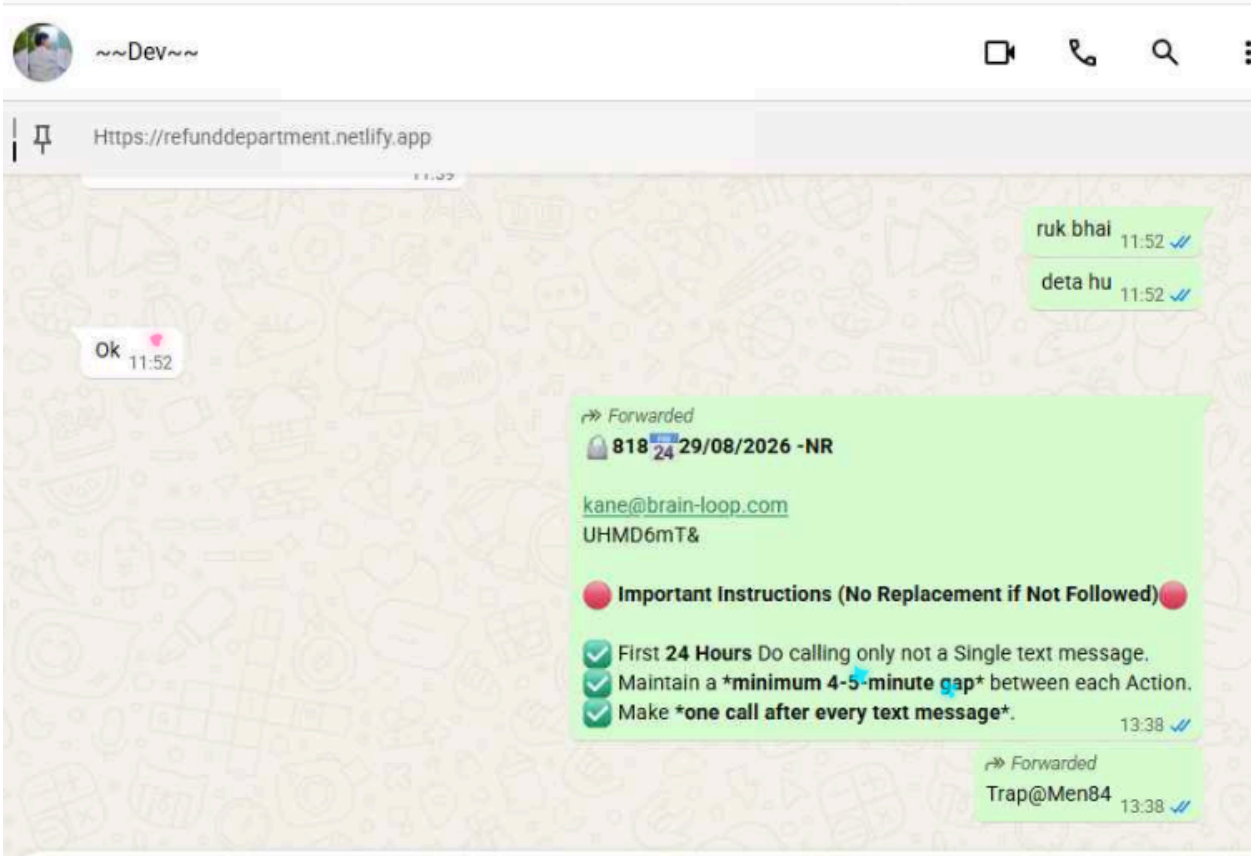



https://voice.google.com/u/0/blocked
Voice
Google Voice isn't available
Sorry, Google Voice isn't supported in your country yet
Switch account
What Is My IP Address? See Yo
https://www.whatismyip.com
New Chrome available
WhatIsMyIP.com
What Is My IP?
My IPv4: 103
My IPv6: Not Detected
VISIBLE FROM YOUR CONNECTION
City: Delhi
State/Region: Delhi
Postal Code: 110008
Country: India
ISP: Spectra Technologies India Private Limited
Time Zone: UTC +05:30
Protect My Privacy with a
View larger map
Delhi
दिल्ली
Red Fort
Raj Ghat Memorial
New Delhi
Map Data
Terms
Report a map error
LOCATION NOT CORRECT?
Update IP Location



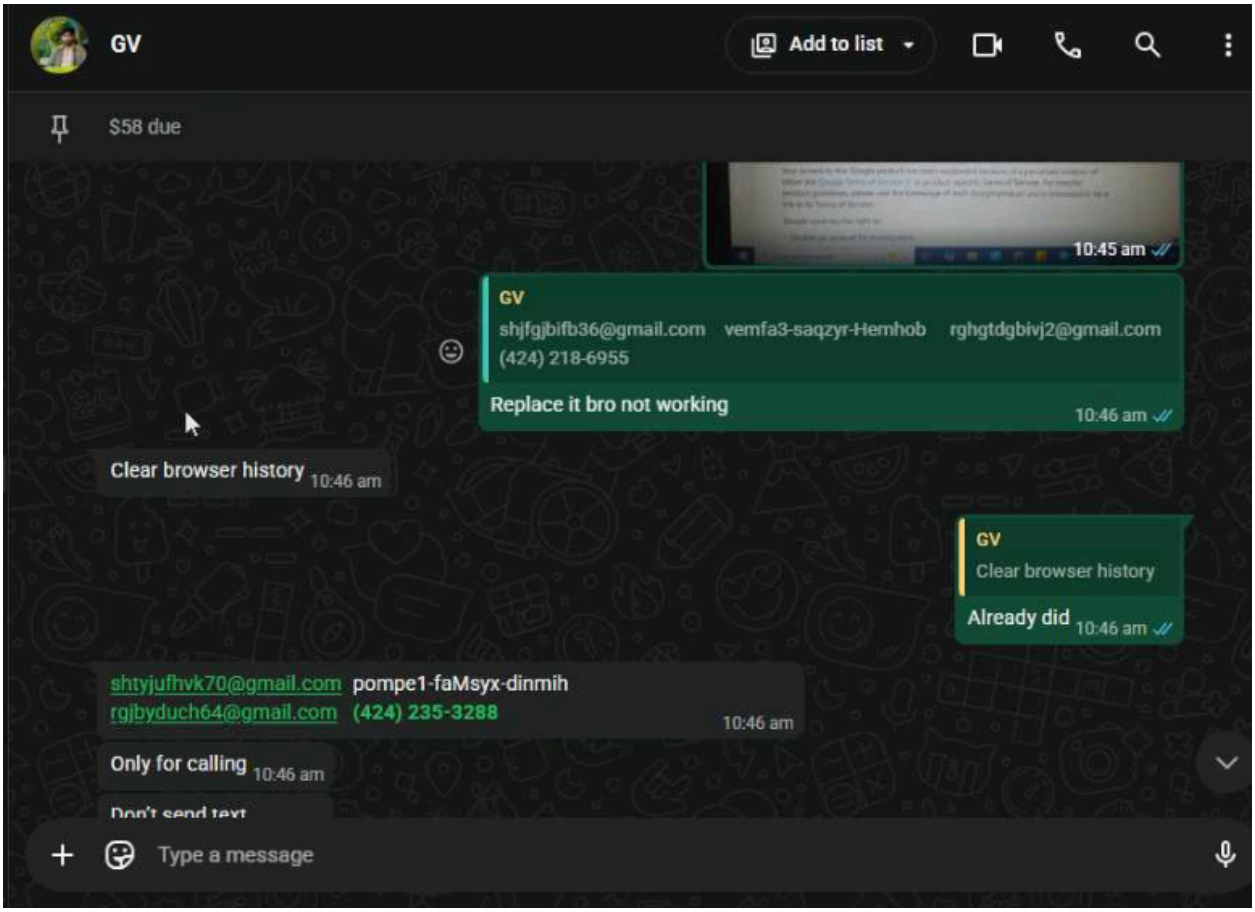
This screenshot was submitted to Demurrage by an anonymous source and verified prior to inclusion in this report.

Marks establish Google Business or standard accounts on behalf of scammers and sell them at a premium, providing login credentials along with instructions on how to use the numbers and avoid fraud detection.



These screenshots were submitted to Demurrage by an anonymous source and verified prior to inclusion in this report.

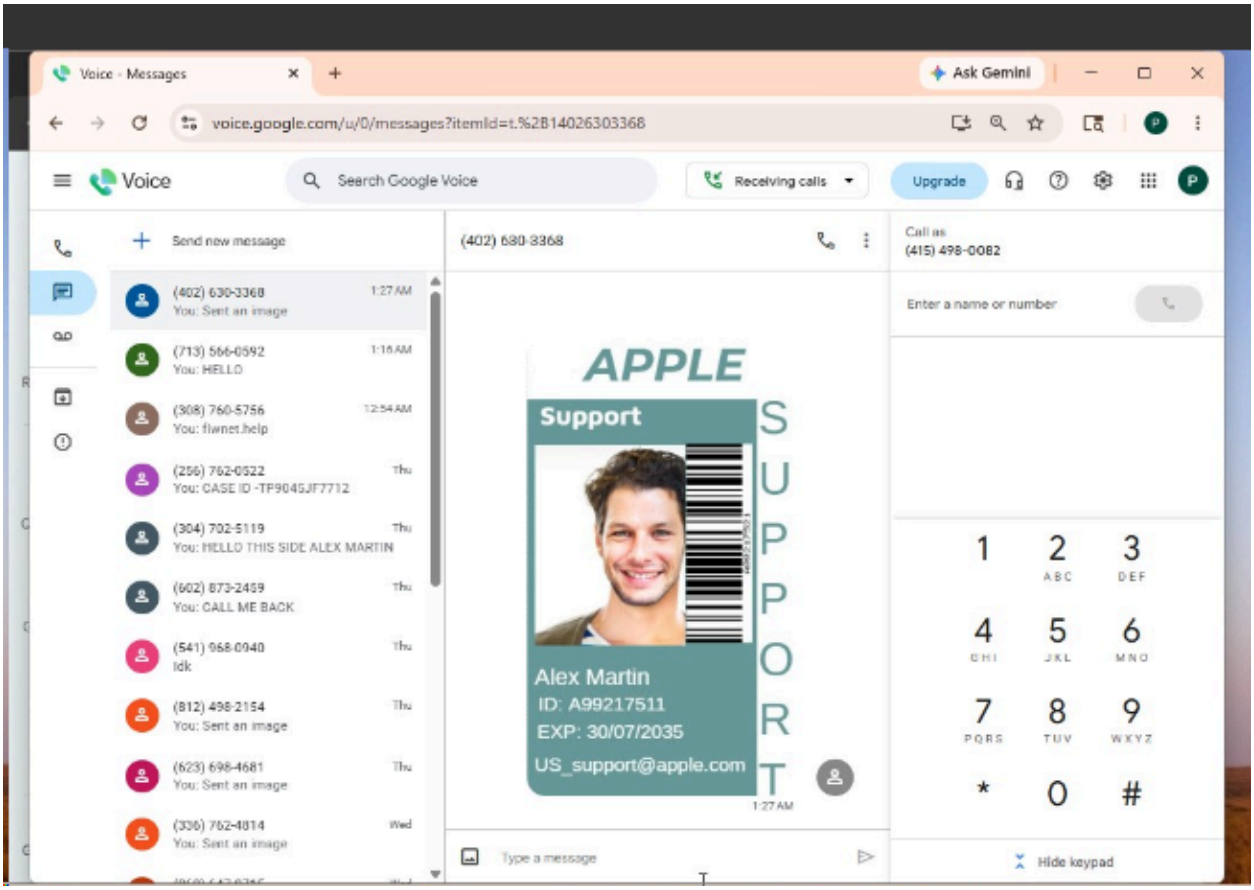
In some cases, marks have been observed replacing reported and deactivated numbers at the scammer's request, further demonstrating that marks maintain an ongoing and active relationship with the scammers they serve.

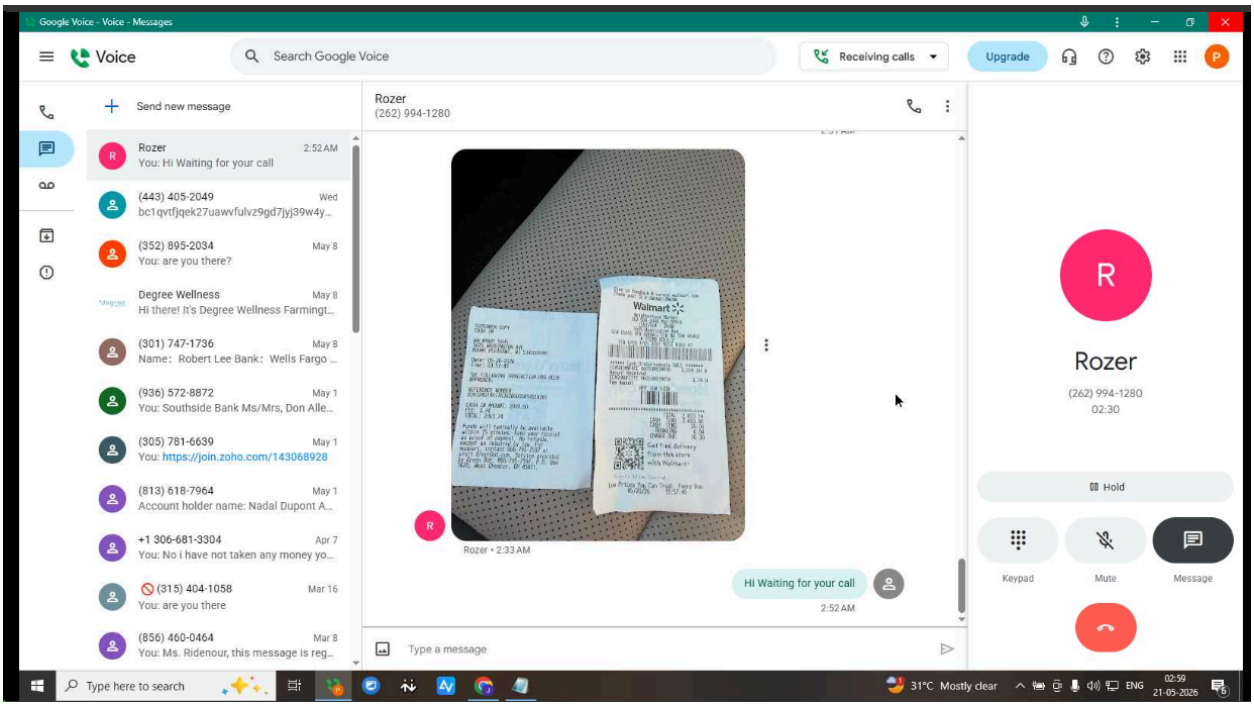


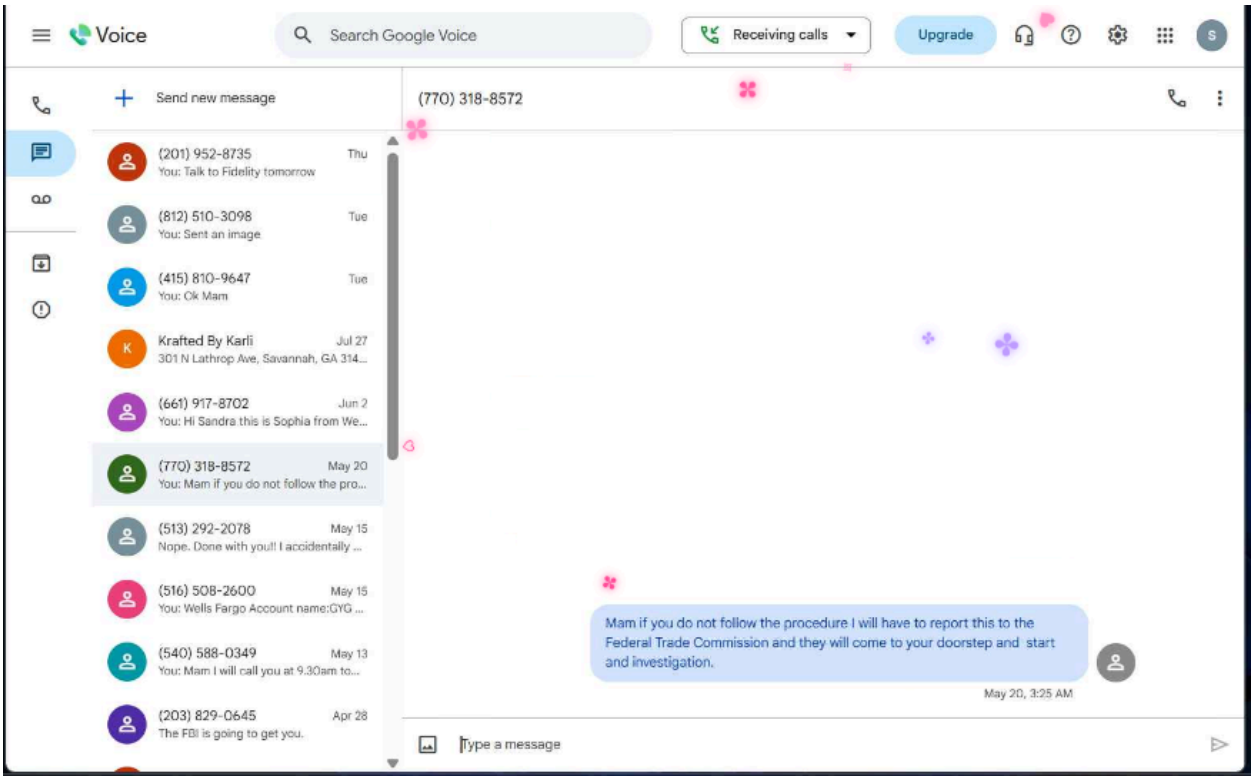
These screenshots were submitted to Demurrage by an anonymous source and verified prior to inclusion in this report.

Scammers now rely heavily on Google Voice to facilitate their scams, directing victims to call a designated line through which scammers can communicate via text and images and issue further instructions, all while accessing Google Voice on devices obtained through marks operating within the VoIP provider's network.

Notably, because these accounts are created by marks using U.S. registration details, Google Voice logs activity in U.S. time. As a result, when scammers in India access these accounts, their activity is recorded in U.S. Eastern Time, revealing that scammers are operating in the early hours of the Indian morning to accommodate the time difference with the United States.


Voice - Messages
Ask Gemini
voice.google.com/u/0/messages?itemId=t.%2B14026303368
Voice
Search Google Voice
Receiving calls
Upgrade
Send new message
(402) 630-3368
(402) 630-3368 1:27 AM
You: Sent an image
(713) 566-0592 1:16 AM
You: HELLO
(308) 760-5756 12:54 AM
You: flwnet.help
(256) 762-0522 Thu
You: CASE ID -TP9045JF7712
(304) 702-5119 Thu
You: HELLO THIS SIDE ALEX MARTIN
(602) 873-2459 Thu
You: CALL ME BACK
(541) 968-0940 Thu
Idk
(812) 498-2154 Thu
You: Sent an image
(623) 698-4681 Thu
You: Sent an image
(336) 762-4814 Wed
You: Sent an image
(402) 630-3368
Call as
(415) 498-0082
Enter a name or number
APPLE
Support
SUPPORT
Alex Martin
ID: A99217511
EXP: 30/07/2035
US_support@apple.com
1:27 AM
Type a message
Hide keypad

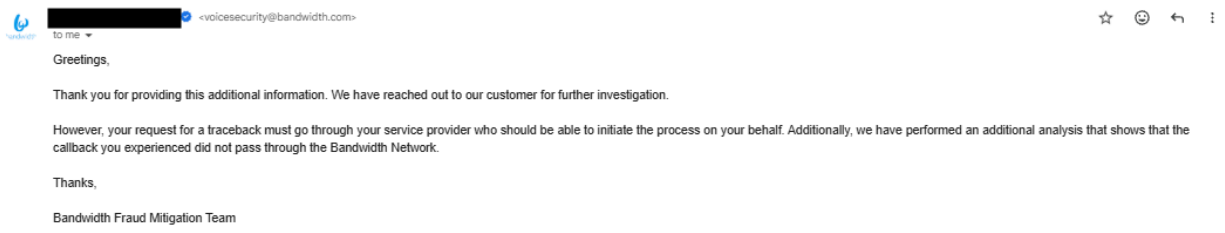

Google Voice - Voice - Messages
Voice
Search Google Voice
Receiving calls
Upgrade
Send new message
Rozer
You: Hi Waiting for your call 2:52 AM
(443) 405-2049 Wed
(352) 895-2034 May 8
You: are you there?
Degree Wellness May 8
(301) 747-1736 May 8
(936) 572-8872 May 1
(305) 781-6639 May 1
(813) 618-7964 May 1
+1 306-681-3304 Apr 7
(315) 404-1058 Mar 16
You: are you there
(856) 460-0464 Mar 8
Rozer
(262) 994-1280
Rozer • 2:33 AM
Hi Waiting for your call
2:52 AM
Type a message
R
Rozer
(262) 994-1280
02:30
Hold
Keypad
Mute
Message
Type here to search
31°C Mostly clear
ENG
02:59
21-05-2026



These screenshots were submitted to Demurrage by an anonymous source and verified prior to inclusion in this report.

A simple IP traceback can confirm that these Google Voice numbers are being accessed by scammers in India. Although Google Voice registration is not available outside of the United States, there is no penalty for establishing a Google Business account in the United States and subsequently transferring the login credentials to someone in another country. Once an account has been created, nothing prevents overseas scammers from accessing it using their own IP addresses, which remain traceable back to India.

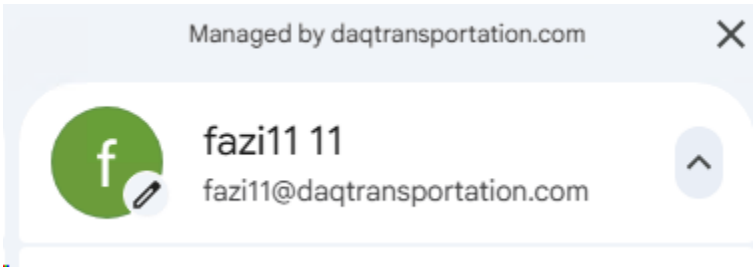
Demurrage brought this to Bandwidth's attention and requested that a traceback be performed, but Bandwidth refused, stating that the call did not traverse its network and that the wholesale provider must handle the report.



This position is unacceptable given that consumers are directed to Bandwidth to report Google Voice numbers in the first place, and it further underscores the need for Google to establish its own dedicated reporting portal to address this ongoing issue.

The Infrastructure Used to Defeat KYC Controls

More sophisticated marks will register shell companies in the United States, build placeholder websites, and use U.S. IP addresses to open Google Voice Business accounts, which require a registered business, before selling the fully verified accounts to scammers overseas. More concerning still, many of these marks are not based in the United States. Google Voice Business marks have been traced back to Pakistan, further illustrating how deeply marks have infiltrated major U.S. VoIP provider networks.



Contact Information

Abuse Contact

Phone
[redacted]

Email
abuse-complaints [at] squarespace [dot] com

Registrant Contact

Name
[redacted]

Organization
daqtransportation.com

Address
[redacted]
Kendall Park, NJ, [redacted]
US

Phone
[redacted]

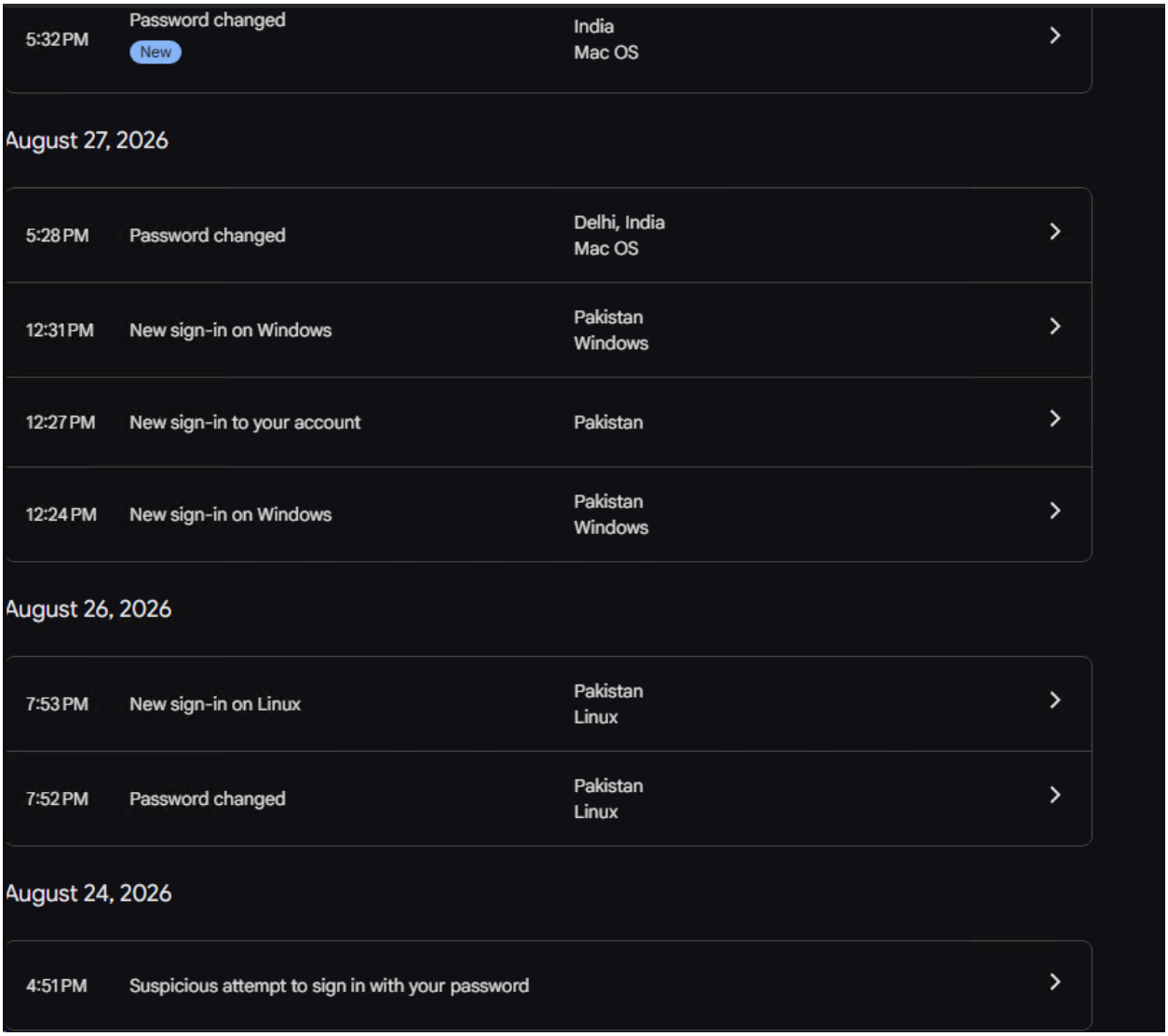
Email
maliknouman1245 [at] gmail [dot] com

Admin Contact

Address
null null

Tech Contact

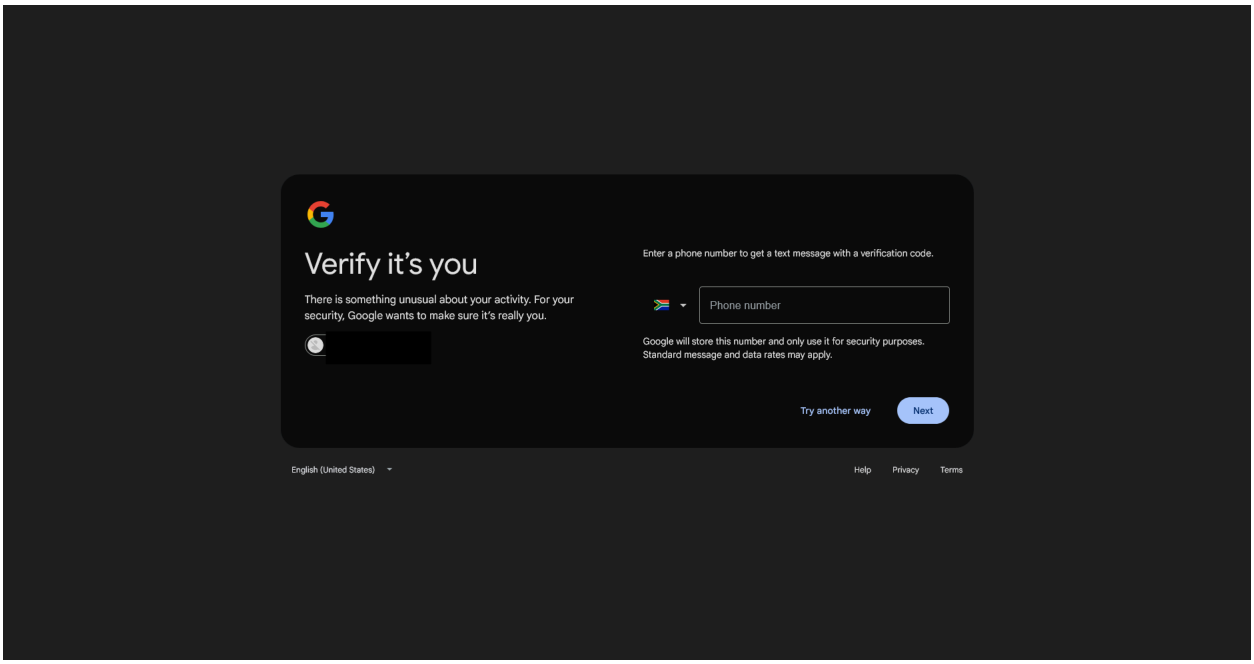
Address
null null

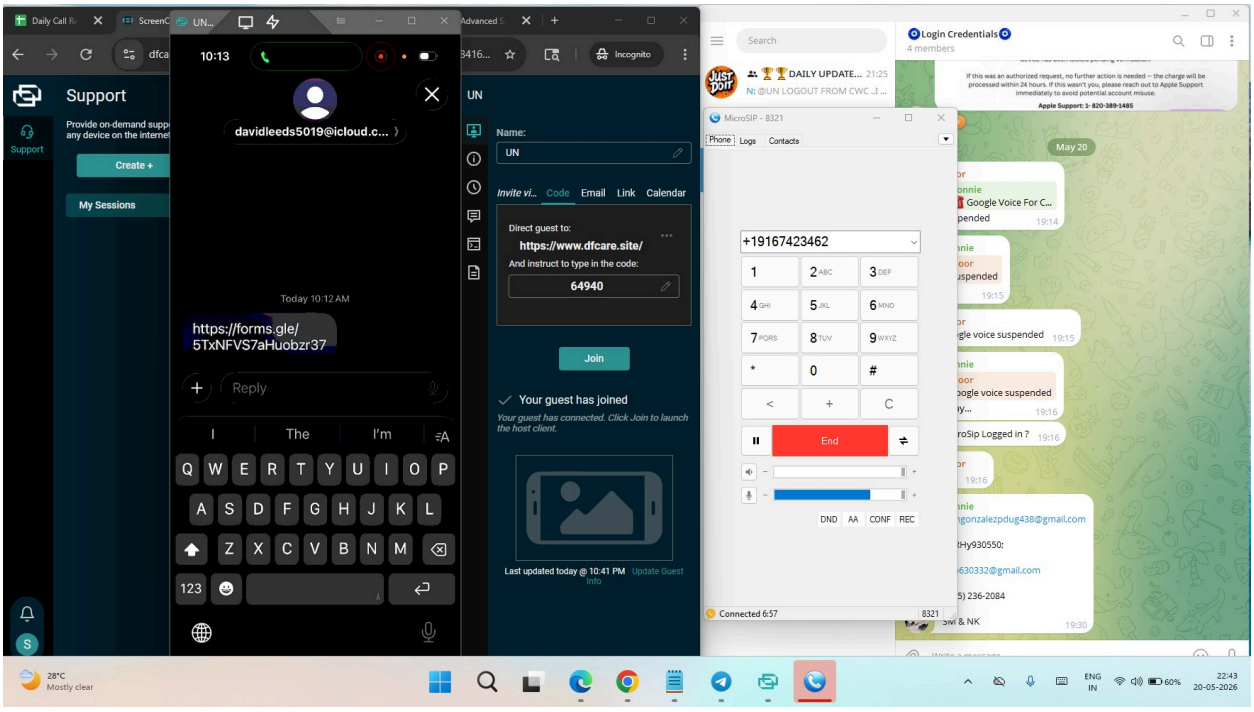


These screenshots were submitted to Demurrage by an anonymous source and verified prior to inclusion in this report.

This is precisely why forwarding fraud reports to wholesale providers and expecting them to act on those reports is fundamentally flawed. Marks are the wholesale providers, and they are knowingly selling accounts and providing assistance to scammers while those accounts are being used to commit fraud. More concerning still, marks have been observed forwarding fraud notifications received from Bandwidth directly to the scammers whose Google Voice numbers have been flagged.

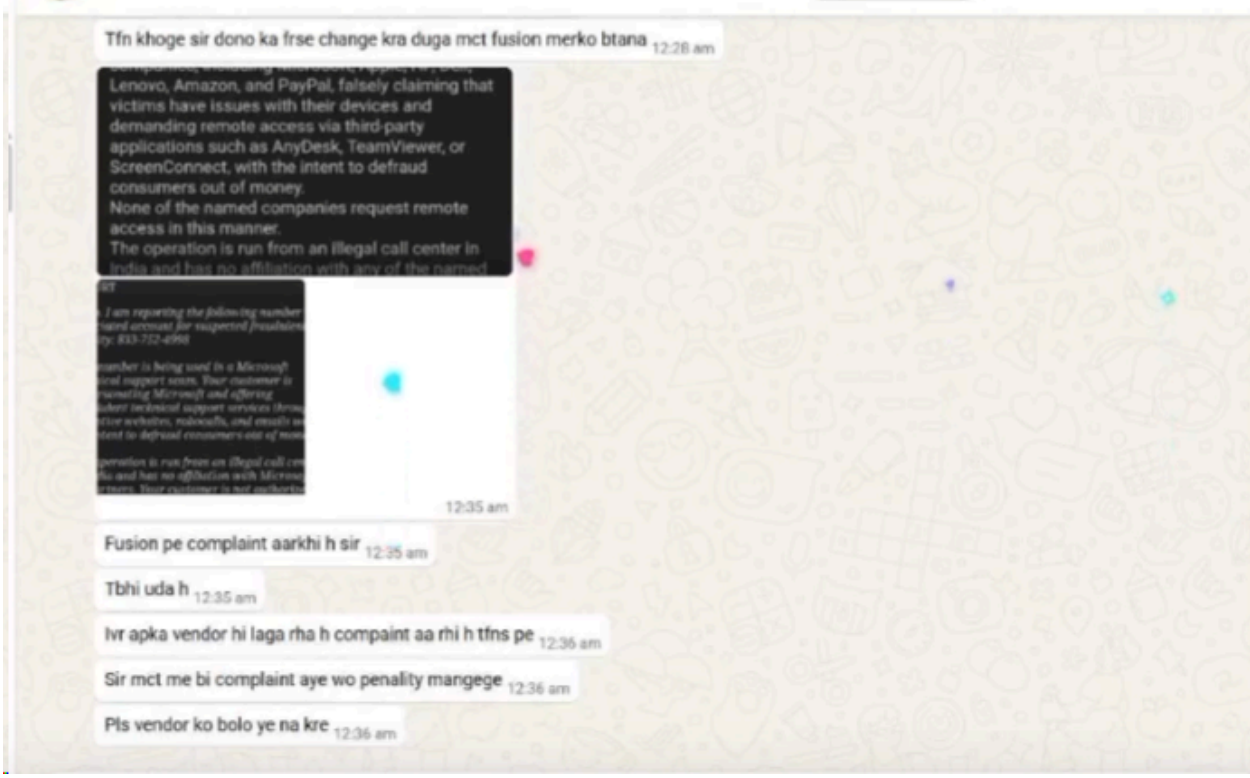
In the screenshot below, a scammer is seen attempting to use Google Voice on their device while communicating with a mark on WhatsApp, stating that the Google Voice number is no longer working.





These screenshots were submitted to Demurrage by an anonymous source and verified prior to inclusion in this report.

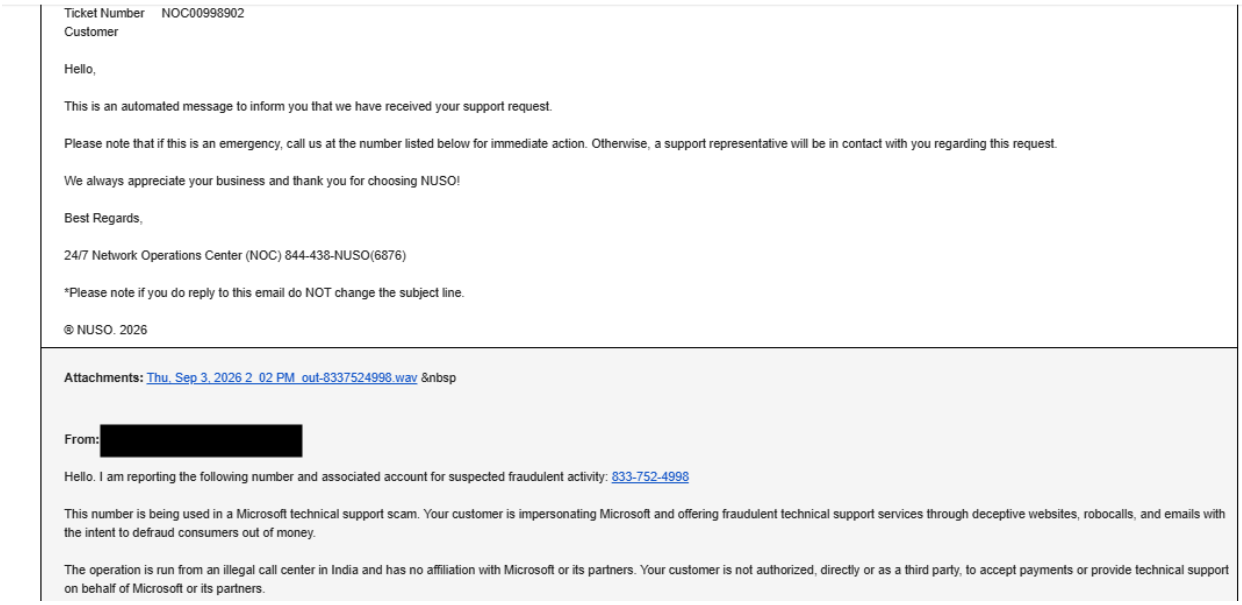
Other VoIP providers, such as Nuso, have adopted the same practice of forwarding complaints to their wholesale providers, who have also proven to be marks based in India. In the screenshot below, submitted to Demurrage by an anonymous source tracking illegal call centers in India, a scammer is seen receiving a message via WhatsApp from a mark at Nuso, notifying them that their number has been reported. This is another instance of a telecom placing complete trust in a wholesale provider that proved to be a mark.



These screenshots were submitted to Demurrage by an anonymous source and verified prior to inclusion in this report.

Upon closer examination, the report in question is the one originally submitted to Nuso by Demurrage. The mark, who was communicating with the scammers in Hindi, did not respond to the report. While Nuso attributed the lack of response to a holiday weekend in the United States, the report was filed on September 3, 2026, and Nuso's support staff responded to the ticket throughout the weekend, apologizing for the wholesale

provider's failure to update the case rather than directly reviewing the evidence and blocking the reported number.



Ticket Number NOC00998902
Customer

Hello,

This is an automated message to inform you that we have received your support request.

Please note that if this is an emergency, call us at the number listed below for immediate action. Otherwise, a support representative will be in contact with you regarding this request.

We always appreciate your business and thank you for choosing NUSO!

Best Regards,

24/7 Network Operations Center (NOC) 844-438-NUSO(6876)

*Please note if you do reply to this email do NOT change the subject line.

® NUSO. 2026

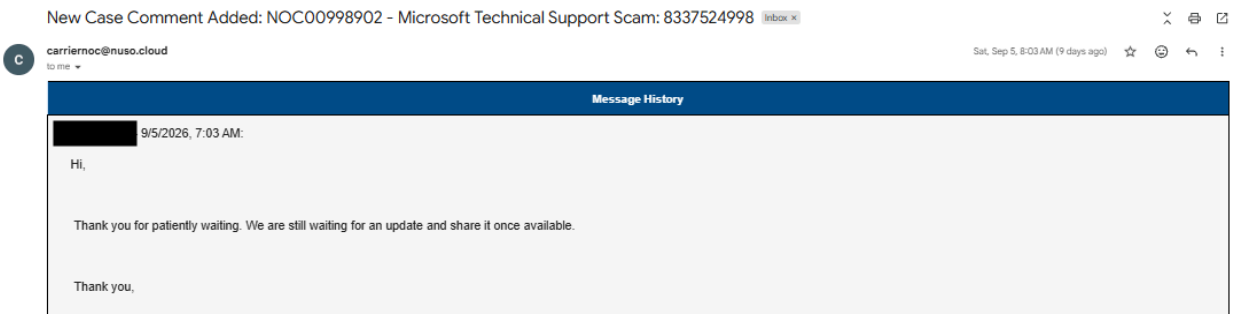
Attachments: Thu, Sep 3, 2026 2_02 PM_out-8337524998.wav

From: [redacted]

Hello. I am reporting the following number and associated account for suspected fraudulent activity: 833-752-4998

This number is being used in a Microsoft technical support scam. Your customer is impersonating Microsoft and offering fraudulent technical support services through deceptive websites, robocalls, and emails with the intent to defraud consumers out of money.

The operation is run from an illegal call center in India and has no affiliation with Microsoft or its partners. Your customer is not authorized, directly or as a third party, to accept payments or provide technical support on behalf of Microsoft or its partners.



New Case Comment Added: NOC00998902 - Microsoft Technical Support Scam: 8337524998 Inbox ×

carriernoc@nuso.cloud
to me

Sat, Sep 5, 8:03 AM (9 days ago)

Message History

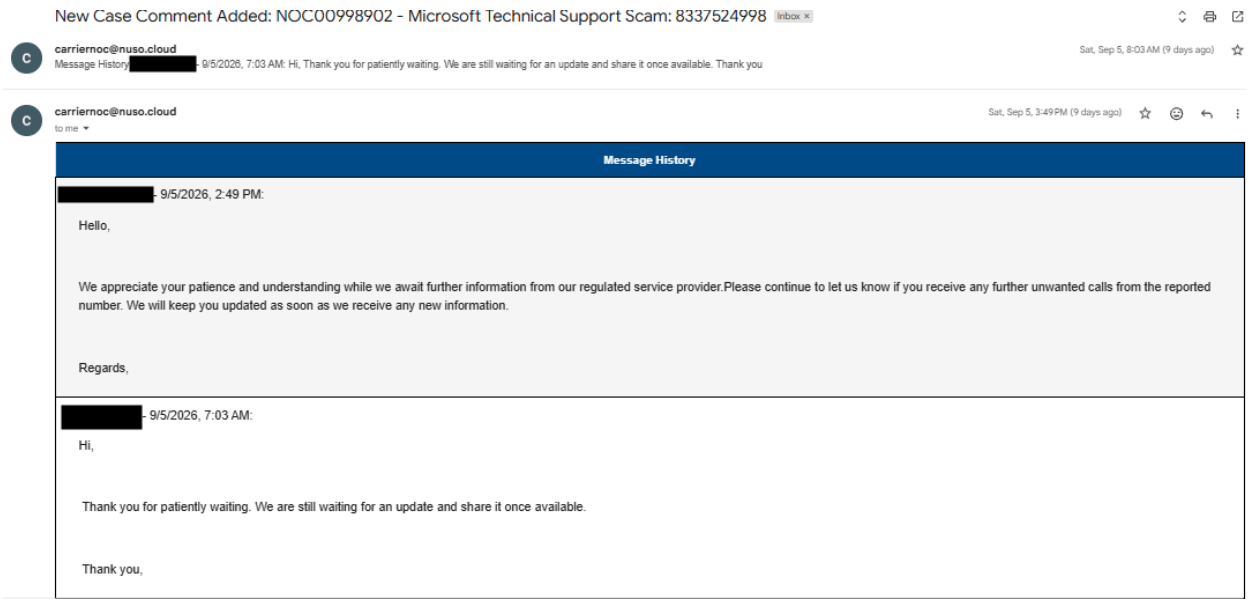
[redacted] 9/5/2026, 7:03 AM:

Hi,

Thank you for patiently waiting. We are still waiting for an update and share it once available.

Thank you,

This occurred across multiple numbers on Nuso, all traced back to the same mark on September 3, 2026, with Nuso offering the same explanation each time for the wholesale provider's failure to respond. As of September 14, 2026, the mark has not responded to the complaint and the outcome of this case remains unresolved.



New Case Comment Added: NOC00998902 - Microsoft Technical Support Scam: 8337524998 Inbox ×

carriernoc@nuso.cloud
Message History [redacted] - 9/5/2026, 7:03 AM: Hi, Thank you for patiently waiting. We are still waiting for an update and share it once available. Thank you
Sat, Sep 5, 8:03 AM (9 days ago)

carriernoc@nuso.cloud
to me
Sat, Sep 5, 3:49 PM (9 days ago)

Message History

[redacted] - 9/5/2026, 2:49 PM:

Hello,

We appreciate your patience and understanding while we await further information from our regulated service provider.Please continue to let us know if you receive any further unwanted calls from the reported number. We will keep you updated as soon as we receive any new information.

Regards,

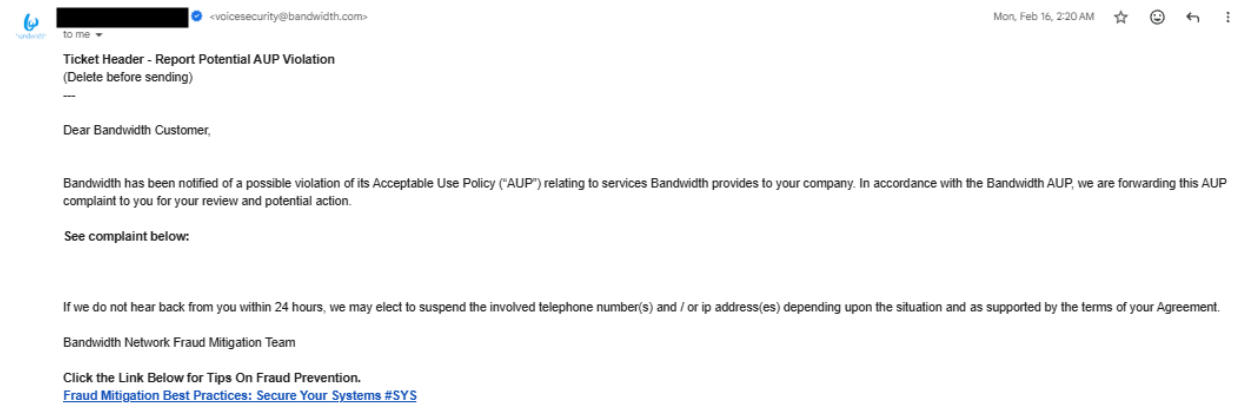
[redacted] - 9/5/2026, 7:03 AM:

Hi,

Thank you for patiently waiting. We are still waiting for an update and share it once available.

Thank you,

Bandwidth's position that calls and numbers must be handled by its wholesale providers appears to be contradicted by its own internal communications. On at least one occasion, Bandwidth appears to have sent Demurrage a message intended for its wholesale providers, in which Bandwidth takes a notably different position regarding its ability to intervene and shut down a number if the wholesale provider does not comply.



[redacted] <voicesecurity@bandwidth.com>
to me
Mon, Feb 16, 2:20 AM

Ticket Header - Report Potential AUP Violation
(Delete before sending)

Dear Bandwidth Customer,

Bandwidth has been notified of a possible violation of its Acceptable Use Policy ("AUP") relating to services Bandwidth provides to your company. In accordance with the Bandwidth AUP, we are forwarding this AUP complaint to you for your review and potential action.

See complaint below:

If we do not hear back from you within 24 hours, we may elect to suspend the involved telephone number(s) and / or ip address(es) depending upon the situation and as supported by the terms of your Agreement.

Bandwidth Network Fraud Mitigation Team

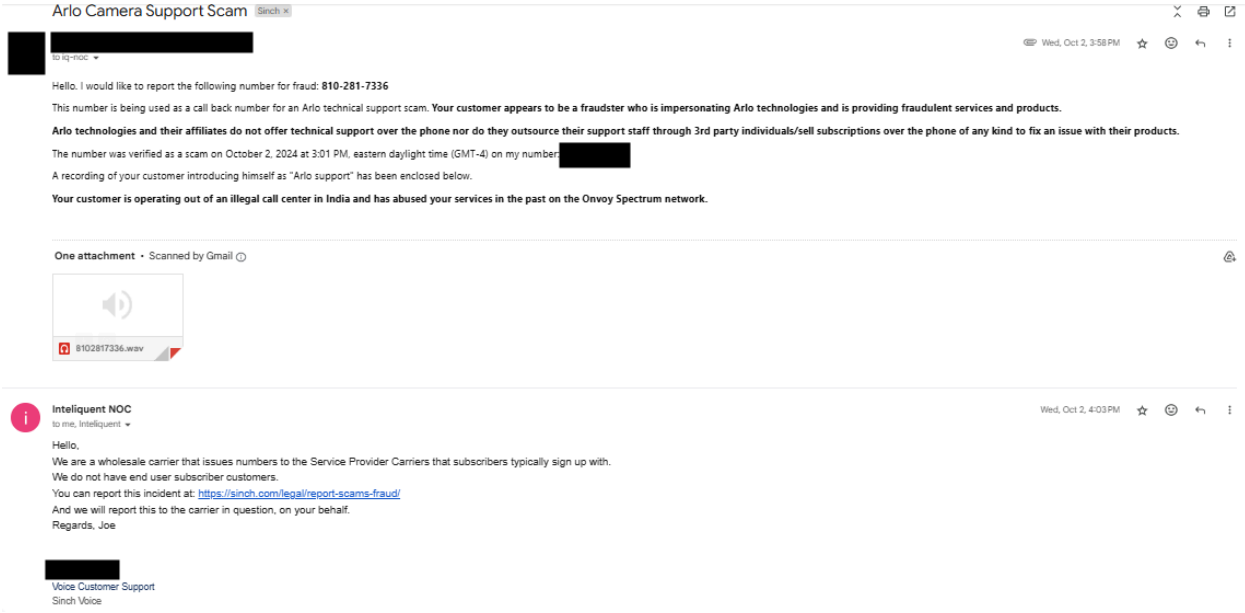
Click the Link Below for Tips On Fraud Prevention.
Fraud Mitigation Best Practices: Secure Your Systems #SYS

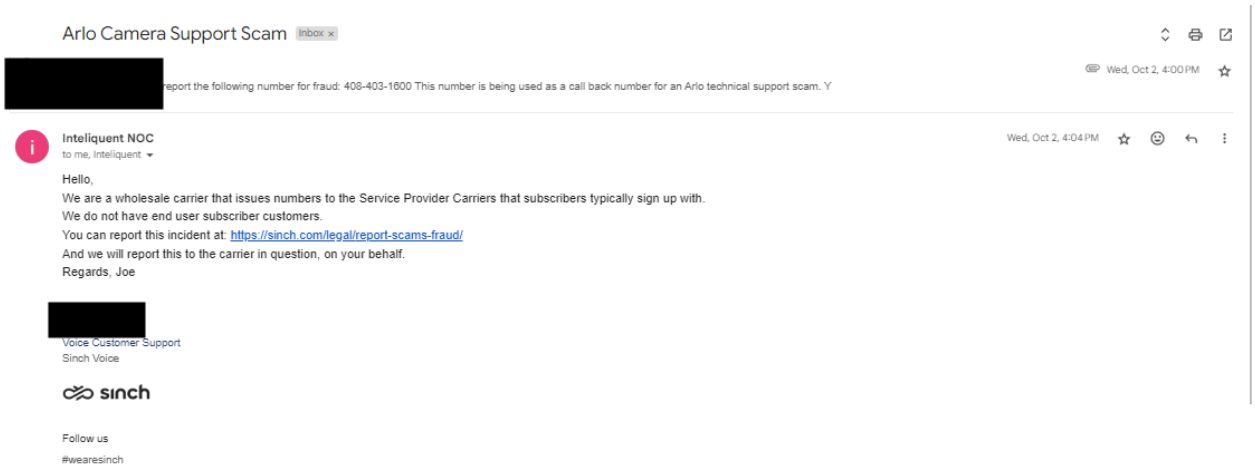
If accurate, this suggests that Bandwidth is capable of taking direct action against a reported number but chooses not to do so.

What Is Not Working: Sinch and Its Refusal to Communicate

While Bandwidth places complete trust in its wholesale providers, Sinch takes an entirely different approach, and arguably a worse one. Although Bandwidth's system is flawed, there is at least some level of communication between the person submitting the report and Bandwidth. With Sinch, that does not exist.

For as long as Demurrage has been active, Sinch has done everything it can to avoid direct communication with consumers. Sinch refuses to engage through email, going as far as to deny addressing fraud reports through its official communication channels. Sinch and Intelliquent will also refuse to address fraud reports submitted to their official email addresses, instead redirecting users to a web form designated for reporting robocalls and stating that action cannot be taken via email. The consumer is therefore required to use the web form so that someone within Sinch or Inteliquent can forward the report internally for action to be taken, a process that is both redundant and counterproductive.





Arlo Camera Support Scam Inbox ×

[redacted] report the following number for fraud: 408-403-1600 This number is being used as a call back number for an Arlo technical support scam. Y

Wed, Oct 2, 4:00 PM

Inteliquent NOC
to me, Inteliquent

Wed, Oct 2, 4:04 PM

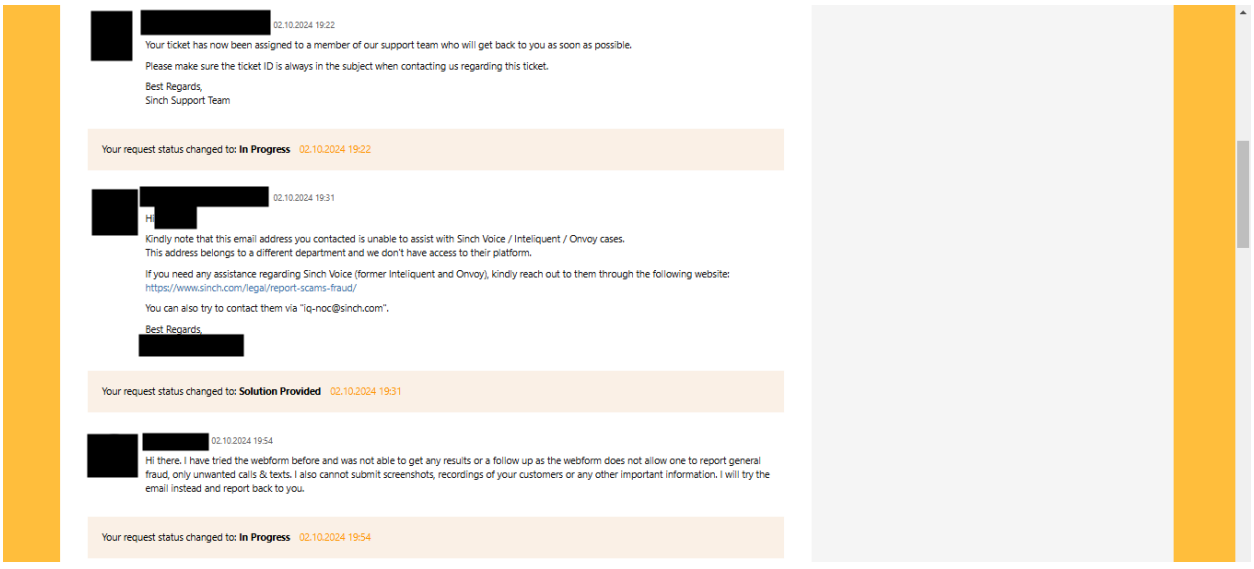
Hello,
We are a wholesale carrier that issues numbers to the Service Provider Carriers that subscribers typically sign up with.
We do not have end user subscriber customers.
You can report this incident at: https://sinch.com/legal/report-scams-fraud/
And we will report this to the carrier in question, on your behalf.
Regards, Joe

[redacted]
Voice Customer Support
Sinch Voice

sinch

Follow us
#wearesinch

Sinch also has a long history of ignoring evidence submitted through other communication channels, often claiming that the submission was made through an incorrect channel rather than forwarding the information to the appropriate department. Reports are routinely closed, dismissed, or met with a redirection to the Sinch web form. In one instance, a Sinch representative provided Demurrage with an Inteliquent email address, only for Intelliquent to respond with the same instruction: use the Sinch web form.



[redacted] 02.10.2024 19:22

Your ticket has now been assigned to a member of our support team who will get back to you as soon as possible.

Please make sure the ticket ID is always in the subject when contacting us regarding this ticket.

Best Regards,
Sinch Support Team

Your request status changed to: **In Progress** 02.10.2024 19:22

[redacted] 02.10.2024 19:31

Hi [redacted]

Kindly note that this email address you contacted is unable to assist with Sinch Voice / Inteliquent / Onvoy cases.
This address belongs to a different department and we don't have access to their platform.

If you need any assistance regarding Sinch Voice (former Inteliquent and Onvoy), kindly reach out to them through the following website:
https://www.sinch.com/legal/report-scams-fraud/

You can also try to contact them via "iq-noc@sinch.com".

Best Regards,
[redacted]

Your request status changed to: **Solution Provided** 02.10.2024 19:31

[redacted] 02.10.2024 19:54

Hi there. I have tried the webform before and was not able to get any results or a follow up as the webform does not allow one to report general fraud, only unwanted calls & texts. I also cannot submit screenshots, recordings of your customers or any other important information. I will try the email instead and report back to you.

Your request status changed to: **In Progress** 02.10.2024 19:54

Your request status changed to: **In Progress** 02.10.2024 19:54

Your request status changed to: **Solution Provided** 02.10.2024 19:59

[redacted] 02.10.2024 20:10

Well, as I expected, neither Intelliquent or Sinch wants to deal with fraud through email. Every email I have contacted, I am told to use the webform but it does absolutely nothing. I have tried the form, many times. The numbers are never investigated. I am never contacted. I cannot send recording or screenshots on it and most importantly and quite frankly, it's ridiculous, the form doesn't accept general fraud reports. I have reported numbers that are used by scammers in India on that webform and none of the numbers were taken down - not one. I will continue to email Sinch until I get someone to respond to these reports. Unless you change your webform to include general fraud reports instead of unwanted calls, I will continue to email this address. All of you wholesalers refuse to shut down the scam traffic on your network no matter how many times I use the webform.



Your request status changed to: **In Progress** 02.10.2024 20:10

[redacted] 02.10.2024 20:23

Hi [redacted]

Sorry to hear that, but thank you for the feedback.

I will check internally if I can find another solution for this.

Best Regards,

[redacted]

Your request status changed to: **Escalated internal** 07.10.2024 12:34

Your request status changed to: **In Progress** 11.10.2024 12:34

Your request status changed to: **Waiting for response** 11.10.2024 16:57

Your request status changed to: **In Progress** 13.10.2024 12:43

Your request status changed to: **Waiting for response** 13.10.2024 12:43

Your request status changed to: **In Progress** 17.10.2024 12:43

[redacted] 17.10.2024 23:27

Hello -

Sinch Voice is in receipt of your email below. Please note that support@sinch.com is not the correct contact for such inquiries or submissions. We are unable to assist you in this matter and we will close this ticket.

All complaints concerning North American scam/fraud calls involving a telephone number associated with Sinch **MUST** be reported via the form on our website at this link:

https://www.sinch.com/legal/report-scams-fraud/

PLEASE NOTE that Sinch and its subsidiaries primarily provide wholesale telecommunications services to other telecommunications service providers and carriers. As a wholesale provider, Sinch generally does not provide service to or have information on file regarding end user subscribers of telephone numbers. We do not make calls to consumers, and we are prohibited by law from knowing the identity of our customer's end users. All reports submitted via this form must be forwarded to our wholesale customer (typically the end user's service provider) for investigation and resolution.

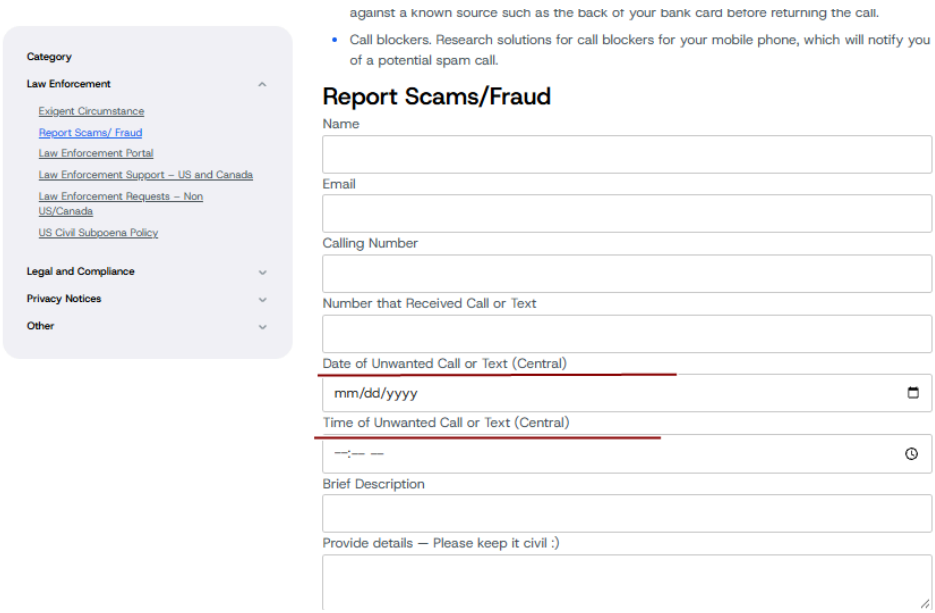
Regards,

Problems with Sinch’s webform

Although Demurrage has published reports on Sinch's track record in the past, including the significant issues with Sinch's preferred reporting method, the Sinch web form, these issues are worth revisiting.

The Sinch web form is outdated. There is no option to attach a screenshot, recording, or any other form of supporting evidence. Like Bandwidth, Sinch will forward the report to its wholesale provider, effectively without any evidence beyond the reported number and the category of scam.

Additionally, the time zone field defaults to Central Time and cannot be changed by the user. This means that if the wholesale provider investigates, the call times will not match the submitted report, and without any supporting evidence, the investigation is likely to be dropped, rendering the web form useless.



Demurrage has found workarounds for these limitations, but if Sinch is serious about addressing fraud on its network, its web form requires significant updates. No web form should default to a fixed time zone. No webform in 2026 should exclude the ability to submit supporting evidence, and no major U.S. telecom should avoid direct

communication the way Sinch does. Email submissions should be accepted regardless of what method is designated as the primary reporting channel, particularly when that channel is outdated and incapable of receiving evidence by default.

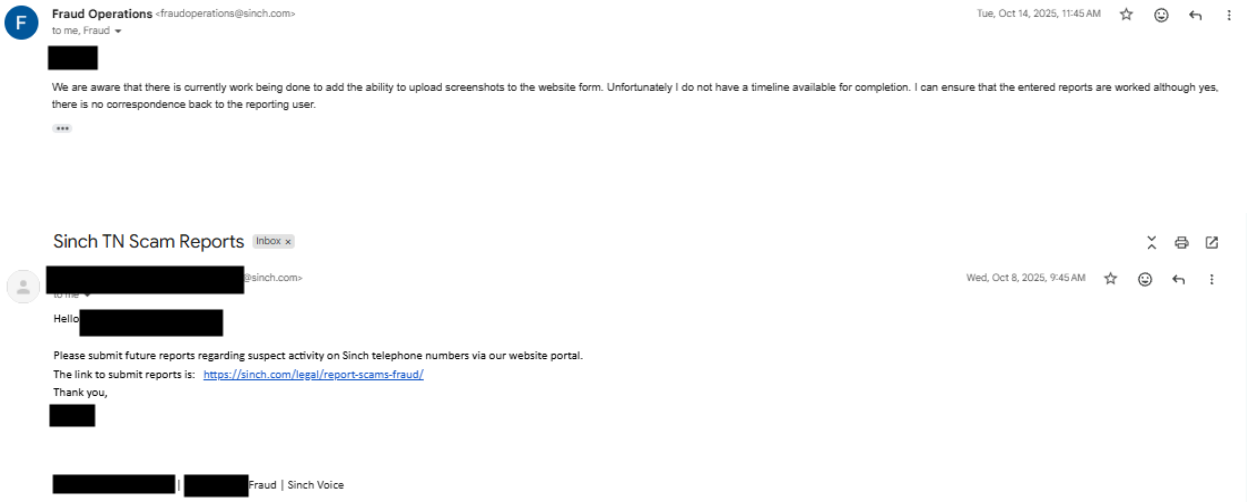
Demurrage has resorted to including evidence by using Google Drive links embedded in the web form's text field, along with manually correcting the time zone for all reported calls.

That a person must go through these lengths simply to submit a fraud report to a major U.S. telecom is unacceptable.

Case Description:	Your customers are sending mass emails with bogus invoices, falsely claiming unauthorized charges on recipients' accounts. They appear to be impersonating Apple from an unlicensed overseas call center in India with no connection to Apple or its affiliates. . Time of the call was Mon, Nov 24, 2025 11:56 AM, eastern daylight time (GMT-4) which is 10:56 AM central time. - Enclosed screenshot of the scam text invoice used by your customer to advertise the reported toll-free number along with a recording of your customer answering the phone, claiming to be "customer support" via Google Drive links. . Screenshot; https://drive.google.com/file/d/1C8Rjun9yb82n-yElHVSB5fWmZR__KOgi/view?usp=sharing . Recording; https://drive.google.com/file/d/1TBMnMOO3SfTSjepV50B2_0aX6Q68SzWt/view?usp=sharing Please investigate and take appropriate action to stop this scam. Thank you.

Regards,
Sinch Voice (Inteliquent)

Sinch has also demonstrated that it is capable of reviewing emails containing evidence, as proven by a direct exchange with a Sinch representative in December 2025, during which Demurrage was in communication regarding a large volume of Microsoft Teams numbers used in refund scams. Although an initial commitment was made to engage with the reports, this was quickly overridden by a more senior Sinch representative, who intervened and redirected Demurrage to the Sinch web form for all further cases. Demurrage responded by noting that the web form provides no outcome or response, but this went unanswered.



When Demurrage subsequently attempted to continue the conversation with the original representative, it was again directed to use the web form. When the issues with the web form were raised, the representative acknowledged that no consumer would ever receive a response or update on any case submitted through it. This means that whether Sinch or the wholesale provider takes action, the person who submitted the complaint is never notified, which fundamentally undermines Sinch's claims that it takes fraud seriously. If action is being taken against scammers, Sinch should communicate the outcome to the consumer. This level of transparency should be mandatory across all major telecoms in the United States.

Marks operating on the Sinch network are effectively shielded by this consistent lack of communication, as it remains unclear whether reports are being forwarded to marks directly or to another provider within Sinch's infrastructure. What is clear, however, is that because all reported numbers and calls traverse Sinch's infrastructure, it is Sinch,

not the marks or their wholesale providers, that bears responsibility. Given Sinch's long history of scammer abuse on its network, this will remain an unresolved problem until significant changes are made.

Marks and scammers are aware that acquiring a number on the Sinch network significantly reduces the risk of that number being acted upon when reported for fraud, a pattern Demurrage has observed repeatedly in the field, with specific cases presented later in this report.

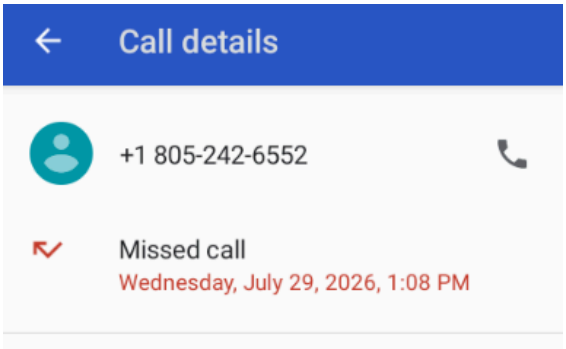
Statistics: Bandwidth

- As of September 2026, a total of 2,176 numbers traced back to Bandwidth were reported for use in tech support fraud, Publishers Clearing House impersonation fraud, various refund scams impersonating Amazon, PayPal, Microsoft, and other entities, and scammer callback numbers, across the following wholesale providers operating on Bandwidth's infrastructure: **Google Voice, Google Ads Connect, RingCentral, Skype, DialPad, J2 Web Services, Teleconnx, Anveo Inc., CallCurrent Inc. (MightyCall), Bulk Solutions, Amazon Connect, GoDaddy.com, Imperial Technologies Inc., NumberBarn LLC, Telzio Inc.,** and **Zoom.**
- Several Bandwidth numbers also traced back to RingCentral and Sinch where SMS was enabled on those accounts. None of the reported numbers were spoofed. Demurrage verifies all numbers prior to submission by calling them directly, and a scammer answered in every case. In all cases, the scammer operation was traced back to India, with the exception of the Publishers Clearing House scams, which were traced back to Jamaica.
- Bandwidth's takedown rate is entirely dependent on its wholesale providers' willingness to act on reports. In the case of Google Voice, the takedown rate is exceptionally low given that the vast majority of these accounts are created and controlled by marks.
- Bandwidth took no disciplinary action against marks for their failure to handle reports in a timely manner, including cases in which marks on Google Voice made false claims about having taken action against scammers, despite evidence submitted by Demurrage over the course of several days.

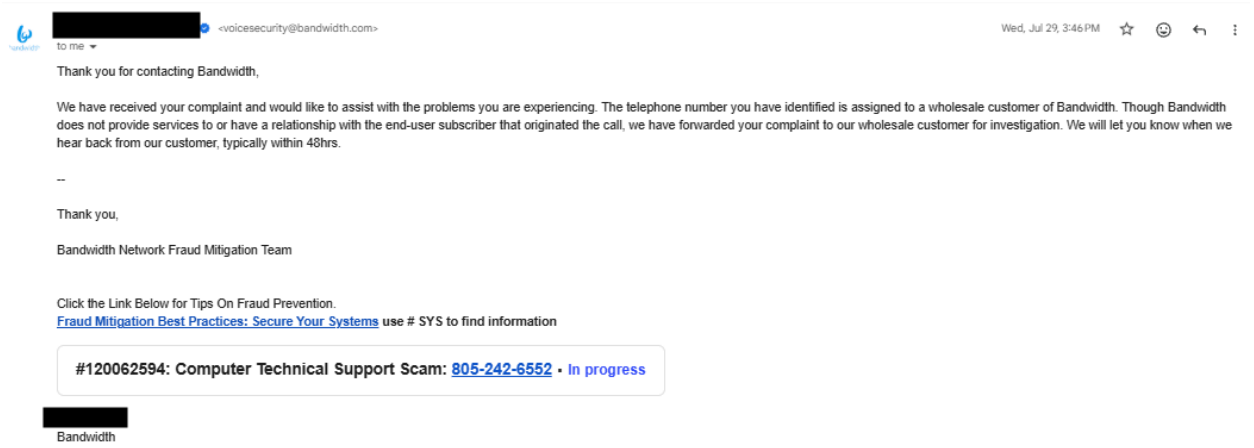
Notable Cases

Case 1: 805-242-6552

This number was used as a callback number for both a GEICO customer support scam and a computer technical support scam. The number was traced back to Google Voice, and after verifying that it was being used as a callback number by a scammer, a report was submitted to Bandwidth on July 29, 2026, at 2:28 PM EST. As Google does not maintain a dedicated contact channel, web form, or email address for resolving issues with Google Voice numbers, Bandwidth must be contacted for all cases involving Google Voice.



On July 29, 2026, at 3:46 PM EST, Bandwidth responded, confirming that the report had been forwarded to the wholesale provider in question and that 48 hours should be allowed for a response. Demurrage considers this window excessive, particularly given that competing telecoms typically respond within minutes or on the same day a report is submitted. Demurrage waited for the outcome of the case.



[redacted] <voicesecurity@bandwidth.com> Wed, Jul 29, 3:46 PM

to me

Thank you for contacting Bandwidth,

We have received your complaint and would like to assist with the problems you are experiencing. The telephone number you have identified is assigned to a wholesale customer of Bandwidth. Though Bandwidth does not provide services to or have a relationship with the end-user subscriber that originated the call, we have forwarded your complaint to our wholesale customer for investigation. We will let you know when we hear back from our customer, typically within 48hrs.

--

Thank you,

Bandwidth Network Fraud Mitigation Team

Click the Link Below for Tips On Fraud Prevention.
Fraud Mitigation Best Practices: Secure Your Systems use # SYS to find information

#120062594: Computer Technical Support Scam: 805-242-6552 • In progress

[redacted]
Bandwidth

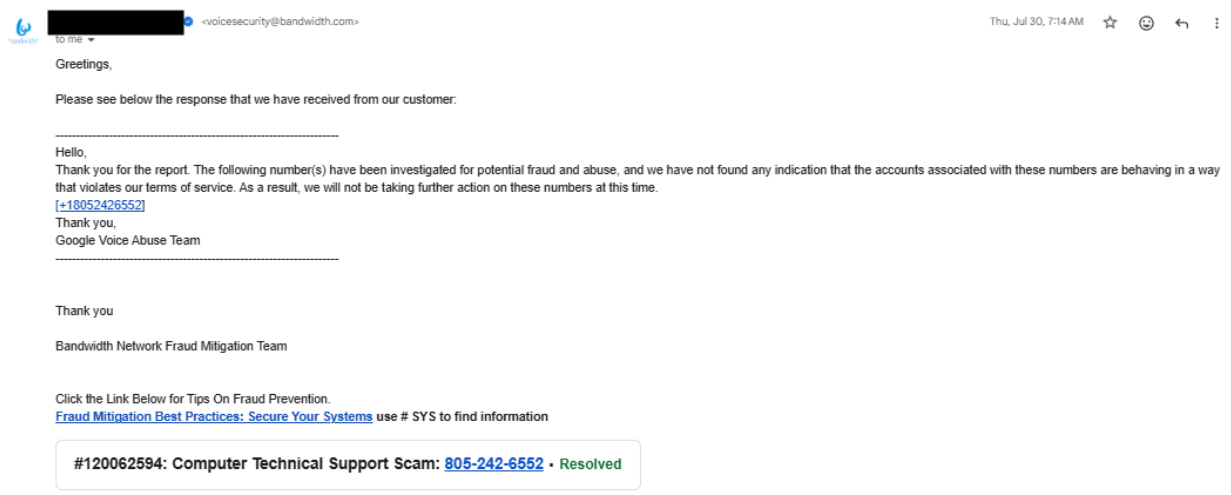
On July 30, 2026 at 7:14 AM, which is the mark responded to the report with the following;

Hello,

Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have not found any indication that the accounts associated with these numbers are behaving in a way that violates our terms of service. As a result, we will not be taking further action on these numbers at this time.

[+18052426552]

Thank you,
Google Voice Abuse Team



[redacted] <voicesecurity@bandwidth.com> Thu, Jul 30, 7:14 AM

to me

Greetings,

Please see below the response that we have received from our customer:

Hello,
Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have not found any indication that the accounts associated with these numbers are behaving in a way that violates our terms of service. As a result, we will not be taking further action on these numbers at this time.
[+18052426552]
Thank you,
Google Voice Abuse Team

Thank you

Bandwidth Network Fraud Mitigation Team

Click the Link Below for Tips On Fraud Prevention.
Fraud Mitigation Best Practices: Secure Your Systems use # SYS to find information

#120062594: Computer Technical Support Scam: 805-242-6552 · Resolved

This proved to be a lie.

On August 3, 2026, at 2:04 PM EST, the number remained active, as the scammer proceeded to call one of Demurrage's dedicated cell phones using the same Google Voice number, even leaving a voicemail, claiming to be “GEICO support” and requesting a callback on the reported number.

Mon, Aug 3, 2026 2_04 PM_8052426552

Demurrage updated the ticket on August 3, 2026, at 2:42 PM EST, four days after the mark claimed that no evidence of fraud had been found on the reported number. The update included screenshots of the scammer calling the dedicated cell phone from the reported Google Voice number, along with the voicemail left by the scammer. Demurrage also requested that a traceback be performed to confirm that the number was being accessed from India rather than the United States, which would easily prove that the KYC information submitted to create the account had been falsified.

[redacted]

Aug 3, 2026, 2:03 PM

Once again, after 5 days, your wholesaler at Google Voice is lying. Your customer is still calling me back, and now is claiming to be "Geico insurance" . I have enclosed a screenshot of the recent call history.

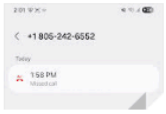
I still don't understand why no one at Bandwidth isn't checking the claims of these complicit Google Voice wholesalers or in general.

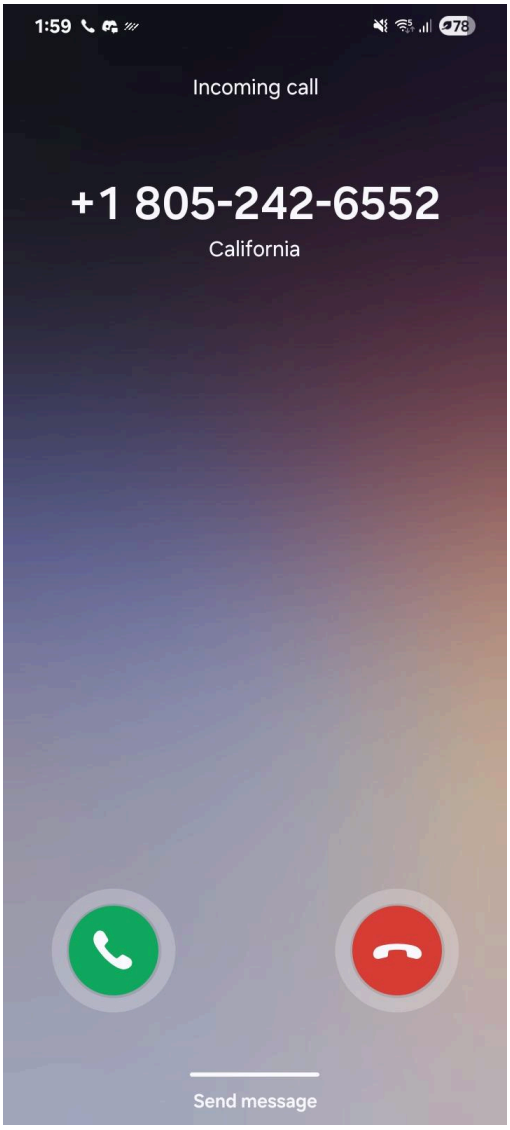
Time of the call: Wed, Aug 3, 2026 1:58 PM, eastern daylight time (GMT-4) on my number; 646-489-3093

•••

2 Attachments • Scanned by Gmail ⓘ Add all to Drive

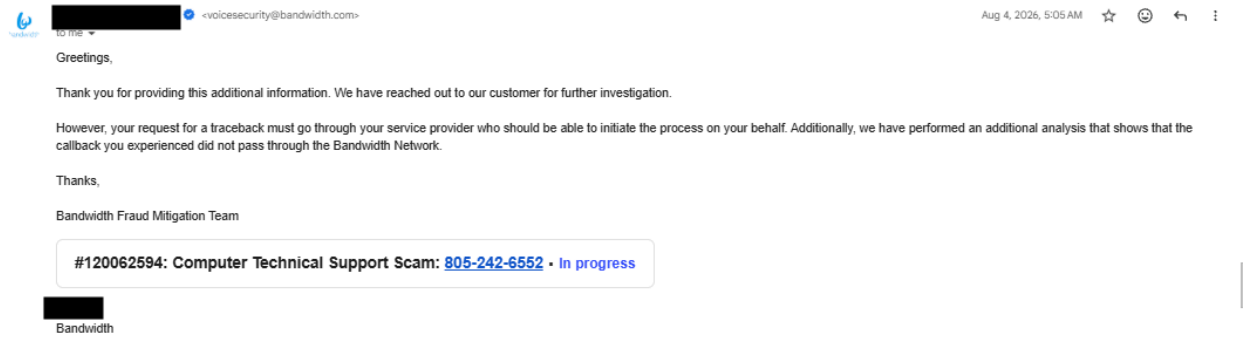






Once again, Bandwidth declined to intervene directly and instead forwarded the updated evidence to the mark, expecting the mark to take action against the scammer. Bandwidth also claimed that a traceback could only be performed through Demurrage's service provider, and that additional analysis had concluded that the call did not traverse its network.

This raises the question once again as to why consumers are directed to Bandwidth to report Google Voice numbers for fraud if Bandwidth maintains that such calls do not traverse its network.


[redacted] <voicesecurity@bandwidth.com> Aug 4, 2026, 5:05 AM

to me

Greetings,

Thank you for providing this additional information. We have reached out to our customer for further investigation.

However, your request for a traceback must go through your service provider who should be able to initiate the process on your behalf. Additionally, we have performed an additional analysis that shows that the callback you experienced did not pass through the Bandwidth Network.

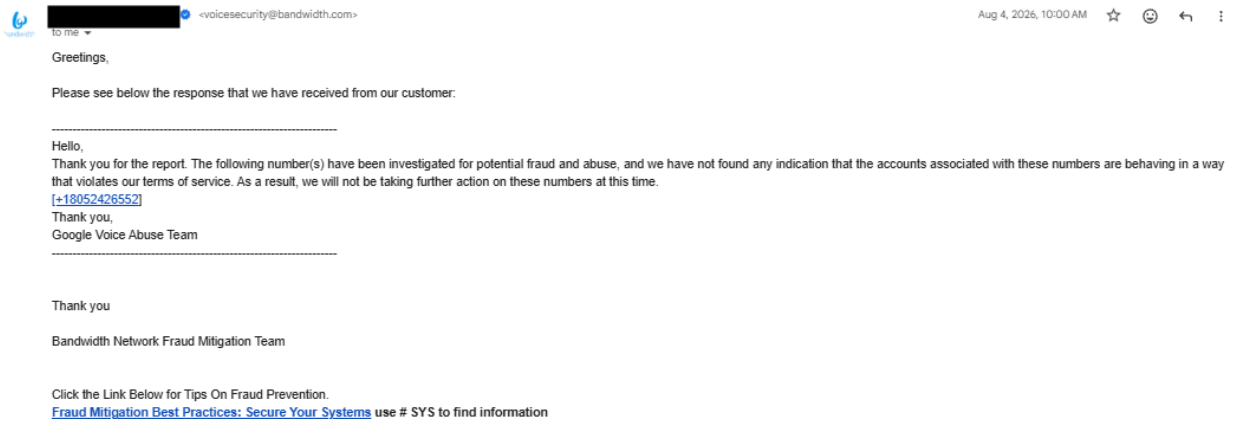
Thanks,

Bandwidth Fraud Mitigation Team

#120062594: Computer Technical Support Scam: 805-242-6552 · In progress

[redacted]
Bandwidth

On August 4, 2026, at 10:00 AM EST, the mark responded again with the same text from July 30, 2026, claiming that no evidence of fraud had been found, despite the updated evidence submitted by Demurrage, including a recording of the scammer identifying as “GEICO support.” This marked the second instance of the mark disregarding the submitted evidence and lying on behalf of the scammers.


[redacted] <voicesecurity@bandwidth.com> Aug 4, 2026, 10:00 AM

to me

Greetings,

Please see below the response that we have received from our customer:

Hello,
Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have not found any indication that the accounts associated with these numbers are behaving in a way that violates our terms of service. As a result, we will not be taking further action on these numbers at this time.
[+18052426552]
Thank you,
Google Voice Abuse Team

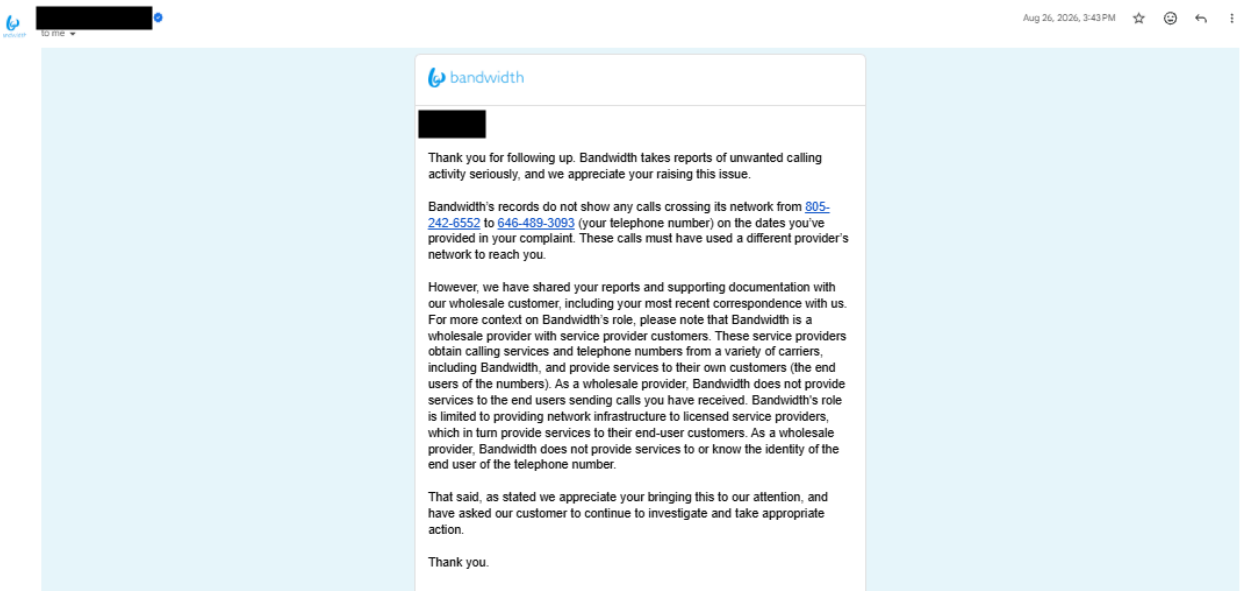
Thank you

Bandwidth Network Fraud Mitigation Team

Click the Link Below for Tips On Fraud Prevention.
Fraud Mitigation Best Practices: Secure Your Systems **use # SYS to find information**

Bandwidth also refused to hold the mark accountable and closed the case for the second time without reviewing the evidence or the claims made by the mark, choosing instead to rely on the mark's assessment. On August 4, 2026, the scammer once again called one of Demurrage's dedicated cell phones from the same Google Voice number. The ticket was reopened and Demurrage informed Bandwidth that the mark had been dishonest.

The ticket remained closed, and neither the mark nor Bandwidth responded to Demurrage's final message until August 26, 2026, at 3:43 PM EST, 22 days later, during which time the number remained active. Bandwidth responded with the following:



[redacted] to me

Aug 26, 2026, 3:43 PM

bandwidth

[redacted]

Thank you for following up. Bandwidth takes reports of unwanted calling activity seriously, and we appreciate your raising this issue.

Bandwidth's records do not show any calls crossing its network from 805-242-6552 to 646-489-3093 (your telephone number) on the dates you've provided in your complaint. These calls must have used a different provider's network to reach you.

However, we have shared your reports and supporting documentation with our wholesale customer, including your most recent correspondence with us. For more context on Bandwidth's role, please note that Bandwidth is a wholesale provider with service provider customers. These service providers obtain calling services and telephone numbers from a variety of carriers, including Bandwidth, and provide services to their own customers (the end users of the numbers). As a wholesale provider, Bandwidth does not provide services to the end users sending calls you have received. Bandwidth's role is limited to providing network infrastructure to licensed service providers, which in turn provide services to their end-user customers. As a wholesale provider, Bandwidth does not provide services to or know the identity of the end user of the telephone number.

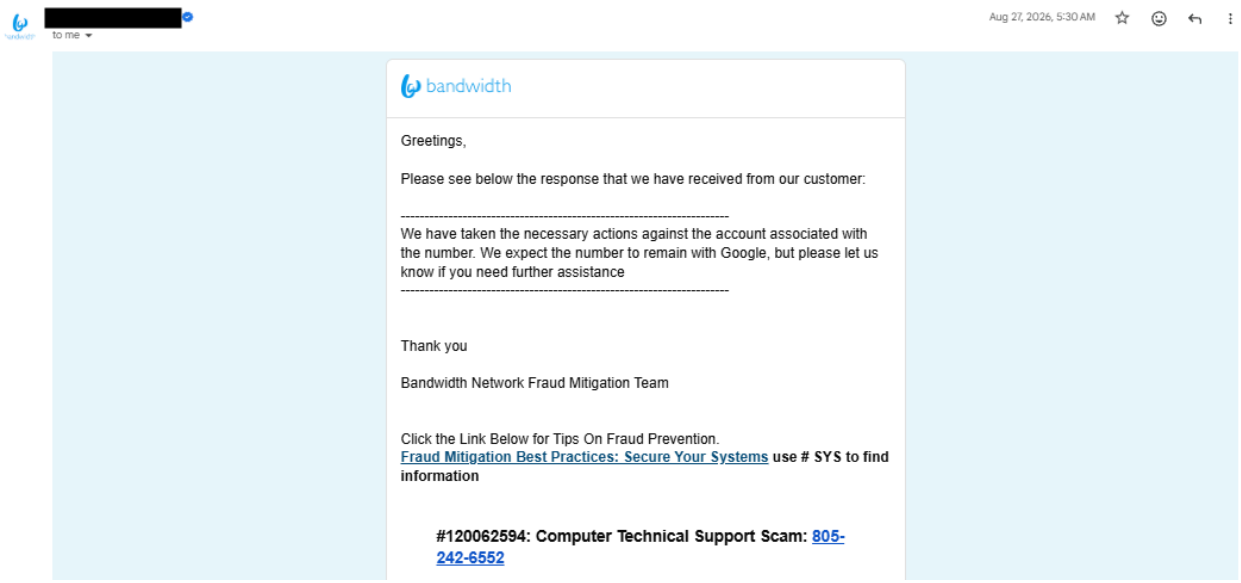
That said, as stated we appreciate your bringing this to our attention, and have asked our customer to continue to investigate and take appropriate action.

Thank you.

Once again, Bandwidth asserted that it is a wholesale provider with service customers, that the calls did not traverse its network, and that as a wholesale provider, Bandwidth does not provide services to or know the identity of the end user associated with the reported number. This appears to contradict two earlier responses presented in this report in which Bandwidth stated that if complaints are not addressed, it may be forced to disconnect the number.

On August 27, 2026, at 5:30 AM EST, Demurrage received a response from the customer of record stating that the number had been shut down for fraud. However, it is

unclear whether this response was sent by the mark or by another party within the Bandwidth network.

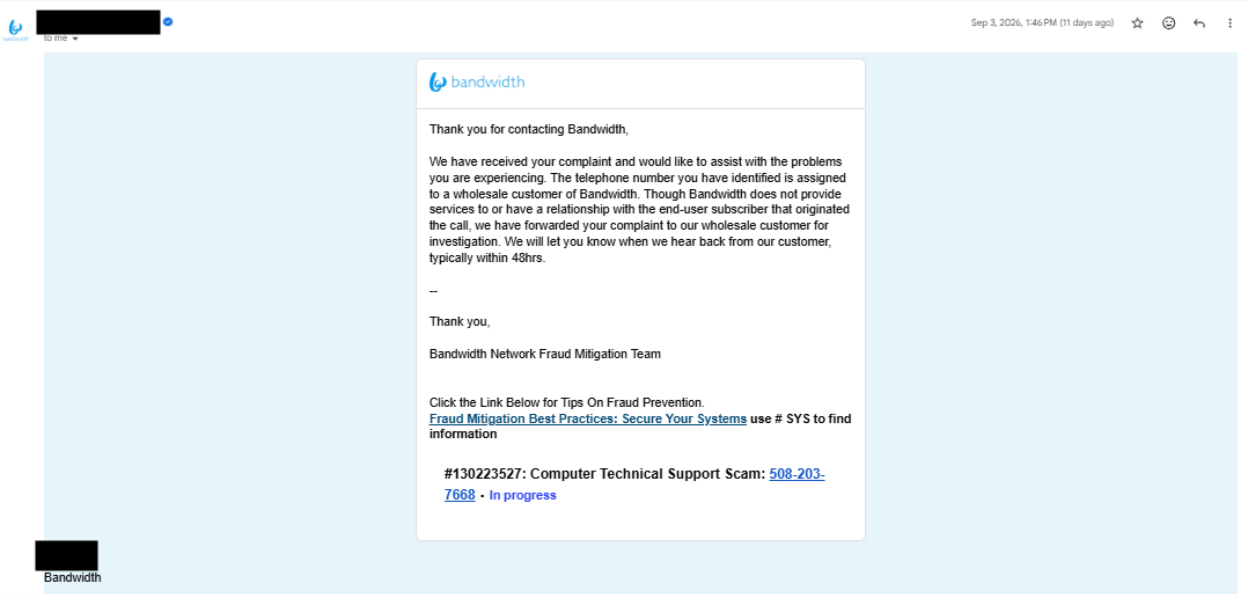


The total time for this case was 22 days.

Case 2: 508-203-7668

This number was used as a callback number for a computer technical support scam. The number was traced back to Google Voice, and after verifying that it was being used as a callback number by a scammer, a report was submitted to Bandwidth on September 3, 2026, at 1:16 PM EST.

On September 3, 2026, at 1:46 PM EST, Bandwidth responded, confirming that the report had been forwarded to the wholesale provider in question and that 48 hours should be allowed for a response.



On September 4, 2026, at 11:18 AM EST, Demurrage received the following response:

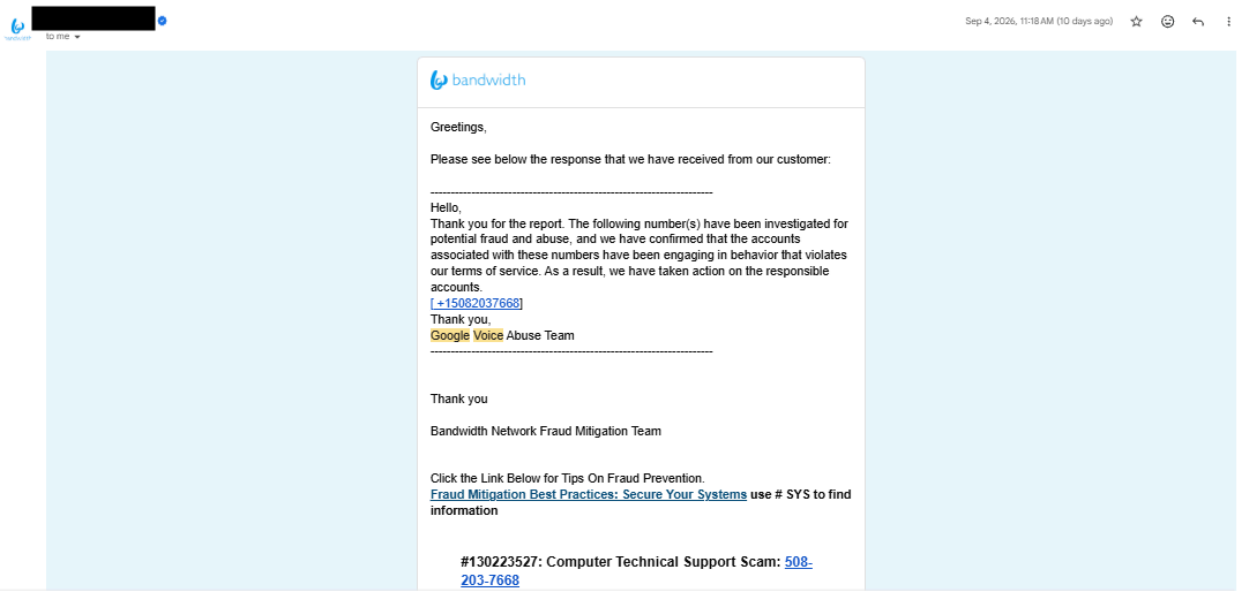
Hello,

Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have confirmed that the accounts associated with these numbers have been engaging in behavior that violates our terms of service. As a result, we have taken action on the responsible accounts.

[+15082037668]

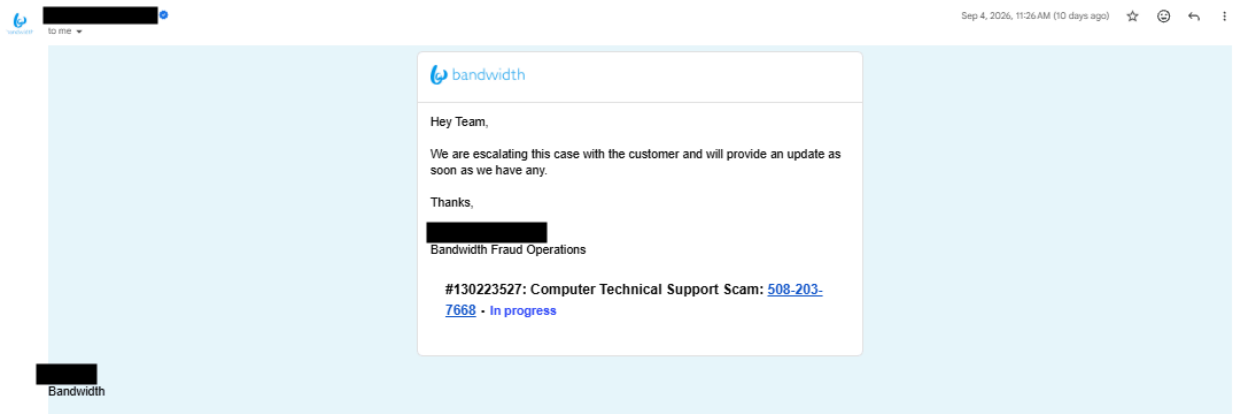
Thank you,

Google Voice Abuse Team

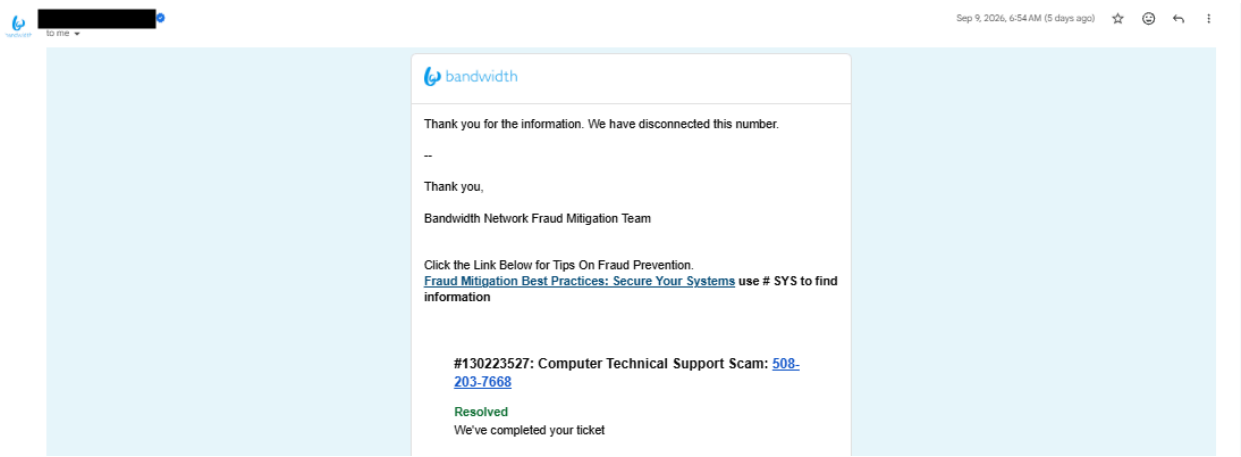


The wholesale provider, who proved to be a mark, had again lied about the outcome of this case, as the number remained active and was now routing calls to voicemail. Demurrage updated the ticket accordingly, noting the mark's dishonesty, and requested that Bandwidth reopen the case.

On September 4, 2026, at 11:26 AM EST, Bandwidth responded with the following:



No further updates were provided by Bandwidth or the mark until September 9, 2026, at 6:54 AM EST, when a response was received confirming that the number had been shut down. Bandwidth took no action to hold the mark accountable for its earlier false claim that the number had already been shut down for fraud.



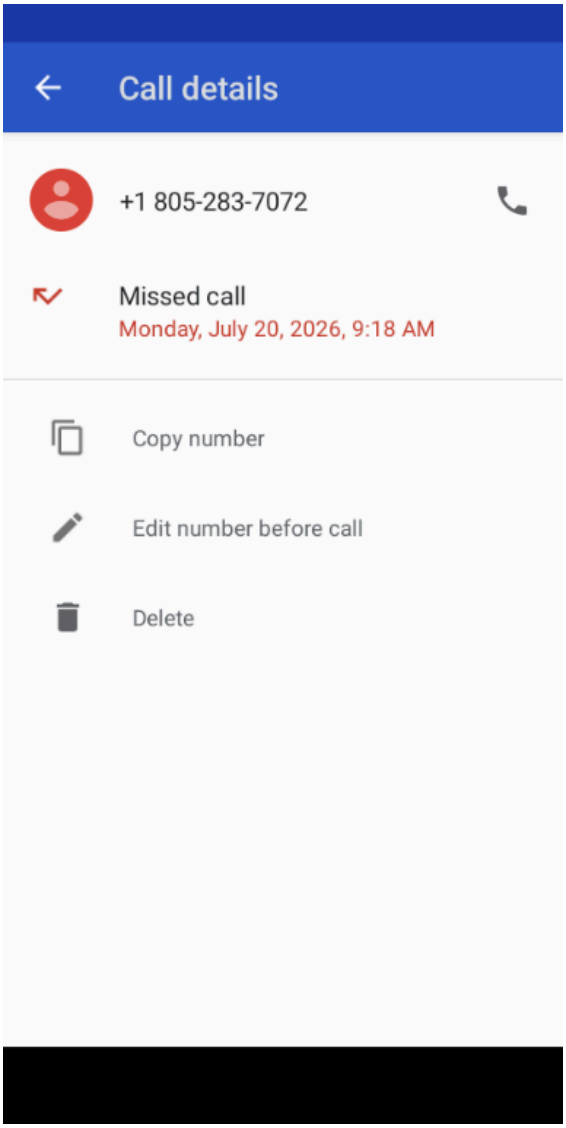
The total time for this case was 6 days.

Case 3: 805-283-7072

This number was used as a callback number for a Microsoft technical support scam. The scammer called one of Demurrage's dedicated cell phones on July 20, 2026, at 9:18 AM EST.

The number was traced back to Google Voice, and after verifying that it was being used as a callback number by a scammer, a report was submitted to Bandwidth the same day.

On July 22, 2026, at 12:36 PM, 2 days later, Bandwidth responded, confirming that the report had been forwarded to the wholesale provider in question and that 48 hours should be allowed for a response.



Microsoft Technical Support Scam: 805-283-7072 Inbox × Google Voice ×

[redacted]
Hello. I am reporting the following number and associated Google Voice account for suspected fraudulent activity: 805-283-7072 This number is being used in a Mi
Jul 20, 2026, 9:37 AM

Synthi from Bandwidth
#117963859: Microsoft Technical Support Scam: 805-283-7072 Submitted We'll pick up your ticket soon Hello. I am reporting the following number and associated Go
Jul 20, 2026, 9:38 AM

[redacted] <voicesecurity@bandwidth.com>
to me
Jul 22, 2026, 12:36 PM

Thank you for contacting Bandwidth,

We have received your complaint and would like to assist with the problems you are experiencing. The telephone number you have identified is assigned to a wholesale customer of Bandwidth. Though Bandwidth does not provide services to or have a relationship with the end-user subscriber that originated the call, we have forwarded your complaint to our wholesale customer for investigation. We will let you know when we hear back from our customer, typically within 48hrs.

--

Thank you,

Bandwidth Network Fraud Mitigation Team

On July 23, 2026, at 11:18 AM EST, Demurrage received the following response:

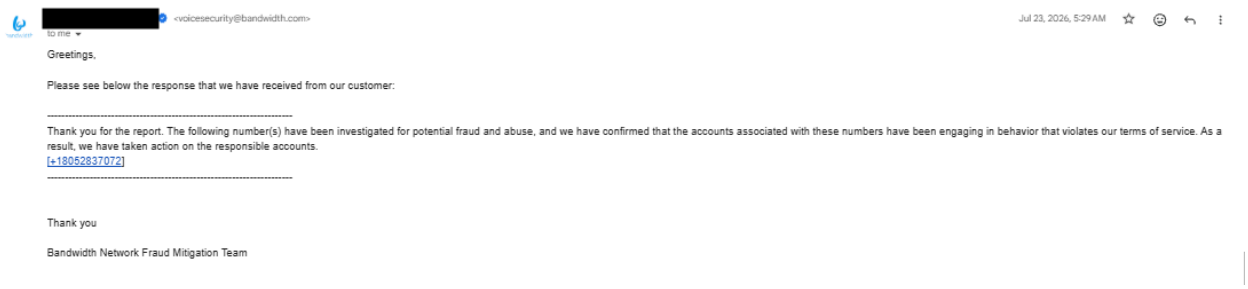
Greetings,

Please see below the response that we have received from our customer:

Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have confirmed that the accounts associated with these numbers have been engaging in behavior that violates our terms of service. As a result, we have taken action on the responsible accounts.

[+18052837072]

Once again, the wholesale provider proved to be a mark and had provided a false report, as the number remained active and was routing calls to voicemail. Demurrage updated the ticket accordingly, noting the mark's dishonesty, and requested that Bandwidth reopen the case. The scammer subsequently called one of Demurrage's dedicated cell phones from the reported Google Voice number, and this information was submitted to Bandwidth, which once again took no action against the mark for misrepresenting the outcome of the case.


[redacted] <voicesecurity@bandwidth.com> Jul 23, 2026, 5:29 AM

to me

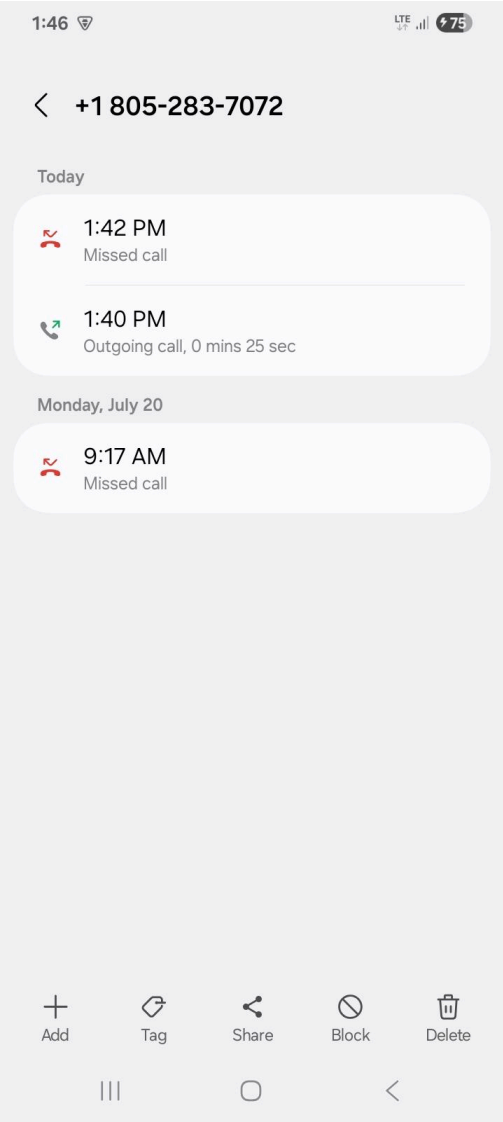
Greetings,

Please see below the response that we have received from our customer:

Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have confirmed that the accounts associated with these numbers have been engaging in behavior that violates our terms of service. As a result, we have taken action on the responsible accounts.
[+18052837072]

Thank you

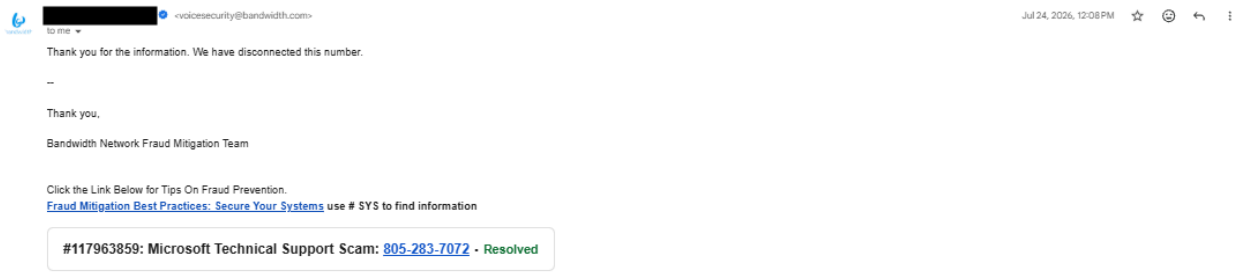
Bandwidth Network Fraud Mitigation Team



On July 24, 2026, at 8:01 AM EST, a support agent closed the ticket without ever providing an update or the outcome of the case.



Demurrage reopened the ticket on July 24, 2026, at 11:54 AM EST, requesting that a support agent review the evidence submitted in the previous report. On July 24, 2026, at 12:08 PM EST, a response was received confirming that the number had been disconnected for fraud.


[redacted] <voicesecurity@bandwidth.com> Jul 24, 2026, 12:08 PM

to me

Thank you for the information. We have disconnected this number.

--

Thank you,

Bandwidth Network Fraud Mitigation Team

Click the Link Below for Tips On Fraud Prevention.
Fraud Mitigation Best Practices: Secure Your Systems use # SYS to find information

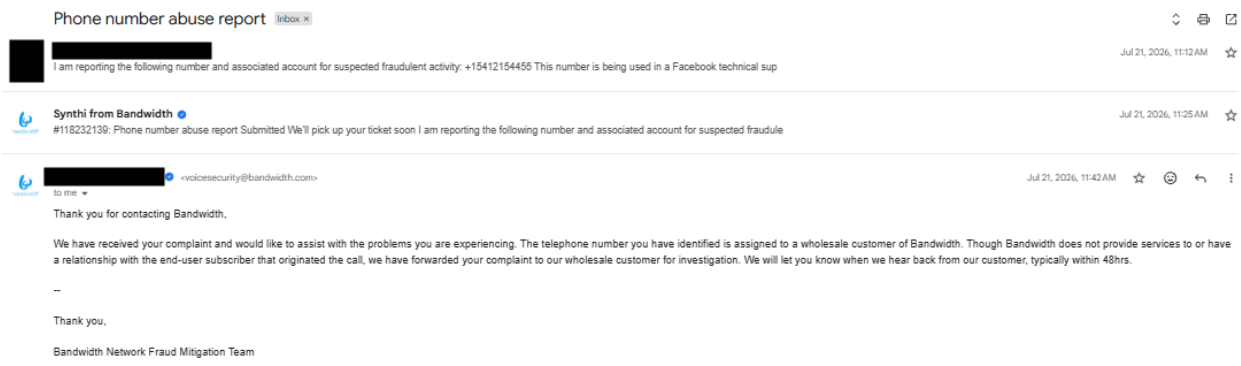
#117963859: Microsoft Technical Support Scam: 805-283-7072 - Resolved

The total time for this case was 4 days.

Case 4: 541-215-4455

This number was used as a callback number for a Facebook technical support scam. The number was traced back to Google Voice, and after verifying that it was being used as a callback number by a scammer, a report was submitted to Bandwidth on July 21, 2026, at 11:12 AM EST.

At 11:42 AM EST, Bandwidth responded, confirming that the report had been forwarded to the wholesale provider in question and that 48 hours should be allowed for a response.


Phone number abuse report Inbox ×

[redacted] Jul 21, 2026, 11:12 AM

I am reporting the following number and associated account for suspected fraudulent activity: +15412154455 This number is being used in a Facebook technical sup

Synthi from Bandwidth Jul 21, 2026, 11:25 AM

#118232139: Phone number abuse report Submitted We'll pick up your ticket soon I am reporting the following number and associated account for suspected fraudule

[redacted] <voicesecurity@bandwidth.com> Jul 21, 2026, 11:42 AM

to me

Thank you for contacting Bandwidth,

We have received your complaint and would like to assist with the problems you are experiencing. The telephone number you have identified is assigned to a wholesale customer of Bandwidth. Though Bandwidth does not provide services to or have a relationship with the end-user subscriber that originated the call, we have forwarded your complaint to our wholesale customer for investigation. We will let you know when we hear back from our customer, typically within 48hrs.

--

Thank you,

Bandwidth Network Fraud Mitigation Team

Neither the wholesale provider nor Bandwidth responded within the 48-hour window. On July 23, 2026, at 8:12 PM EST, Demurrage updated the ticket noting that 48 hours had passed without a response from the wholesale provider.

No further response was received until July 25, 2026, at 8:06 AM EST, when the wholesale provider responded with the following:

Greetings,

Please see below the response that we have received from our customer:

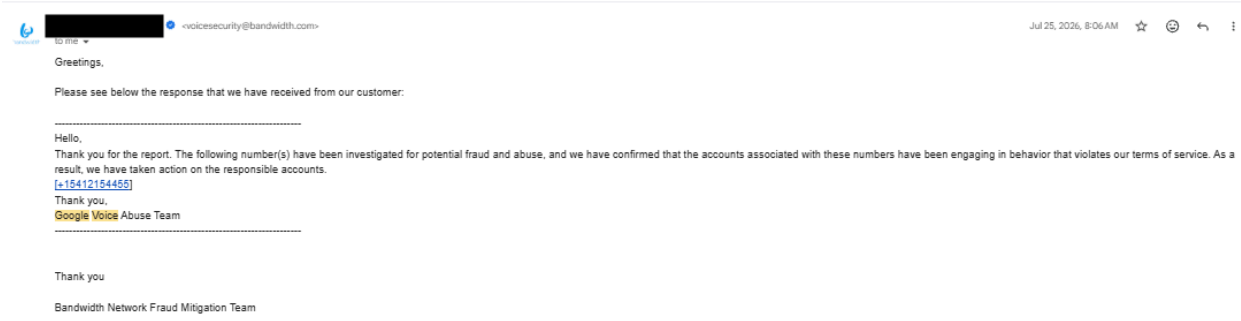
Hello,

Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have confirmed that the accounts associated with these numbers have been engaging in behavior that violates our terms of service. As a result, we have taken action on the responsible accounts.

[+15412154455]

Thank you,

Google Voice Abuse Team


[redacted] <voicesecurity@bandwidth.com> Jul 25, 2026, 8:06 AM

to me

Greetings,

Please see below the response that we have received from our customer:

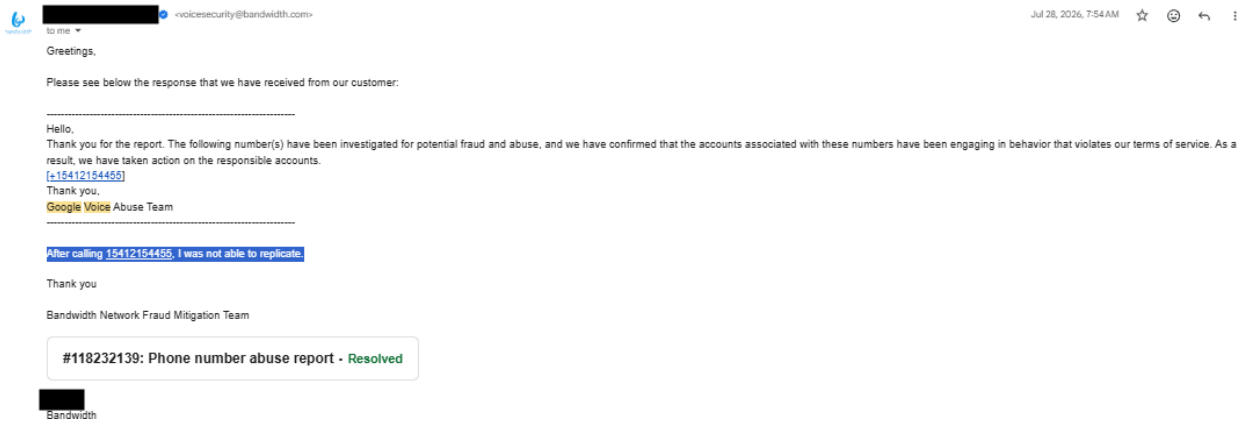
Hello,
Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have confirmed that the accounts associated with these numbers have been engaging in behavior that violates our terms of service. As a result, we have taken action on the responsible accounts.
[+15412154455]
Thank you,
Google Voice Abuse Team

Thank you

Bandwidth Network Fraud Mitigation Team

Once again, the wholesale provider proved to be a mark, as the number remained active. Demurrage updated the ticket on July 27, 2026, at 3:44 PM EST.

On July 28, 2026, at 7:54 AM EST, the mark responded with the same stock reply as July 25, 2026, adding the following: *After calling 1-541-215-4455, I was not able to replicate.*


[redacted] <voicesecurity@bandwidth.com> Jul 28, 2026, 7:54 AM

to me

Greetings,

Please see below the response that we have received from our customer:

Hello,
Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have confirmed that the accounts associated with these numbers have been engaging in behavior that violates our terms of service. As a result, we have taken action on the responsible accounts.
[+15412154455]
Thank you,
Google Voice Abuse Team

After calling 15412154455, I was not able to replicate.

Thank you

Bandwidth Network Fraud Mitigation Team

#118232139: Phone number abuse report · Resolved

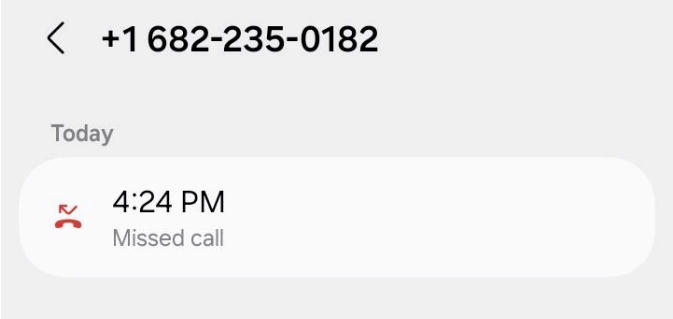
[redacted]
Bandwidth

This response was sufficient for Bandwidth to close the ticket and mark it as resolved, despite never making any attempt to verify the mark's claims, which once again proved to be false as the number remained active. Demurrage reopened the ticket on July 28, 2026, at 1:51 PM EST. No further response was received from either Bandwidth or the mark until July 31, 2026, at 7:39 AM EST, when Bandwidth responded that action had been taken against the associated account.

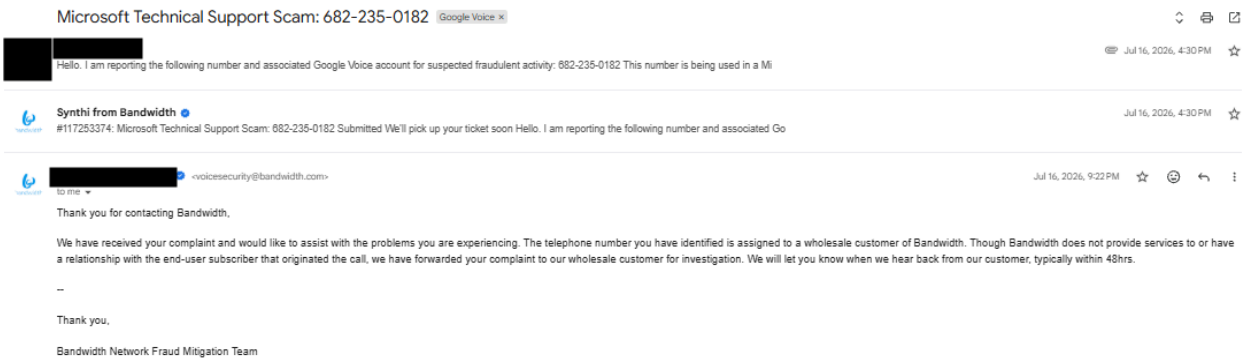
The total time for this case was 10 days.

Case 5: 682-235-0182

This number was used as a callback number for a Microsoft technical support scam. The number was traced back to Google Voice, and after verifying that it was being used as a callback number by a scammer after receiving a call from the scammer on one of the dedicated Demurrage cell phones, a report was submitted to Bandwidth on July 16, 2026, at 4:30 PM EST.

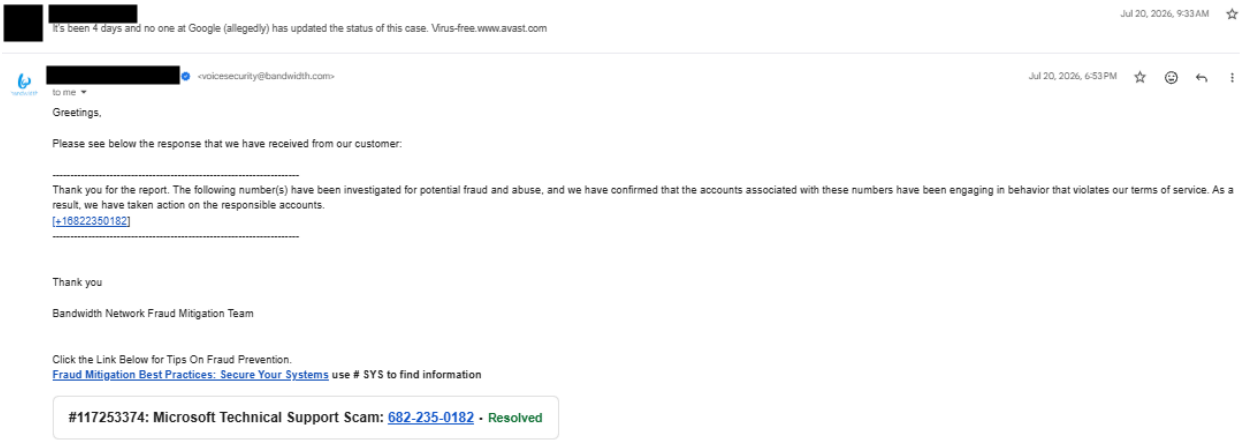


At 11:42 AM EST, Bandwidth responded, confirming that the report had been forwarded to the wholesale provider in question and that 48 hours should be allowed for a response.



No response was received from Bandwidth or the wholesale provider. On July 20, 2026, at 9:33 AM EST, four days later, Demurrage updated the ticket requesting a status update on the case. This is yet another example of Bandwidth failing to hold its wholesale provider accountable for not responding or updating cases within the 48 hour window, which is too long and should not be permitted by any telecom.

On July 20, 2026 at 6:53 PM EST, Bandwidth would respond with the following;


[redacted] It's been 4 days and no one at Google (allegedly) has updated the status of this case. Virus-free.www.avast.com

Jul 20, 2026, 9:33 AM

[redacted] <voicesecurity@bandwidth.com>

Jul 20, 2026, 6:53 PM

to me

Greetings,

Please see below the response that we have received from our customer:

Thank you for the report. The following number(s) have been investigated for potential fraud and abuse, and we have confirmed that the accounts associated with these numbers have been engaging in behavior that violates our terms of service. As a result, we have taken action on the responsible accounts.
[+16822350182]

Thank you

Bandwidth Network Fraud Mitigation Team

Click the Link Below for Tips On Fraud Prevention.
Fraud Mitigation Best Practices: Secure Your Systems use # SYS to find information

#117253374: Microsoft Technical Support Scam: 682-235-0182 - Resolved

The total time for this case was 4 days.

Statistics: Sinch

- As of September 2026, a total of 3,055 numbers traced back to Sinch were reported for use in tech support fraud, Publishers Clearing House impersonation fraud, various refund scams impersonating Amazon, PayPal, Microsoft, and other entities, and scammer callback numbers, across the following wholesale providers operating on Sinch's infrastructure: **Intelliquent, Onvoy, Onvoy Spectrum LLC, Talkatone, TextNow, GoTextMe, TextPlus, Neutral Tandem, Microsoft Teams, Vonage, Peerless, BulkVS, Sinch Voice,** and **Pinger.**
- Of the 3,055 numbers, 2,079 traced back to Onvoy. Given how Sinch structures its lookup data, these numbers were in active use by the following providers that use Onvoy as a pool for tolled numbers: **Microsoft Teams, Vonage, TextNow, TextPlus, GoTextMe, Pinger, Peerless,** and **BulkVS.** Regardless, all of these calls were routed through Sinch's network and infrastructure.
- An additional 920 of the 3,055 numbers traced back to **Intelliquent.**
- An additional 56 of the 3,055 numbers traced back to **Sinch Voice**.
- Cases where emails were sent to both Sinch and Intelliquent were never resolved. Cases submitted through the Sinch web form remain inconclusive, as neither Sinch nor its wholesale providers communicated with Demurrage regarding the status or outcome of any case. If action was taken against a

reported number, no one at Sinch or its wholesale providers took credit for it. Sinch's takedown rate therefore remains unknown.

- The only wholesale providers on Sinch's network that engaged directly with Demurrage when the Sinch web form was used were Pinger and GoTextMe. Direct communication with these providers resulted in action being taken against the reported numbers. Sinch itself took no independent action.
- In cases where an Intelliquent number was reported for fraud, those numbers were never shut down by Sinch or the relevant wholesale provider.
- Several numbers used in Publishers Clearing House scams that traced back to Onvoy were reported multiple times, with Sinch taking no action against the associated accounts.
- The scammer operations associated with all of these cases were traced back to India, Jamaica, and Pakistan.

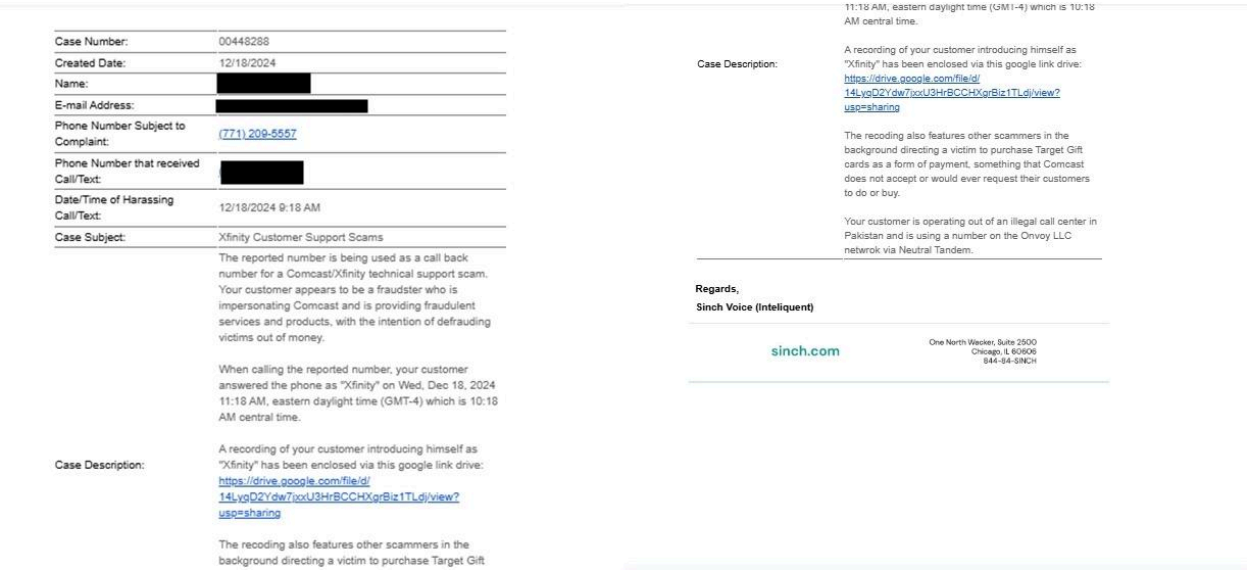
Notable cases

Case 1: (771) 209-5557

This number was used to facilitate an Xfinity customer support scam and was traced back to Onvoy Spectrum LLC through Neutral Tandem, both legacy networks acquired by Sinch.

On December 18, 2024, Demurrage submitted a report to Sinch using the Sinch web form. As the web form does not include an option to submit evidence directly, a Google Drive link was used to share a recording of a scammer answering the reported number and identifying as Xfinity support through an impersonated Xfinity IVR.

As the web form also defaults all call times to Central Time, Demurrage included the correct call time in the body of the submission.



Case Number:	00448288
Created Date:	12/18/2024
Name:	[redacted]
E-mail Address:	[redacted]
Phone Number Subject to Complaint:	(771) 209-5557
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	12/18/2024 9:18 AM
Case Subject:	Xfinity Customer Support Scams
Case Description:	The reported number is being used as a call back number for a Comcast/Xfinity technical support scam. Your customer appears to be a fraudster who is impersonating Comcast and is providing fraudulent services and products, with the intention of defrauding victims out of money. When calling the reported number, your customer answered the phone as "Xfinity" on Wed, Dec 18, 2024 11:18 AM, eastern daylight time (GMT-4) which is 10:18 AM central time. A recording of your customer introducing himself as "Xfinity" has been enclosed via this google link drive: https://drive.google.com/file/d/14LygD2Ydw7jxxU3HrBCCHXgrBiz1TLdj/view?usp=sharing The recoding also features other scammers in the background directing a victim to purchase Target Gift cards as a form of payment, something that Comcast does not accept or would ever request their customers to do or buy. Your customer is operating out of an illegal call center in Pakistan and is using a number on the Onvoy LLC netwrok via Neutral Tandem.

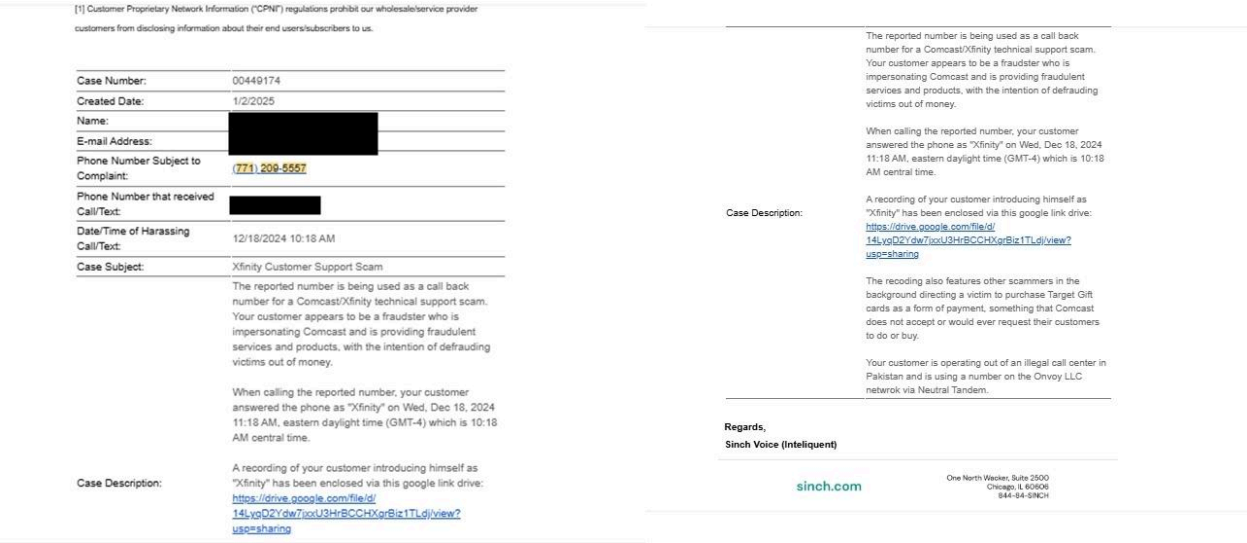
Regards,
Sinch Voice (Inteliquent)

sinch.com

One North Wacker, Suite 2500
Chicago, IL 60606
844-64-SINCH

(771) 209-5557_Wed, Dec 18, 2024 11:18 AM, eastern daylight time (GMT-4)

Sinch did not respond and the number remained active for the remainder of December. A second report was submitted to Sinch on January 2, 2025, again using the Sinch web form, referencing the original case from December 18, 2024.



[1] Customer Proprietary Network Information ("CPNI") regulations prohibit our wholesale/service provider customers from disclosing information about their end users/subscribers to us.

Case Number:	00449174
Created Date:	1/2/2025
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(771) 209-5557
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	12/18/2024 10:18 AM
Case Subject:	Xfinity Customer Support Scam
Case Description:	The reported number is being used as a call back number for a Comcast/Xfinity technical support scam. Your customer appears to be a fraudster who is impersonating Comcast and is providing fraudulent services and products, with the intention of defrauding victims out of money. When calling the reported number, your customer answered the phone as "Xfinity" on Wed, Dec 18, 2024 11:18 AM, eastern daylight time (GMT-4) which is 10:18 AM central time. A recording of your customer introducing himself as "Xfinity" has been enclosed via this google link drive: https://drive.google.com/file/d/14LygD2Ydw7jxxU3HrBCCHXgrBiz1TLdj/view?usp=sharing The recoding also features other scammers in the background directing a victim to purchase Target Gift cards as a form of payment, something that Comcast does not accept or would ever request their customers to do or buy. Your customer is operating out of an illegal call center in Pakistan and is using a number on the Onvoy LLC netwrok via Neutral Tandem.

Regards,
Sinch Voice (Inteliquent)

sinch.com

One North Wacker, Suite 2500
Chicago, IL 60606
844-64-SINCH

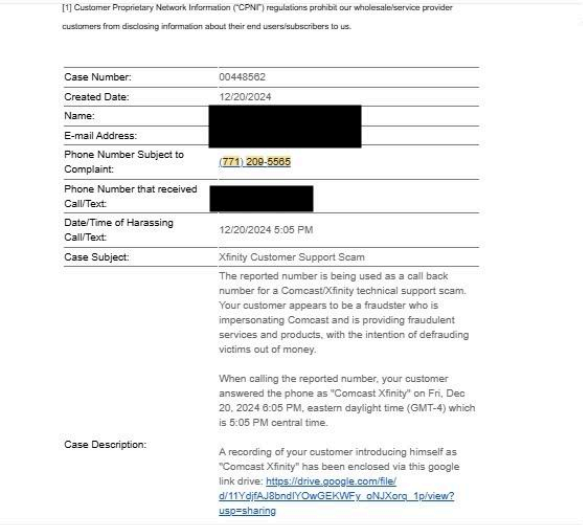
This report also went unanswered and the outcome of this case remains unresolved.

Case 2: (771) 209-5565

This number was used to facilitate an Xfinity customer support scam and was traced back to Onvoy Spectrum LLC through Neutral Tandem, both legacy networks acquired by Sinch.

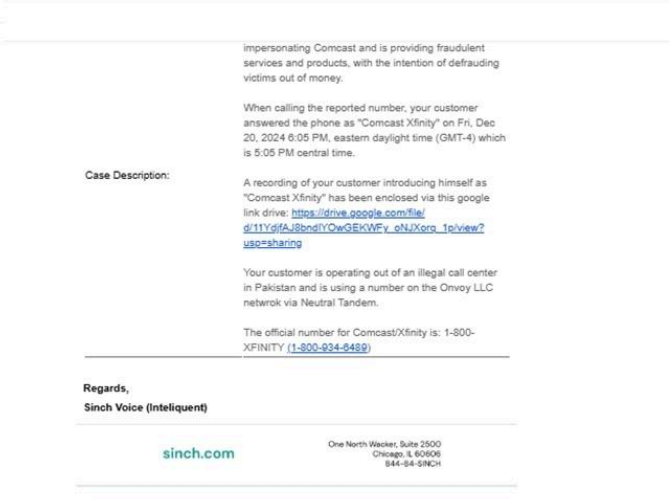
On December 20, 2024, Demurrage submitted a report to Sinch using the Sinch web form. As the web form does not include an option to submit evidence directly, a Google Drive link was used to share a recording of a scammer answering the reported number and identifying as Xfinity support through an impersonated Xfinity IVR.

As the web form also defaults all call times to Central Time, Demurrage included the correct call time in the body of the submission.



[1] Customer Proprietary Network Information ("CPNI") regulations prohibit our wholesale/service provider customers from disclosing information about their end users/subscribers to us.

Case Number:	00448582
Created Date:	12/20/2024
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(771) 209-5565
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	12/20/2024 5:05 PM
Case Subject:	Xfinity Customer Support Scam
Case Description:	The reported number is being used as a call back number for a Comcast/Xfinity technical support scam. Your customer appears to be a fraudster who is impersonating Comcast and is providing fraudulent services and products, with the intention of defrauding victims out of money. When calling the reported number, your customer answered the phone as "Comcast Xfinity" on Fri, Dec 20, 2024 6:05 PM, eastern daylight time (GMT-4) which is 5:05 PM central time. A recording of your customer introducing himself as "Comcast Xfinity" has been enclosed via this google link drive: https://drive.google.com/file/d/11YdjfAJ8bndIYOwGEKWFy_oNJXorg_1p/view?usp=sharing



impersonating Comcast and is providing fraudulent services and products, with the intention of defrauding victims out of money.

When calling the reported number, your customer answered the phone as "Comcast Xfinity" on Fri, Dec 20, 2024 6:05 PM, eastern daylight time (GMT-4) which is 5:05 PM central time.

Case Description:

A recording of your customer introducing himself as "Comcast Xfinity" has been enclosed via this google link drive: https://drive.google.com/file/d/11YdjfAJ8bndIYOwGEKWFy_oNJXorg_1p/view?usp=sharing

Your customer is operating out of an illegal call center in Pakistan and is using a number on the Onvoy LLC netwrok via Neutral Tandem.

The official number for Comcast/Xfinity is: 1-800-XFINITY (1-800-934-6489)

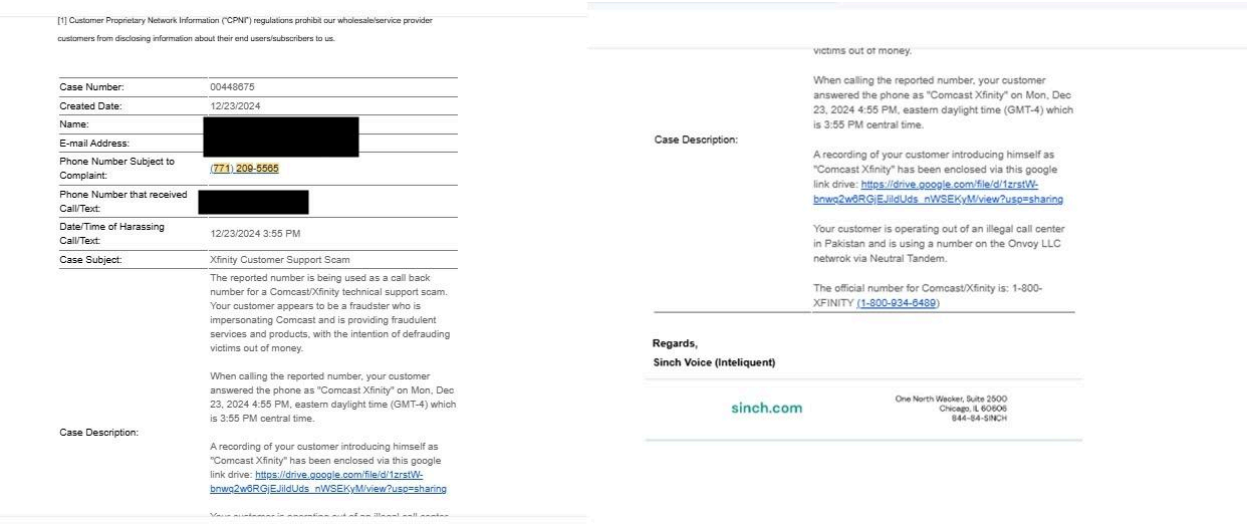
Regards,
Sinch Voice (Inteliquent)

sinch.com

One North Wacker, Suite 2500
Chicago, IL 60606
844-64-SINCH

(771) 209-5565_ Fri, Dec 20, 2024 6:05 PM

Sinch did not respond and the number remained active. A second report was submitted to Sinch on December 23, 2024, again using the Sinch web form, and included a second recording of a scammer answering the reported number and identifying as Xfinity support through an impersonated Xfinity IVR menu.



[1] Customer Proprietary Network Information ("CPNI") regulations prohibit our wholesale/service provider customers from disclosing information about their end users/subscribers to us.

Case Number:	00448675
Created Date:	12/23/2024
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(771) 209-5565
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	12/23/2024 3:55 PM
Case Subject:	Xfinity Customer Support Scam
Case Description:	The reported number is being used as a call back number for a Comcast/Xfinity technical support scam. Your customer appears to be a fraudster who is impersonating Comcast and is providing fraudulent services and products, with the intention of defrauding victims out of money. When calling the reported number, your customer answered the phone as "Comcast Xfinity" on Mon, Dec 23, 2024 4:55 PM, eastern daylight time (GMT-4) which is 3:55 PM central time. A recording of your customer introducing himself as "Comcast Xfinity" has been enclosed via this google link drive: https://drive.google.com/file/d/1zrstW-bnwq2w6RGjEJildUds_nWSEKyM/view?usp=sharing

victims out of money.

When calling the reported number, your customer answered the phone as "Comcast Xfinity" on Mon, Dec 23, 2024 4:55 PM, eastern daylight time (GMT-4) which is 3:55 PM central time.

Case Description:

A recording of your customer introducing himself as "Comcast Xfinity" has been enclosed via this google link drive: https://drive.google.com/file/d/1zrstW-bnwq2w6RGjEJildUds_nWSEKyM/view?usp=sharing

Your customer is operating out of an illegal call center in Pakistan and is using a number on the Onvoy LLC netwrok via Neutral Tandem.

The official number for Comcast/Xfinity is: 1-800-XFINITY (1-800-934-6489)

Regards,
Sinch Voice (Inteliquent)

sinch.com

One North Wacker, Suite 2500
Chicago, IL 60606
844-64-SINCH

(771) 209-5565_Mon, Dec 23, 2024 4:55 PM

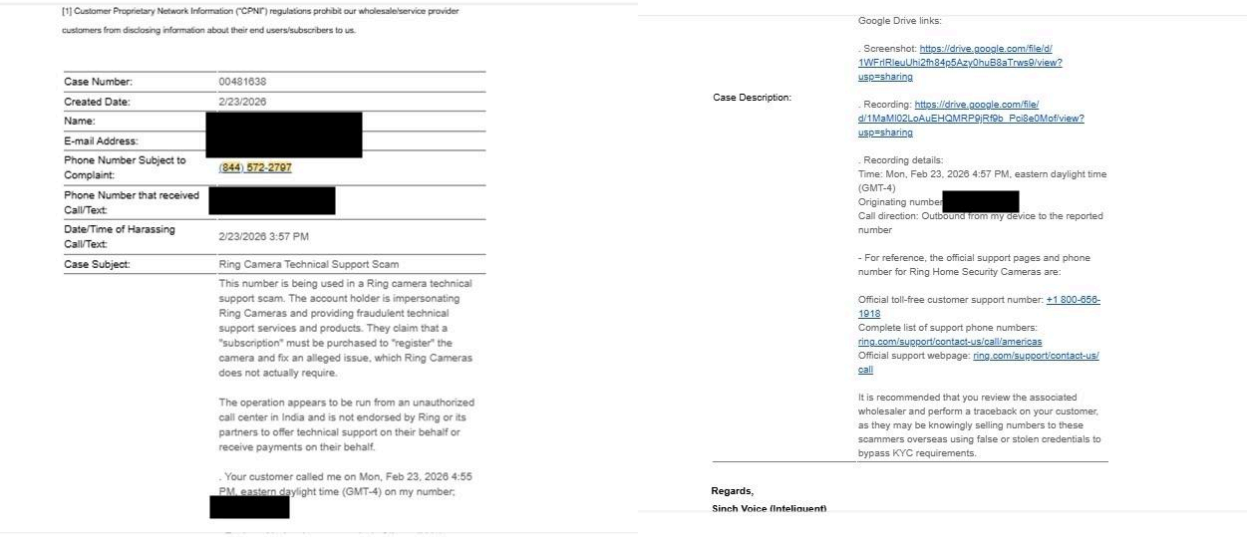
This report also went unanswered and the outcome of this case remains unresolved.

Case 3: (844) 572-2797

This number was used to facilitate a Ring camera customer support scam and was traced back to Intelliquent.

On February 23, 2026, Demurrage submitted a report to Sinch using the Sinch web form. As the web form does not include an option to submit evidence directly, a Google Drive link was used to share a recording of a scammer answering the reported number and identifying as "camera support," along with a screenshot of the scammer calling one of Demurrage's dedicated cell phones from the reported toll-free number.

As the web form defaults all call times to Central Time, Demurrage included the correct call time in the body of the submission.



[1] Customer Proprietary Network Information ("CPNI") regulations prohibit our wholesale/service provider customers from disclosing information about their end users/subscribers to us.

Case Number:	00481638
Created Date:	2/23/2026
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(844) 572-2797
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	2/23/2026 3:57 PM
Case Subject:	Ring Camera Technical Support Scam

Case Description:

This number is being used in a Ring camera technical support scam. The account holder is impersonating Ring Cameras and providing fraudulent technical support services and products. They claim that a "subscription" must be purchased to "register" the camera and fix an alleged issue, which Ring Cameras does not actually require.

The operation appears to be run from an unauthorized call center in India and is not endorsed by Ring or its partners to offer technical support on their behalf or receive payments on their behalf.

. Your customer called me on Mon, Feb 23, 2026 4:55 PM, eastern daylight time (GMT-4) on my number: [redacted]

Google Drive links:

. Screenshot: https://drive.google.com/file/d/1WFrIRleuUhi2fh84p5Azy0huB8aTrws9/view?usp=sharing

. Recording: https://drive.google.com/file/d/1MaMI02LoAuEHQMRP9jRf9b_PciBe0Mof/view?usp=sharing

. Recording details:
Time: Mon, Feb 23, 2026 4:57 PM, eastern daylight time (GMT-4)
Originating number: [redacted]
Call direction: Outbound from my device to the reported number

- For reference, the official support pages and phone number for Ring Home Security Cameras are:

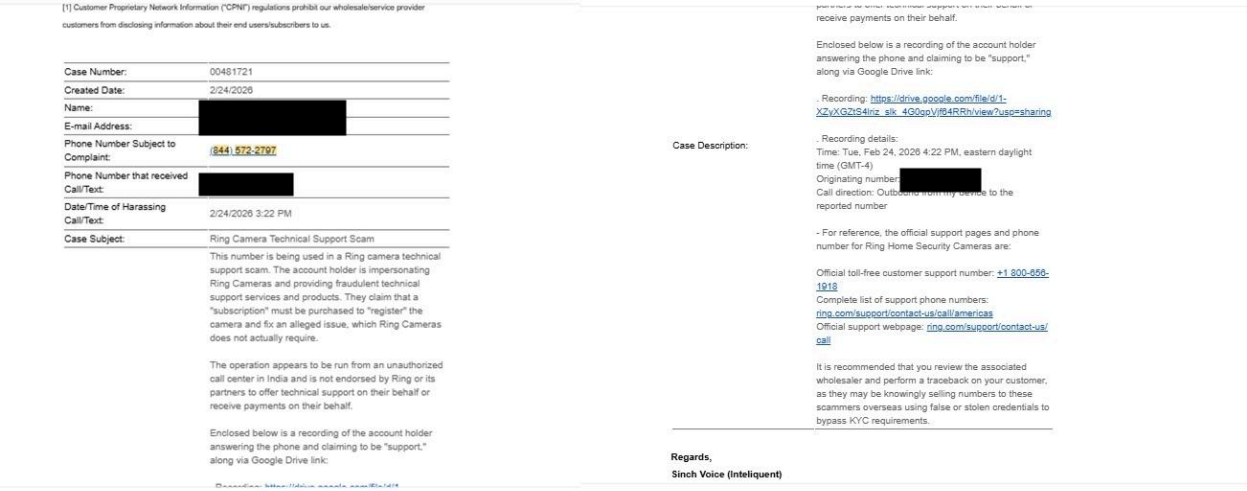
Official toll-free customer support number: +1 800-656-1918
Complete list of support phone numbers: ring.com/support/contact-us/call/americas
Official support webpage: ring.com/support/contact-us/call

It is recommended that you review the associated wholesaler and perform a traceback on your customer, as they may be knowingly selling numbers to these scammers overseas using false or stolen credentials to bypass KYC requirements.

Regards,
Sinch Voice (Inteliquent)

Mon, Feb 23, 2026 4_55 PM_out-88842712142

Sinch did not respond and the number remained active. A second report was submitted to Sinch on February 24, 2026, again using the Sinch web form, and included a recording of a scammer answering the reported number and identifying as "support." This report also went unanswered and the number remained active.



[1] Customer Proprietary Network Information ("CPNI") regulations prohibit our wholesale/service provider customers from disclosing information about their end users/subscribers to us.

Case Number:	00481721
Created Date:	2/24/2026
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(844) 572-2797
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	2/24/2026 3:22 PM
Case Subject:	Ring Camera Technical Support Scam

Case Description:

This number is being used in a Ring camera technical support scam. The account holder is impersonating Ring Cameras and providing fraudulent technical support services and products. They claim that a "subscription" must be purchased to "register" the camera and fix an alleged issue, which Ring Cameras does not actually require.

The operation appears to be run from an unauthorized call center in India and is not endorsed by Ring or its partners to offer technical support on their behalf or receive payments on their behalf.

Enclosed below is a recording of the account holder answering the phone and claiming to be "support," along via Google Drive link:

receive payments on their behalf.

Enclosed below is a recording of the account holder answering the phone and claiming to be "support," along via Google Drive link:

. Recording: https://drive.google.com/file/d/1-XZyXGZtS4lriz_slk_4G0qpVjf84RRh/view?usp=sharing

. Recording details:
Time: Tue, Feb 24, 2026 4:22 PM, eastern daylight time (GMT-4)
Originating number: [redacted]
Call direction: Outbound from my device to the reported number

- For reference, the official support pages and phone number for Ring Home Security Cameras are:

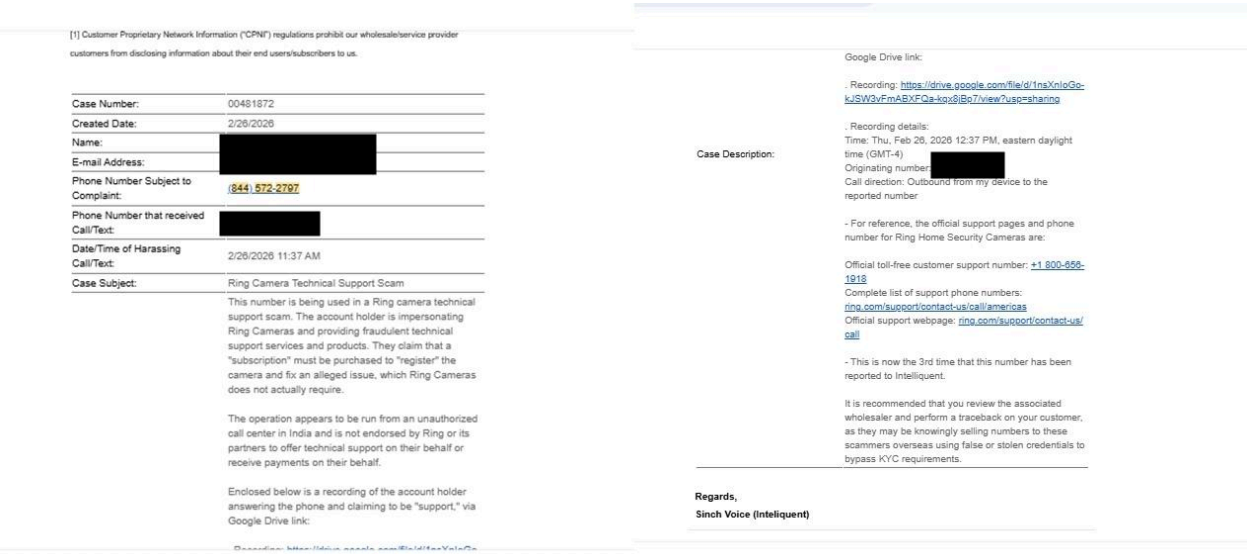
Official toll-free customer support number: +1 800-656-1918
Complete list of support phone numbers: ring.com/support/contact-us/call/americas
Official support webpage: ring.com/support/contact-us/call

It is recommended that you review the associated wholesaler and perform a traceback on your customer, as they may be knowingly selling numbers to these scammers overseas using false or stolen credentials to bypass KYC requirements.

Regards,
Sinch Voice (Inteliquent)

Tue, Feb 24, 2026 4_22 PM_out-8445722797

A third report was submitted to Sinch on February 26, 2026, again using the Sinch web form, and included a recording of a scammer answering the reported number and identifying as "support."



[1] Customer Proprietary Network Information ("CPNI") regulations prohibit our wholesale/service provider customers from disclosing information about their end users/subscribers to us.

Case Number:	00481872
Created Date:	2/26/2026
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(844) 572-2797
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	2/26/2026 11:37 AM
Case Subject:	Ring Camera Technical Support Scam

Case Description:

This number is being used in a Ring camera technical support scam. The account holder is impersonating Ring Cameras and providing fraudulent technical support services and products. They claim that a "subscription" must be purchased to "register" the camera and fix an alleged issue, which Ring Cameras does not actually require.

The operation appears to be run from an unauthorized call center in India and is not endorsed by Ring or its partners to offer technical support on their behalf or receive payments on their behalf.

Enclosed below is a recording of the account holder answering the phone and claiming to be "support," via Google Drive link:

Google Drive link:

- Recording: https://drive.google.com/file/d/1nsXnIoGo-kJSW3vFmABXFQa-kqx8jBp7/view?usp=sharing

- Recording details:
Time: Thu, Feb 26, 2026 12:37 PM, eastern daylight time (GMT-4)
Originating number: [redacted]
Call direction: Outbound from my device to the reported number

- For reference, the official support pages and phone number for Ring Home Security Cameras are:

Official toll-free customer support number: +1 800-656-1918
Complete list of support phone numbers: ring.com/support/contact-us/call/americas
Official support webpage: ring.com/support/contact-us/call

- This is now the 3rd time that this number has been reported to Intelliquent.

It is recommended that you review the associated wholesaler and perform a traceback on your customer, as they may be knowingly selling numbers to these scammers overseas using false or stolen credentials to bypass KYC requirements.

Regards,
Sinch Voice (Intelliquent)

Thu, Feb 26, 2026 12_37 PM_out-8445722797

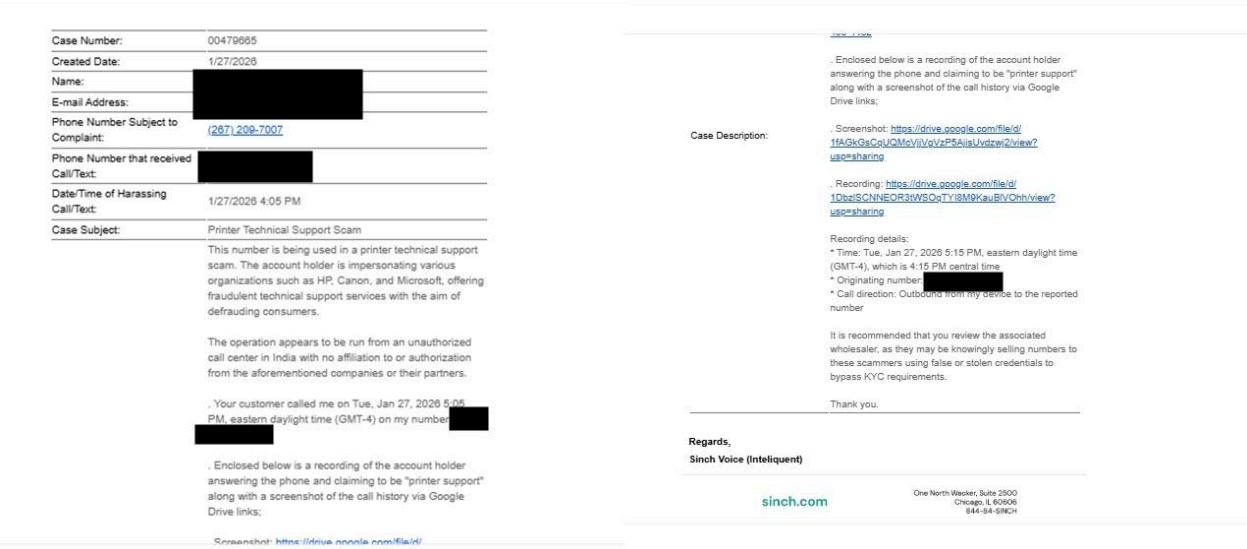
This report also went unanswered and the number remained active. Neither Sinch nor Inteliquent took action against the scammers or the wholesale providers, and no response was ever received from Sinch, Intelliquent, or the wholesale provider throughout the entirety of this case.

Case 4: (267) 209-7007

This number was used as a callback number for a printer technical support scam and was traced back to Onvoy.

On January 27, 2026, Demurrage submitted a report to Sinch using the Sinch web form after receiving a call from the scammer on one of Demurrage's dedicated cell phones. As the web form does not include an option to submit evidence directly, a Google Drive link was used to share a screenshot of the call history and a recording of a scammer answering the reported number and identifying as "printer support."

As the web form defaults all call times to Central Time, Demurrage included the correct call time in the body of the submission.



Case Number:	00479665
Created Date:	1/27/2026
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(267) 209-7007
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	1/27/2026 4:05 PM
Case Subject:	Printer Technical Support Scam

This number is being used in a printer technical support scam. The account holder is impersonating various organizations such as HP, Canon, and Microsoft, offering fraudulent technical support services with the aim of defrauding consumers.

The operation appears to be run from an unauthorized call center in India with no affiliation to or authorization from the aforementioned companies or their partners.

. Your customer called me on Tue, Jan 27, 2026 5:05 PM, eastern daylight time (GMT-4) on my number [redacted]

. Enclosed below is a recording of the account holder answering the phone and claiming to be "printer support" along with a screenshot of the call history via Google Drive links;

. Screenshot: https://drive.google.com/file/d/

. Enclosed below is a recording of the account holder answering the phone and claiming to be "printer support" along with a screenshot of the call history via Google Drive links;

Case Description:

. Screenshot: https://drive.google.com/file/d/1fAGkGsCqUQMcVjiVgVzF5AiisUvdzwj2/view?usp=sharing

. Recording: https://drive.google.com/file/d/1DbzISCNNEOR3tWSOqTYI8M9KauBlVOhh/view?usp=sharing

Recording details:
* Time: Tue, Jan 27, 2026 5:15 PM, eastern daylight time (GMT-4), which is 4:15 PM central time
* Originating number: [redacted]
* Call direction: Outbound from my device to the reported number

It is recommended that you review the associated wholesaler, as they may be knowingly selling numbers to these scammers using false or stolen credentials to bypass KYC requirements.

Thank you.

Regards,
Sinch Voice (Inteliquent)

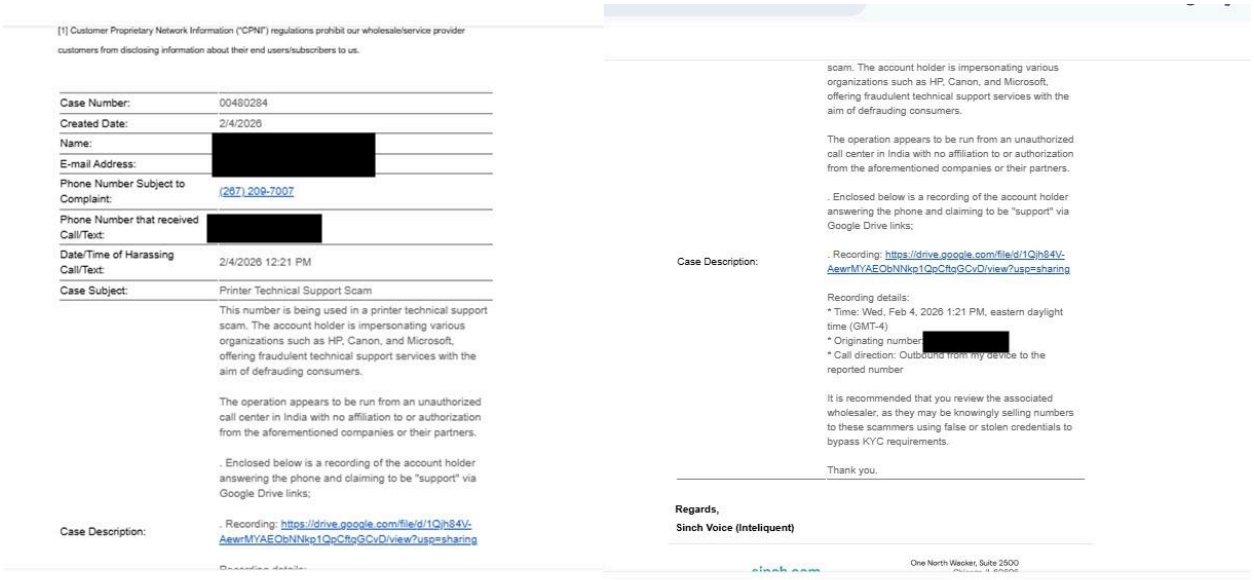
sinch.com

One North Wacker, Suite 2500
Chicago, IL 60606
844-64-SINCH

Tue, Jan 27, 2026 5_15 PM_out_2672097007.

Sinch did not respond and the number remained active.

A second report was submitted to Sinch on February 4, 2026, again using the Sinch web form, and included a recording of a scammer answering the reported number and identifying as "support," along with a screenshot of the call history.



[1] Customer Proprietary Network Information ("CPNI") regulations prohibit our wholesale/service provider customers from disclosing information about their end users/subscribers to us.

Case Number:	00480284
Created Date:	2/4/2026
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(267) 209-7007
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	2/4/2026 12:21 PM
Case Subject:	Printer Technical Support Scam
Case Description:	This number is being used in a printer technical support scam. The account holder is impersonating various organizations such as HP, Canon, and Microsoft, offering fraudulent technical support services with the aim of defrauding consumers. The operation appears to be run from an unauthorized call center in India with no affiliation to or authorization from the aforementioned companies or their partners. . Enclosed below is a recording of the account holder answering the phone and claiming to be "support" via Google Drive links; . Recording: https://drive.google.com/file/d/1Qjh84V-AewrMYAEObNNkp1QpCftqGCvD/view?usp=sharing

Case Description:

scam. The account holder is impersonating various organizations such as HP, Canon, and Microsoft, offering fraudulent technical support services with the aim of defrauding consumers.

The operation appears to be run from an unauthorized call center in India with no affiliation to or authorization from the aforementioned companies or their partners.

. Enclosed below is a recording of the account holder answering the phone and claiming to be "support" via Google Drive links;

. Recording: https://drive.google.com/file/d/1Qjh84V-AewrMYAEObNNkp1QpCftqGCvD/view?usp=sharing

Recording details:
* Time: Wed, Feb 4, 2026 1:21 PM, eastern daylight time (GMT-4)
* Originating number: [redacted]
* Call direction: Outbound from my device to the reported number

It is recommended that you review the associated wholesaler, as they may be knowingly selling numbers to these scammers using false or stolen credentials to bypass KYC requirements.

Thank you.

Regards,
Sinch Voice (Inteliquent)

sinch.com One North Wacker, Suite 2500

Wed, Feb 4, 2026 1_21 PM_out-2672097007

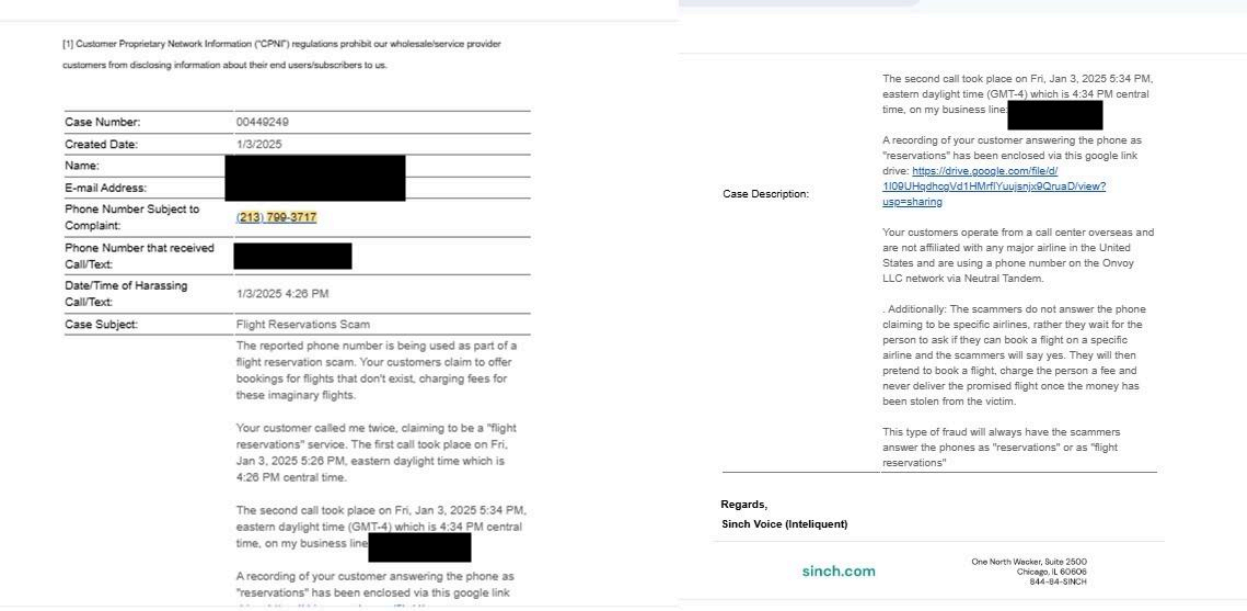
This report also went unanswered and the number remained active. Sinch took no action against the scammer or the wholesale provider, and no response was ever received from Sinch or the wholesale provider throughout the entirety of this case.

Case 5: (213) 799-3717

was traced back to Onvoy through Neutral Tandem, both legacy networks acquired by Sinch.

On January 3, 2025, Demurrage submitted a report to Sinch using the Sinch webform after receiving a call from the scammer on one of Demurrage's dedicated cell phones. As the webform does not include an option to submit evidence directly, a Google Drive link was used to share a screenshot of the call history.

As the web form defaults all call times to Central Time, Demurrage included the correct call time in the body of the submission.



[1] Customer Proprietary Network Information ("CPNI") regulations prohibit our wholesale/service provider customers from disclosing information about their end users/subscribers to us.

Case Number:	00449249
Created Date:	1/3/2025
Name:	[redacted]
E-mail Address:	
Phone Number Subject to Complaint:	(213) 799-3717
Phone Number that received Call/Text:	[redacted]
Date/Time of Harassing Call/Text:	1/3/2025 4:26 PM
Case Subject:	Flight Reservations Scam

Case Description:

The reported phone number is being used as part of a flight reservation scam. Your customers claim to offer bookings for flights that don't exist, charging fees for these imaginary flights.

Your customer called me twice, claiming to be a "flight reservations" service. The first call took place on Fri, Jan 3, 2025 5:26 PM, eastern daylight time which is 4:26 PM central time.

The second call took place on Fri, Jan 3, 2025 5:34 PM, eastern daylight time (GMT-4) which is 4:34 PM central time, on my business line [redacted]

A recording of your customer answering the phone as "reservations" has been enclosed via this google link drive: https://drive.google.com/file/d/1l09UHqdhcgVd1HMrfiYuujsnjx9QruaD/view?usp=sharing

Your customers operate from a call center overseas and are not affiliated with any major airline in the United States and are using a phone number on the Onvoy LLC network via Neutral Tandem.

. Additionally: The scammers do not answer the phone claiming to be specific airlines, rather they wait for the person to ask if they can book a flight on a specific airline and the scammers will say yes. They will then pretend to book a flight, charge the person a fee and never deliver the promised flight once the money has been stolen from the victim.

This type of fraud will always have the scammers answer the phones as "reservations" or as "flight reservations"

Regards,
Sinch Voice (Inteliquent)

sinch.com

One North Wacker, Suite 2500
Chicago, IL 60606
844-84-SINCH

(213) 799-3717_ Fri, Jan 3, 2025 5:34 PM, eastern daylight time (GMT-4)

Sinch did not respond and took no action against the scammer or the wholesale provider. No response was ever received from Sinch or the wholesale provider throughout the entirety of this case.

What Works: Telecom Action That Actually Stops Fraud

This section examines the actions taken by the following telecoms in response to fraud reports submitted by Demurrage, along with the effect those actions have had on scammer activity within their networks: Lumen & IP Horizon

Evidence is presented in the form of email records and timestamps for each report submitted. Each telecom was selected based on the following criteria: volume of reports submitted, action taken, response time, communication, and consistency in enforcing those actions.

Both telecoms scored highly across every criterion. Each communicated consistently and readily accepted fraud reports from Demurrage. Response times were quick, with Lumen consistently recording the fastest takedowns, followed by IP Horizon. In each case, the telecom placed a block on the reported number before forwarding the complaint to the relevant wholesale provider, and did so within a reasonable timeframe.

The action of blocking the number before engaging the wholesale provider is the critical differentiating factor.

Once a number is blocked, the mark can no longer dispute the report or offer justifications for keeping the number active, the campaign ends, and the scammers lose their number. This stands in direct contrast to the approach observed at Bandwidth, where wholesale providers are often given the opportunity to contest reports despite overwhelming evidence of fraud, including recordings of scammers identifying as Microsoft, Amazon, and other impersonated companies, as well as screenshots of scam invoices designed to frighten victims into calling the reported numbers. In those cases, wholesale providers frequently claim that the number was used for legitimate third-party technical support, the submitted evidence is disregarded, and the number is allowed to remain active.

Because Lumen reviews the evidence before forwarding a complaint to the wholesale provider, it effectively prevents marks and scammers from stalling the process or misrepresenting the nature of the reported number's use.

IP Horizon goes one step further. In addition to blocking the reported number, any consumer who subsequently calls that number is played a public service announcement, stating the number was reported for fraudulent activity.

This is a significant and commendable step, and one that every major telecom should consider adopting when blocking or disconnecting a number for fraud.

When telecoms step in directly and take action against fraud, they remove the scammer's ability to continue their campaign and eliminate the mark's ability to stall or override the report. These approaches should be standard practice for every major VoIP provider in the United States.

Statistics: Lumen

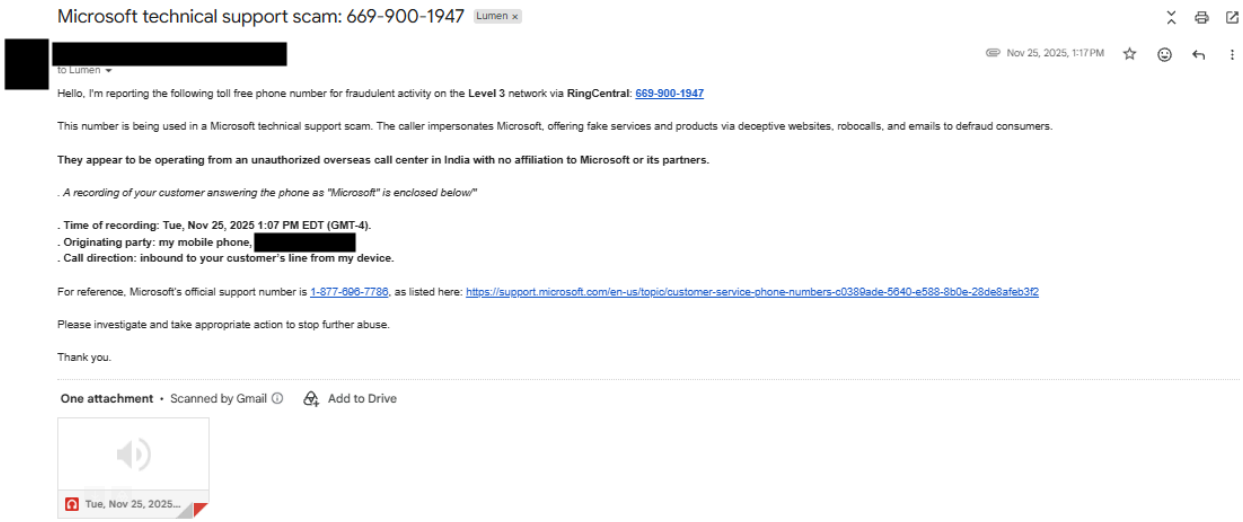
- As of September 2026, a total of 1,438 numbers traced back to Lumen were reported for use in tech support fraud, Publishers Clearing House impersonation fraud, and scammer callback numbers, across the following legacy telecoms operating on Lumen's infrastructure: Level 3 Communications, CentralLink and Skype.
- Several Level 3 numbers were also traced back to RingCentral, which uses Lumen's network for tolled numbers. None of the reported numbers were spoofed. Demurrage verifies all numbers prior to submission by calling them directly, and a scammer answered in every case.
- In all cases, the scammer operation was traced back to India, with the exception of the Publishers Clearing House scams, which were traced back to Jamaica.
- All 1,438 cases were resolved, representing a 100 percent takedown rate on Lumen's part.
- All cases were submitted to Lumen at the following email address: ***fraudoperations@lumen.com***

Notable Cases

Case 1: 669-900-1947

This was used as a callback number to facilitate a Microsoft technical support scam. The number was traced back to Lumen through the legacy CenturyLink network, with further verification confirming that it also traced back to RingCentral.

On November 25, 2025, at 1:17 PM EST, Demurrage submitted a report to Lumen including a recording of a scammer answering the reported number and identifying as Microsoft support.



Microsoft technical support scam: 669-900-1947 Lumen ×

[redacted]

Nov 25, 2025, 1:17 PM

to Lumen

Hello, I'm reporting the following toll free phone number for fraudulent activity on the **Level 3** network via **RingCentral**: 669-900-1947

This number is being used in a Microsoft technical support scam. The caller impersonates Microsoft, offering fake services and products via deceptive websites, robocalls, and emails to defraud consumers.

They appear to be operating from an unauthorized overseas call center in India with no affiliation to Microsoft or its partners.

. A recording of your customer answering the phone as "Microsoft" is enclosed below!"

. Time of recording: Tue, Nov 25, 2025 1:07 PM EDT (GMT-4).
. Originating party: my mobile phone, [redacted]
. Call direction: inbound to your customer's line from my device.

For reference, Microsoft's official support number is 1-877-696-7786, as listed here: https://support.microsoft.com/en-us/topic/customer-service-phone-numbers-c0389ade-5640-e588-8b0e-28de8afeb3f2

Please investigate and take appropriate action to stop further abuse.

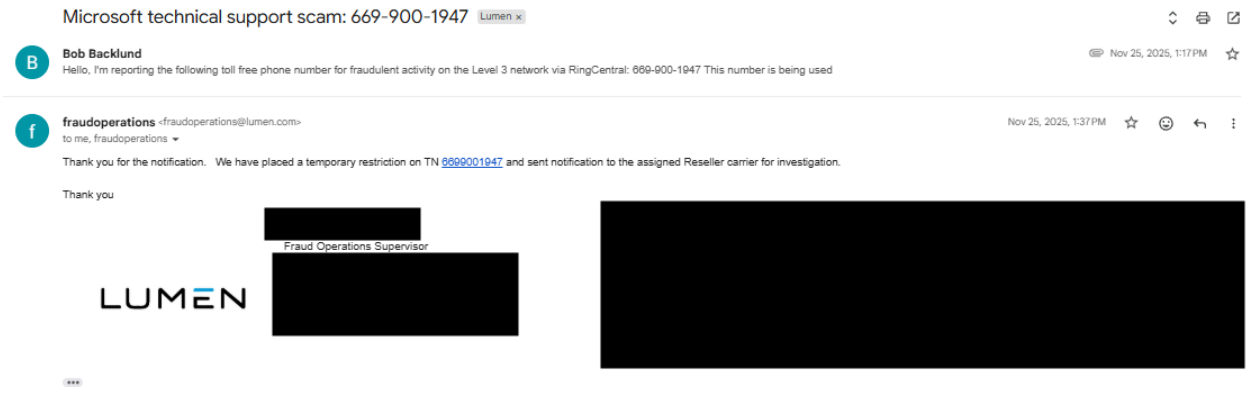
Thank you.

One attachment • Scanned by Gmail ⓘ Add to Drive

Tue, Nov 25, 2025...

Tue, Nov 25, 2025 1:07 PM_out-6699001947

On November 25, 2025, at 1:37 PM EST, Lumen responded, confirming that a temporary block had been placed on the number and that the case had been forwarded to their wholesale provider, who proved to be a mark. The mark made no attempt to contest the report and moved on.

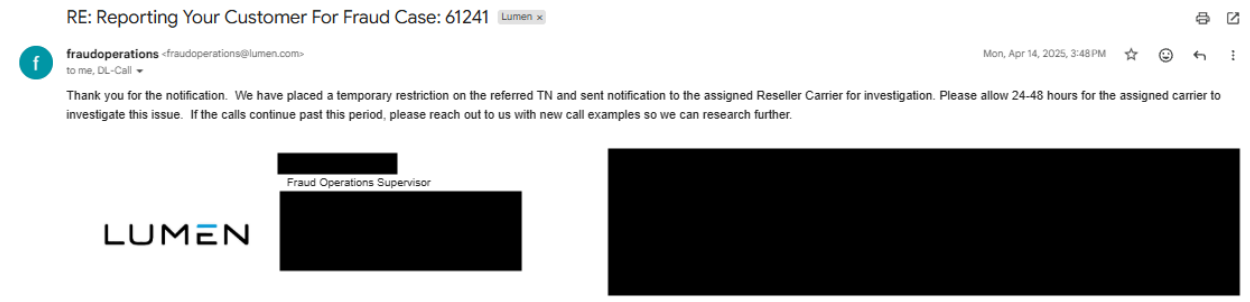


Total response time for this case was 20 minutes.

Case 2: 347-328-9694

This number was used as a callback number to facilitate a Publishers Clearing House scam. The number was traced back to Lumen through the legacy CenturyLink network, with further verification confirming that it also traced back to RingCentral.

On April 14, 2025, at 3:42 PM EST, Demurrage submitted a report to Lumen including a recording of a scammer answering the reported number and identifying himself as Dave Sawyer of Publishers Clearing House.



Mon, Apr 14, 2025 3_37 PM_out_3473289694

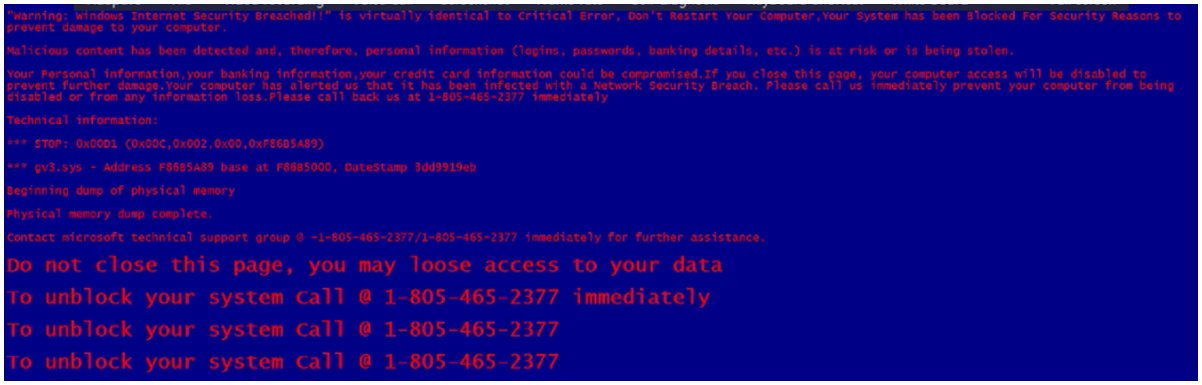
On April 14, 2025, at 3:48 PM EST, Lumen responded, confirming that a temporary block had been placed on the number and that the case had been forwarded to their

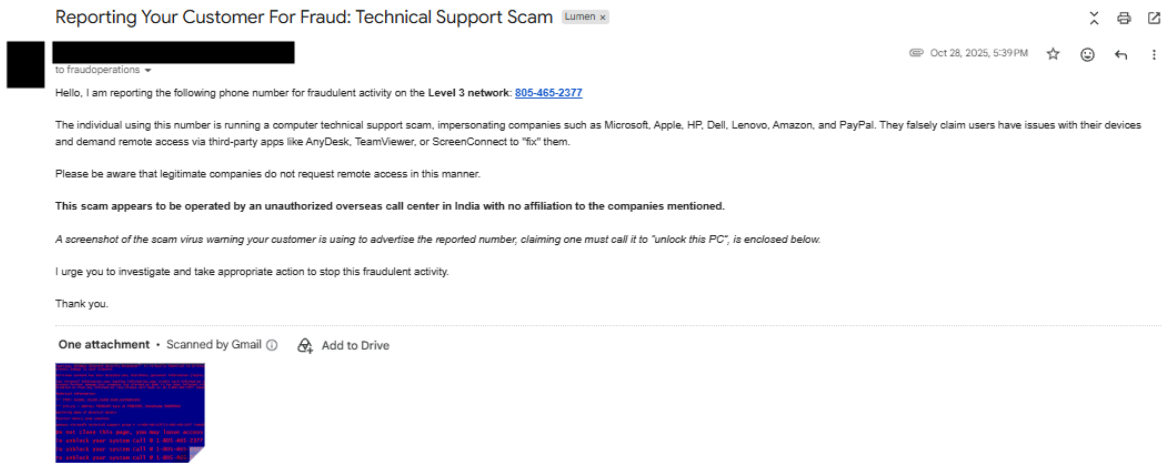
wholesale provider. Neither the scammer nor the wholesale provider made any attempt to contest the report, and the number remained blocked.

Total response time for this case was 6 minutes, the fastest takedown recorded at that point in the investigation.

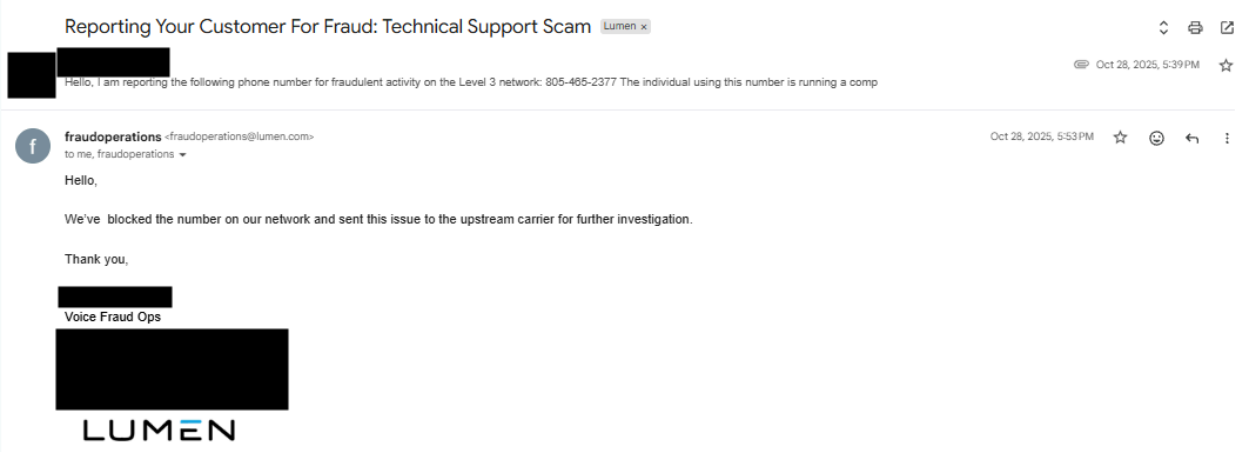
Case 3: 805-465-2377

This number was used to facilitate a Microsoft technical support scam delivered via a pop-up. The number was traced back to Lumen through the legacy Level 3 network. On October 28, 2025, at 5:39 PM EST, Demurrage submitted a report to Lumen including a screenshot of the scam pop-up.





On October 28, 2025, at 5:53 PM EST, Lumen responded, confirming that a temporary block had been placed on the number and that the case had been forwarded to their upstream provider. Neither the scammer nor the upstream provider made any attempt to contest the report, and the number remained blocked.



Reporting Your Customer For Fraud: Technical Support Scam Lumen ×

[redacted]

Hello, I am reporting the following phone number for fraudulent activity on the Level 3 network: 805-465-2377 The individual using this number is running a comp

Oct 28, 2025, 5:39 PM

fraudoperations <fraudoperations@lumen.com>
to me, fraudoperations

Oct 28, 2025, 5:53 PM

Hello,

We've blocked the number on our network and sent this issue to the upstream carrier for further investigation.

Thank you,

[redacted]
Voice Fraud Ops
[redacted]
LUMEN

Total response time for this case was 14 minutes.

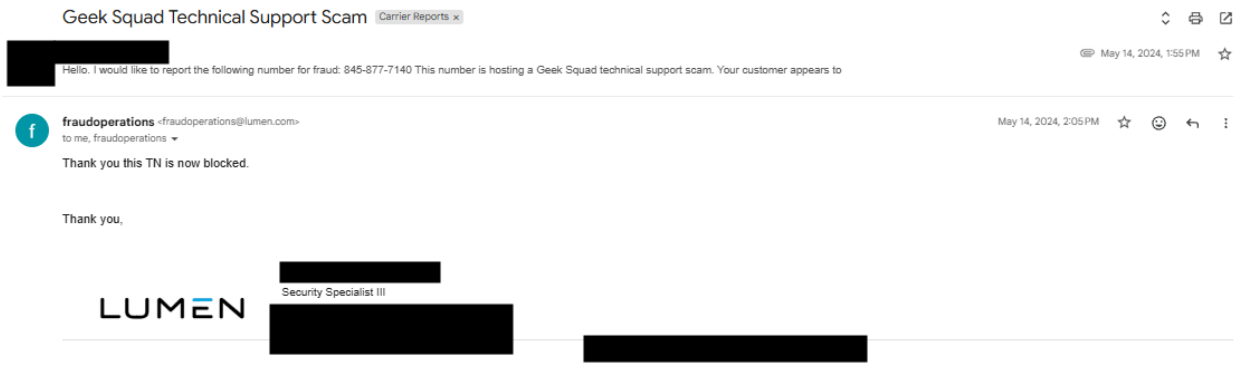
Case 4: 845-877-7140

This number was used as a call back number for a Geek Squad technical support scam. The number was traced back to Lumen.

On May 14, 2024, 1:55 PM EST, Demurrage submitted a report to Lumen including a recording of the scammer answering the phone, claiming to be Geek Squad.

May 14, 2024_1_54 PM_845-877-7140

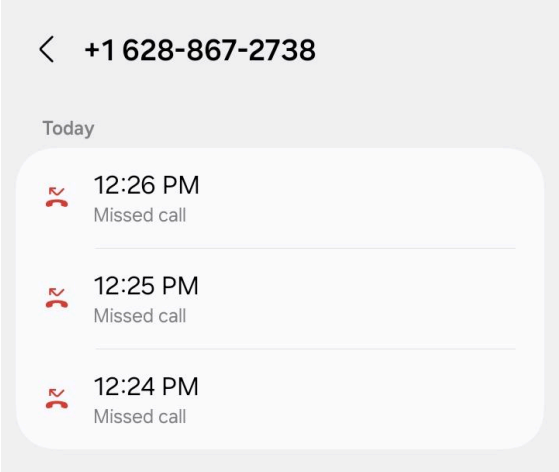
On May 14, 2024, 2:05 PM EST, Lumen responded, confirming that they had blocked had been placed on the number and that the case had been forwarded to their upstream provider. Neither the scammer nor the upstream provider made any attempt to contest the report, and the number remained blocked.



Total response time for this case was 10 minutes.

Case 5: 628-867-2738

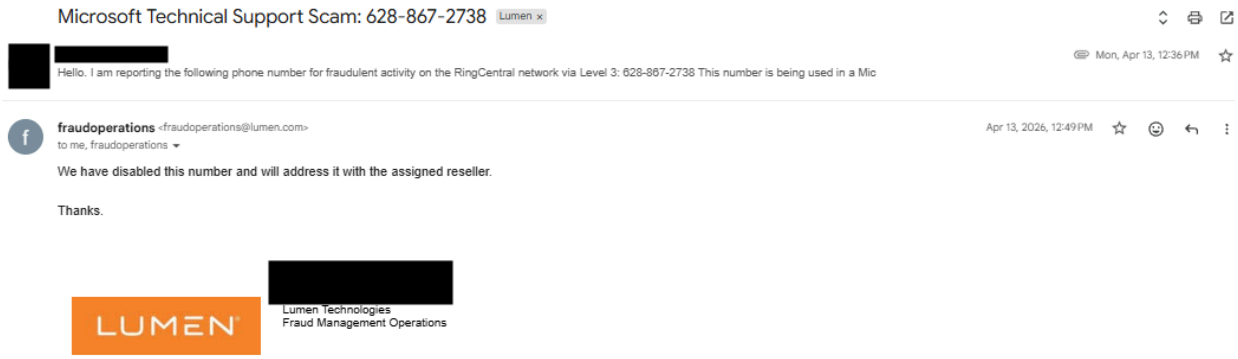
This number was used as a call back number for a Microsoft technical support scam. The number was traced back to Lumen via the legacy Level 3 network. The scammer called back one of Demurrage's dedicated cell phones on April 13, 2026 at 12:24 PM, 12:25 PM, 12:26 PM, EST.



On Apr 13, 2026, 12:36 PM EST, Demurrage submitted a report to Lumen including a recording of the scammer answering the phone, claiming to be "customer support service" along with a screenshot of the timestamps from the dedicated cell phone that received that calls.

Mon, Apr 13, 2026 12_26 PM_out-628-867-2738

On April 13, 2026, at 12:49 PM EST, Lumen responded, confirming that the number had been disabled and that the report had been forwarded to their assigned reseller, who proved to be a mark. Since the number was already disabled, neither the mark nor the scammer made any attempt to dispute the report and were forced to move on.



Total response time for this case was 13 minutes.

Statistics: IP Horizon

- As of September 2026, a total of 267 numbers traced back to IP Horizon were reported for use in tech support fraud, flight reservation scams, Spectrum and Xfinity customer support impersonation fraud, and scammer callback numbers.
- In all cases, the scammer operations were traced back to India and Pakistan.
- All 267 cases were resolved, representing a 100 percent takedown rate on IP Horizon's part.
- All cases were submitted to IP Horizon at the following email address: ***abuse@iphorizon.com***

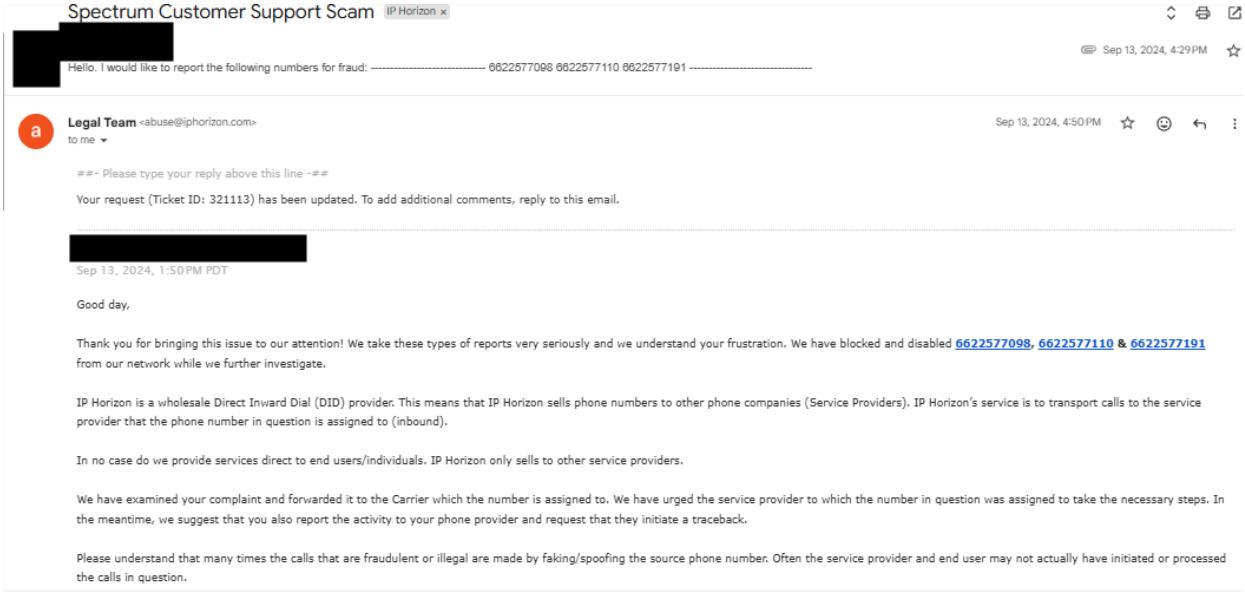
Notable Cases

Case 1: 6622577098 , 6622577110 , 6622577191

These three numbers were being used in a Spectrum customer support scam. After verifying that the numbers were being used to commit fraud and obtaining recordings of scammers answering each number using an impersonated Spectrum menu and identifying as Spectrum support, Demurrage submitted a report to IP Horizon on September 13, 2024, at 4:29 PM EST, covering all three numbers in a single email.

6622577098_September 13, 2024 at 4:07 PM, Eastern Daylight Time (GMT-4)
6622577110_September 13, 2024 at 4:10 PM, Eastern Daylight Time (GMT-4)
6622577191_September 13, 2024 at 4:14 PM, Eastern Daylight Time (GMT-4)

On September 13, 2024, at 4:50 PM EST, IP Horizon responded, confirming that all three reported numbers had been blocked and disabled pending further investigation, and that the report had been forwarded to the carrier within their network. With the numbers blocked and unable to receive calls, neither the scammer nor the carrier made any attempt to dispute the report or reclaim the numbers, and both moved on.



Spectrum Customer Support Scam IP Horizon ×

[redacted]

Sep 13, 2024, 4:29 PM

Hello. I would like to report the following numbers for fraud: ---------- 6622577098 6622577110 6622577191 ----------

a **Legal Team** <abuse@iphorizon.com>
to me

Sep 13, 2024, 4:50 PM

##- Please type your reply above this line -##

Your request (Ticket ID: 321113) has been updated. To add additional comments, reply to this email.

[redacted]

Sep 13, 2024, 1:50 PM PDT

Good day,

Thank you for bringing this issue to our attention! We take these types of reports very seriously and we understand your frustration. We have blocked and disabled 6622577098, 6622577110 & 6622577191 from our network while we further investigate.

IP Horizon is a wholesale Direct Inward Dial (DID) provider. This means that IP Horizon sells phone numbers to other phone companies (Service Providers). IP Horizon's service is to transport calls to the service provider that the phone number in question is assigned to (inbound).

In no case do we provide services direct to end users/individuals. IP Horizon only sells to other service providers.

We have examined your complaint and forwarded it to the Carrier which the number is assigned to. We have urged the service provider to which the number in question was assigned to take the necessary steps. In the meantime, we suggest that you also report the activity to your phone provider and request that they initiate a traceback.

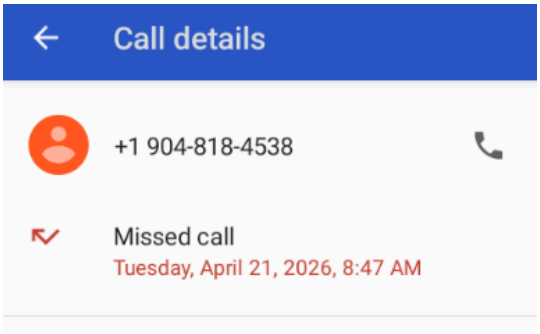
Please understand that many times the calls that are fraudulent or illegal are made by faking/spoofing the source phone number. Often the service provider and end user may not actually have initiated or processed the calls in question.

Total response time for this case was 21 minutes.

Case 2: 904-818-4538

This number was used as a callback number for an Amazon refund scam delivered via a robocall to one of Demurrage's dedicated cell phones. The number was traced back to IP Horizon, and after calling it back to verify that it was active and being used by the same scammers who initiated the robocall, Demurrage submitted a report to IP Horizon on Apr 21, 2026, 9:07 AM EST.

The report included two recordings of the robocall and of a scammer answering the reported number and identifying as Amazon support, along with a screenshot of the call history from the dedicated cell phone.

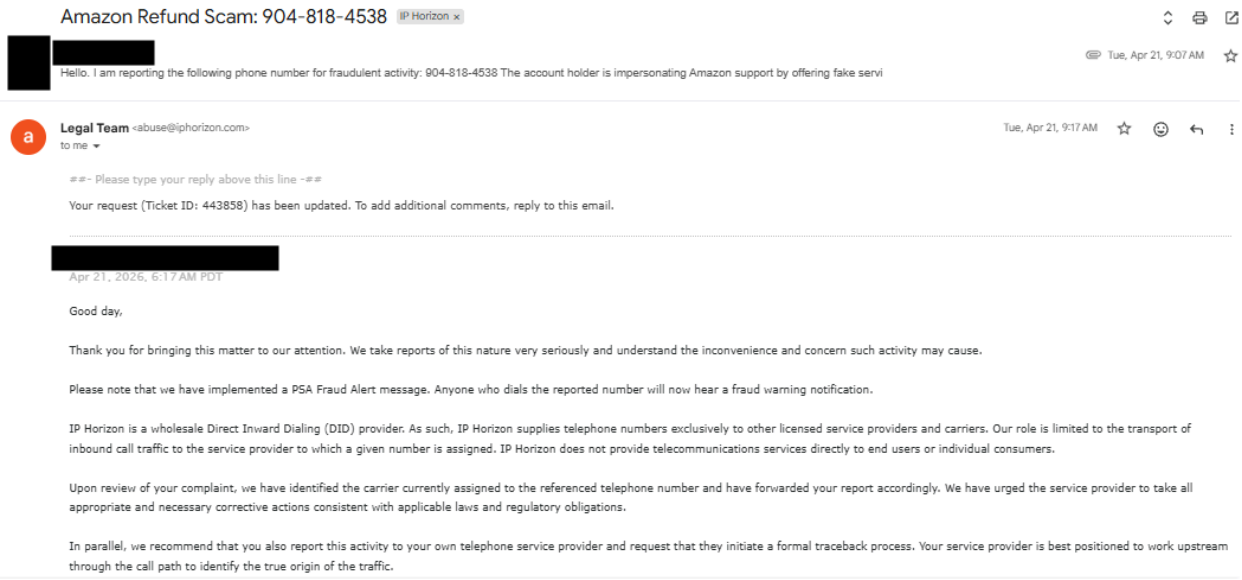


Tue, Apr 21, 2026 8_49 AM_9048184538

Tue, Apr 21, 2026 9_00 AM_out-9048184538

It should be noted that while a robocall may appear to be sufficient evidence on its own, spoofing is rampant and used daily by scammers to send mass robocalls. In this case, the robocall instructed the recipient to call back the number displayed in the caller ID. In some instances, calls of this type use spoofed numbers and instruct the consumer to call a separate number provided only within the recording itself. Demurrage exhausts all verification steps to rule out spoofing and confirm that a number is actively being used in a scam before submitting any report to the relevant telecom.

On April 22, 2026, at 9:17 AM EST, IP Horizon responded, confirming that the number had been blocked and that traffic had been blocked across its network. With the number blocked, neither the scammers nor the wholesale provider made any attempt to dispute the report, and the scammers had no choice but to move on.



Amazon Refund Scam: 904-818-4538 IP Horizon ×

[redacted]

Tue, Apr 21, 9:07 AM

Hello. I am reporting the following phone number for fraudulent activity: 904-818-4538 The account holder is impersonating Amazon support by offering fake servi

Legal Team <abuse@iphorizon.com>
to me

Tue, Apr 21, 9:17 AM

##- Please type your reply above this line -##

Your request (Ticket ID: 443858) has been updated. To add additional comments, reply to this email.

[redacted]
Apr 21, 2026, 6:17 AM PDT

Good day,

Thank you for bringing this matter to our attention. We take reports of this nature very seriously and understand the inconvenience and concern such activity may cause.

Please note that we have implemented a PSA Fraud Alert message. Anyone who dials the reported number will now hear a fraud warning notification.

IP Horizon is a wholesale Direct Inward Dialing (DID) provider. As such, IP Horizon supplies telephone numbers exclusively to other licensed service providers and carriers. Our role is limited to the transport of inbound call traffic to the service provider to which a given number is assigned. IP Horizon does not provide telecommunications services directly to end users or individual consumers.

Upon review of your complaint, we have identified the carrier currently assigned to the referenced telephone number and have forwarded your report accordingly. We have urged the service provider to take all appropriate and necessary corrective actions consistent with applicable laws and regulatory obligations.

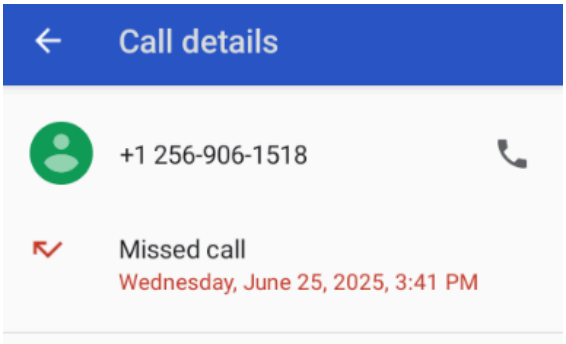
In parallel, we recommend that you also report this activity to your own telephone service provider and request that they initiate a formal traceback process. Your service provider is best positioned to work upstream through the call path to identify the true origin of the traffic.

Total response time for this case was 10 minutes.

Case 3: 256-906-1518

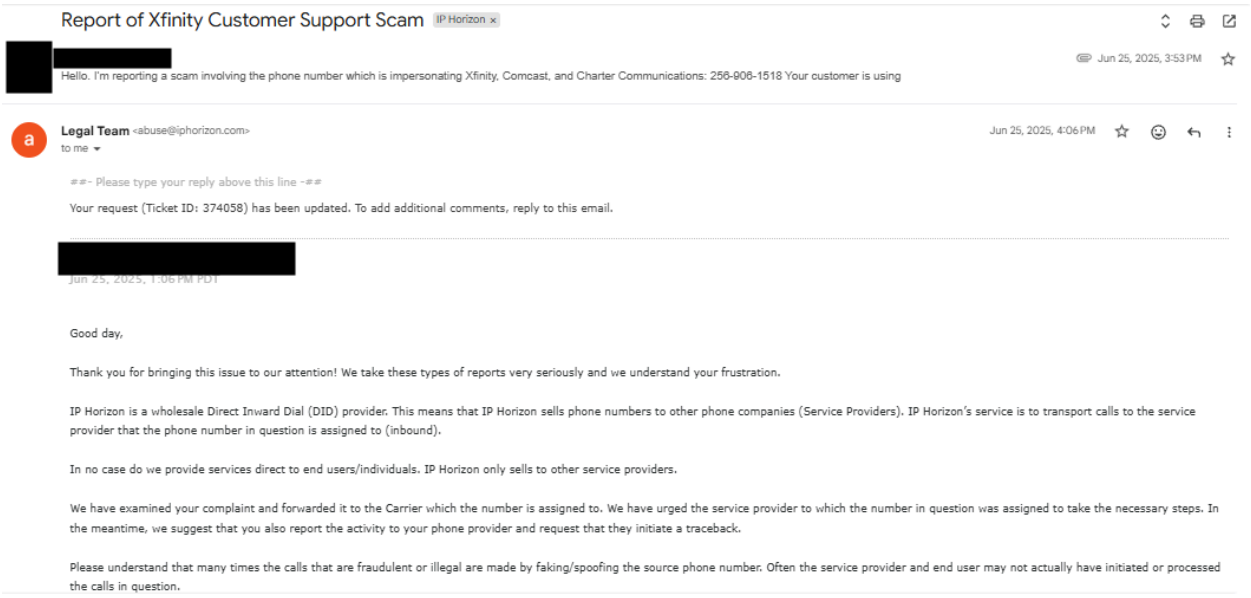
This number was used as a callback number for an Xfinity customer support scam. After a scammer called one of Demurrage's dedicated cell phones, the number was traced back to IP Horizon. Demurrage called the number back to verify that it was active and being used by a scammer, then submitted a report to IP Horizon on June 25, 2025, at 3:53 PM EST.

The report included a recording of a scammer answering the reported number through an impersonated Xfinity menu and identifying as Xfinity support, along with a screenshot of the call history from the dedicated cell phone.



Wed, Jun 25, 2025 3_43 PM_out_2569061518

On June 25, 2025, at 4:06 PM EST, IP Horizon responded, confirming that the report had been received and forwarded to their carrier for investigation. Although IP Horizon did not explicitly state that the number had been blocked, Demurrage confirmed upon calling the number back that it was no longer active. Neither the scammers nor the carrier contested the report, and the scammers were forced to move on.


Report of Xfinity Customer Support Scam IP Horizon ×

[redacted]

Jun 25, 2025, 3:53 PM

Hello. I'm reporting a scam involving the phone number which is impersonating Xfinity, Comcast, and Charter Communications: 256-906-1518 Your customer is using

Legal Team <abuse@iphorizon.com>
to me

Jun 25, 2025, 4:06 PM

##- Please type your reply above this line -##

Your request (Ticket ID: 374058) has been updated. To add additional comments, reply to this email.

[redacted]

Jun 25, 2025, 1:06 PM PDT

Good day,

Thank you for bringing this issue to our attention! We take these types of reports very seriously and we understand your frustration.

IP Horizon is a wholesale Direct Inward Dial (DID) provider. This means that IP Horizon sells phone numbers to other phone companies (Service Providers). IP Horizon's service is to transport calls to the service provider that the phone number in question is assigned to (inbound).

In no case do we provide services direct to end users/individuals. IP Horizon only sells to other service providers.

We have examined your complaint and forwarded it to the Carrier which the number is assigned to. We have urged the service provider to which the number in question was assigned to take the necessary steps. In the meantime, we suggest that you also report the activity to your phone provider and request that they initiate a traceback.

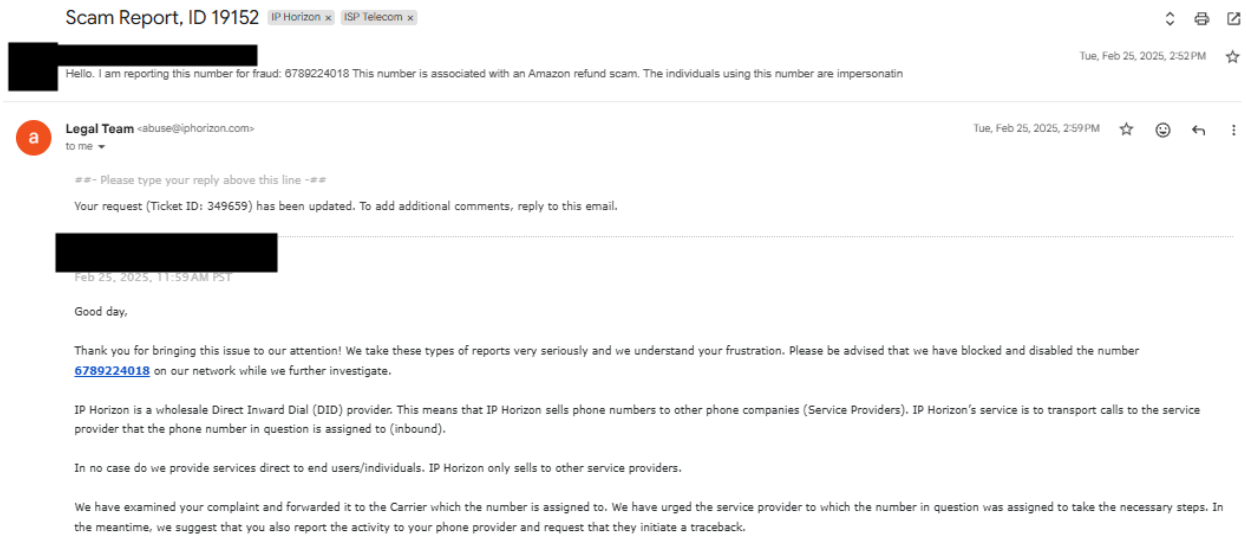
Please understand that many times the calls that are fraudulent or illegal are made by faking/spoofing the source phone number. Often the service provider and end user may not actually have initiated or processed the calls in question.

Total response time for this case was 13 minutes.

Case 4: 678-922-4018

This number was used as a callback number for an Amazon refund scam and was submitted to Demurrage by a third party. Demurrage called the number back to verify that it was active and being used by a scammer, then submitted a report to IP Horizon on February 25, 2025, at 2:52 PM EST.

On February 25, 2025, at 2:59 PM EST, IP Horizon responded confirming that the reported number had been blocked and that the report had been forwarded to their carrier for investigation. Neither the scammers nor the carrier contested the report, and the scammers were forced to move on.



Scam Report, ID 19152 IP Horizon × ISP Telecom ×

[redacted]

Tue, Feb 25, 2025, 2:52 PM

Hello. I am reporting this number for fraud: 6789224018 This number is associated with an Amazon refund scam. The individuals using this number are impersonatin

Legal Team <abuse@iphorizon.com>

to me

Tue, Feb 25, 2025, 2:59 PM

##- Please type your reply above this line -##

Your request (Ticket ID: 349659) has been updated. To add additional comments, reply to this email.

[redacted]

Feb 25, 2025, 11:59 AM PST

Good day,

Thank you for bringing this issue to our attention! We take these types of reports very seriously and we understand your frustration. Please be advised that we have blocked and disabled the number 6789224018 on our network while we further investigate.

IP Horizon is a wholesale Direct Inward Dial (DID) provider. This means that IP Horizon sells phone numbers to other phone companies (Service Providers). IP Horizon's service is to transport calls to the service provider that the phone number in question is assigned to (inbound).

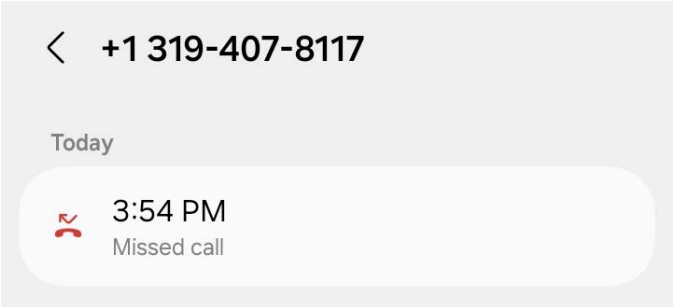
In no case do we provide services direct to end users/individuals. IP Horizon only sells to other service providers.

We have examined your complaint and forwarded it to the Carrier which the number is assigned to. We have urged the service provider to which the number in question was assigned to take the necessary steps. In the meantime, we suggest that you also report the activity to your phone provider and request that they initiate a traceback.

Total response time for this case was 7 minutes.

Case 5: 319-407-8117

This number was used as a callback number for an Amazon refund scam that called one of the dedicated Demurrage cell phone numbers.

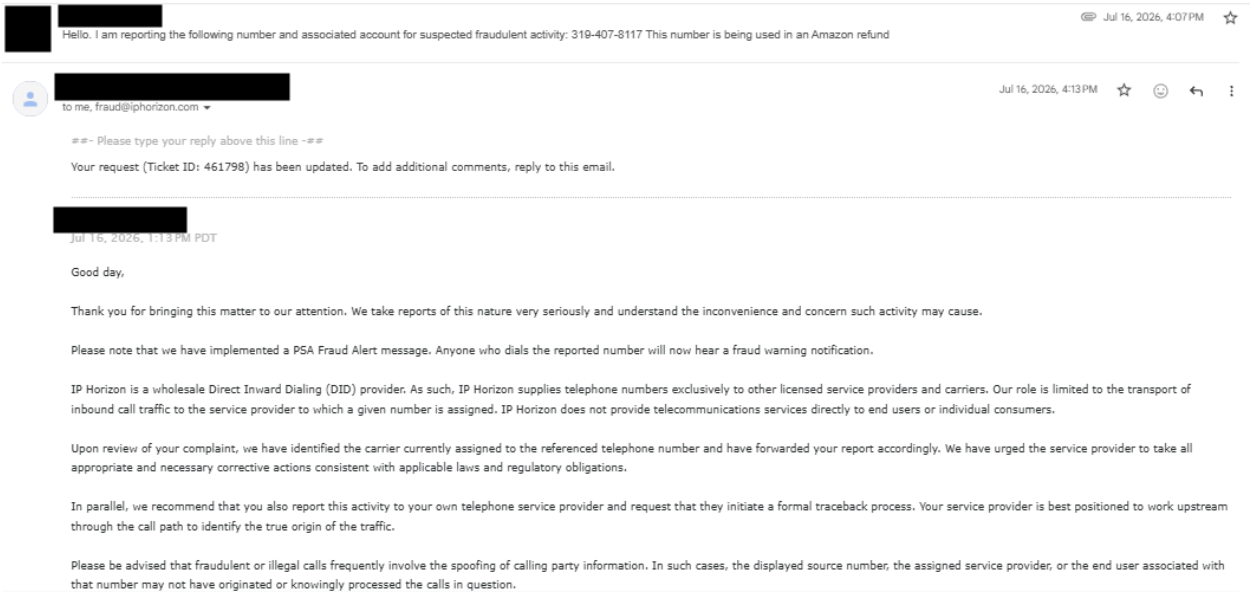


Demurrage called the number back to verify that it was active and being used by a scammer, and upon further investigation confirmed that it also traced back to the wholesale carrier Call48. Demurrage then submitted a report to IP Horizon on July 16, 2026, at 4:07 PM EST.

The report included a screenshot of the initial call made by the scammer to our dedicated cell phone along with a recording of the scammer answering the phone, claiming to be “Amazon customer service”

Thu, Jul 16, 2026 4_02 PM_out-31940781172

On July 16, 2026, at 4:13 PM EST, IP Horizon responded confirming that the reported number had been blocked and that the report had been forwarded to their carrier for investigation. In addition, IP Horizon implemented a public service announcement informing any consumer who attempts to call the number that it has been reported for suspicious activity. Neither the scammers nor the carrier contested the report once the block was in place, and the scammers were forced to move on.



[redacted] Jul 16, 2026, 4:07 PM

Hello. I am reporting the following number and associated account for suspected fraudulent activity: 319-407-8117 This number is being used in an Amazon refund

[redacted] Jul 16, 2026, 4:13 PM

to me, fraud@iphorizon.com

##- Please type your reply above this line -##

Your request (Ticket ID: 461798) has been updated. To add additional comments, reply to this email.

[redacted]

Jul 16, 2026, 1:13 PM PDT

Good day,

Thank you for bringing this matter to our attention. We take reports of this nature very seriously and understand the inconvenience and concern such activity may cause.

Please note that we have implemented a PSA Fraud Alert message. Anyone who dials the reported number will now hear a fraud warning notification.

IP Horizon is a wholesale Direct Inward Dialing (DID) provider. As such, IP Horizon supplies telephone numbers exclusively to other licensed service providers and carriers. Our role is limited to the transport of inbound call traffic to the service provider to which a given number is assigned. IP Horizon does not provide telecommunications services directly to end users or individual consumers.

Upon review of your complaint, we have identified the carrier currently assigned to the referenced telephone number and have forwarded your report accordingly. We have urged the service provider to take all appropriate and necessary corrective actions consistent with applicable laws and regulatory obligations.

In parallel, we recommend that you also report this activity to your own telephone service provider and request that they initiate a formal traceback process. Your service provider is best positioned to work upstream through the call path to identify the true origin of the traffic.

Please be advised that fraudulent or illegal calls frequently involve the spoofing of calling party information. In such cases, the displayed source number, the assigned service provider, or the end user associated with that number may not have originated or knowingly processed the calls in question.

Total response time for this case was 6 minutes, tying Lumen's record for the fastest takedown documented by Demurrage.

Closing Statements

The data confirms that several major VoIP providers in the United States have the ability to directly intervene and shut down phone numbers on their networks for fraud, regardless of which wholesale provider or carrier is responsible for the sale or which customer owns the number. However, some choose not to do so.

If telecoms are serious about complying with FTC and FCC standards, they must adopt and implement the practices demonstrated by Lumen and IP Horizon. No telecom should permit its wholesale providers to stall or lie about the outcomes of fraud reports. No telecom should disregard submitted evidence in favor of deferring to its wholesale provider on the grounds that the reported number does not directly belong to the telecom, particularly when all calls are being carried over that telecom's own infrastructure.

In the cases of Google Voice and Microsoft Teams, it is ludicrous that consumers must go through Bandwidth and Sinch to report numbers used in fraud. Corporations this

large would be expected to maintain their own dedicated systems and contact channels for fraud reporting. Requiring consumers to navigate through a wholesale carrier such as Bandwidth or Sinch is not only tediously difficult but also counterproductive. These are issues that Microsoft and Google must address directly, particularly given that Bandwidth and Sinch have demonstrated a consistent pattern of disregarding submitted evidence, or a refusal to communicate with the individuals who submitted the complaint. This represents a direct failure on the part of both companies, and that goes double for Microsoft, given that Skype numbers previously had to be reported through either Bandwidth or Lumen.

Google Voice remains one of the most abused services in this industry, and Google has shown little to no interest in addressing this, as it is effectively impossible to contact Google directly regarding fraud committed through its services. Bandwidth's handling of such reports is equally ineffective.

Bandwidth and Sinch appear not to recognize that the reason they have previously been fined by the FTC and FCC is that all reported numbers trace back to their networks and infrastructure. It is Bandwidth and Sinch who bear responsibility, not the marks or their wholesale providers. These two VoIP providers carry the greatest volume of numbers linked to illegal call centers in India and Pakistan, a consequence of both their reliance on marks and the inadequate regulatory standards they maintain.

Bandwidth and Sinch's policies only serve to enable marks to continuously abuse their networks. Sinch's reputation is near universally poor among even basic consumers familiar with Onvoy, and Bandwidth's reputation fares no better. Despite claims that Bandwidth is implementing tools such as AI-based screening, these measures do little to hold their wholesale providers and marks accountable for the ongoing sale of numbers to overseas scammers and the misrepresentations that accompany it.

It is time to recognize that the answer to this problem lies within the telecoms themselves. Their customers and wholesale providers are the source of the problem, and this is no longer a matter of speculation but of documented fact.

Telecoms must remove marks from their networks, and while some are already doing so, it is not happening fast enough. Stricter requirements for becoming a wholesale provider need to be established, and telecoms must maintain accountability over their wholesale partners. Until this issue is acknowledged and addressed by all major telecoms and their governing bodies in the United States, it will persist.

Investment in Artificial Intelligence will not solve this problem. It will only make it worse.

Demurrage will continue its efforts to report as many scam numbers as possible. In an ideal world, however, Demurrage would not need to exist, as the governing bodies responsible for protecting consumers would have this issue under control.

The next move belongs to those governing bodies, and Demurrage will be watching.

Email Records: Sinch

Demurrage Archives_ Email Records For Sinch .pdf

Demurrage Archives_ Email Records For Sinch Continued (Onvoy).pdf

Email Records: Bandwidth

Demurrage Archives_ Email Records Bandwidth.pdf

Email Records: Lumen

Demurrage Archives: Email Records For Lumen

Email Records: IP Horizon

Demurrage Archives: Email Records For IP Horizon