Review of Ring Central Fraud Controls.

March 10, 2026

By the Demurrage Team

Contents

Introduction 03

The Investigation - Part 1: Toll-Free Numbers & Contacting RingCentral… 17
Statistics 17
Case #1: Citibank Refund Scam 18
Case #2: Coinbase Technical Support Scam 19
Case #3: Microsoft Technical Support Scam 20
Case #4: Bitcoin Technical Support Scam 22
Case #5: Computer Technical Support Scam 23
Case #6 & #7: Canon Printer Technical Support Scams 24
Case #8: Citibank Refund Scam 25
Case #9: Citibank Refund Scam 26
Case #10: Microsoft Technical Support Scam 27
Case #11: Microsoft Technical Support Scam 28
Case #12: Coinbase Technical Support Scam 29
Case #13, #14, #15: HP/Canon Printer Technical Support Scam 30
Case #16, #17, #18, #19: HP Printer Technical Support Scam 31
Case #20: HP Printer Technical Support Scam 33

The Investigation - Part 2: The Toll-Free / NonToll-Free Number Connection 34
Timeline 34
Scam Invoices, the Impersonation of… 37
Testimony By AVAHS 41
Non Toll-Free Residential Numbers… 42
Case 1: 651-815-4469 43
Case 2: 203-205-9355 49
Case 3: 813-725-5534 51
The Most Responsible Telecom In The Industry… 54
Case 4: 518-631-3721 54
Case 5 & 6: 818-230-2770, 858-529-8920 56
Case 7: 669-900-1947 (Microsoft Technical Support Scam) 57
Case 8: 626-737-3976 (Microsoft Technical Support Scam) 57
Case 9: 424-704-5986 (Computer Technical Support Scam) 59

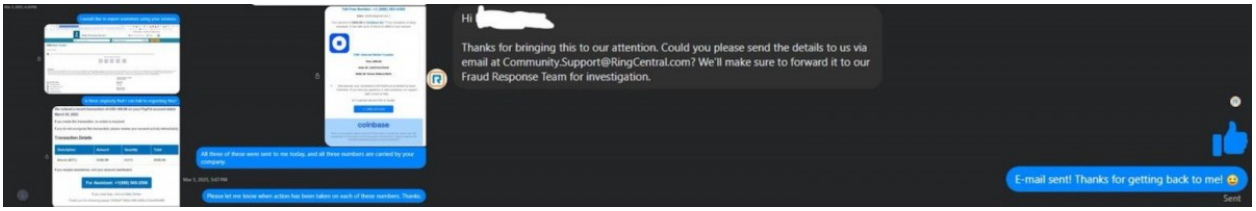
Closing Statements 60
Glossary 62

Introduction

This document is a continuation of a report published on March 28, 2025, in which the Demurrage team examined measures taken by RingCentral to address phone fraud occurring on its network.

The previous report documented 23 cases of toll-free numbers used in tech support fraud by overseas scammers operating primarily from illegal call centers in India.

Reports were submitted to RingCentral's fraud department at ***Community.Support@ringcentral.com***, an address provided to Demurrage by a RingCentral support agent via Facebook Messenger.



Of the 23 cases submitted, only 2 received any response, each acknowledging that the report had been forwarded to the fraud team. No further updates were provided on either case, and the remaining 21 received no response at all.

None of the 23 cases were ever confirmed by RingCentral as having been shut down for fraud. While several numbers appear to have been shut down, it remains unclear whether this was the result of RingCentral's intervention or whether the scammers simply moved on to new toll-free numbers, either on RingCentral or with other VoIP providers.

The Difference Between Robocalls and DIDs Used in Tech Support Fraud

Before proceeding, it should be noted that this report, along with the previous two reports, does not involve robocalls. While Demurrage understands that robocalls are a problem heavily focused on by governing bodies such as the FCC and FTC, the cases presented involve the use of DIDs (VoIP numbers) such as toll-free and non-toll-free numbers, as well as prepaid SIM residential numbers, being used to commit tech support fraud.

In this type of fraud, scammers set up campaigns with the goal of making the consumer call them. While scammers may call victims back, they do so manually rather than using bots or machines to initiate automated robocalls

Robocall laws and tactics used to combat them have no effect on tech support fraud, where a consumer receives a text or email impersonating PayPal or Apple claiming that an unpaid invoice is due and one must call the listed phone number to dispute the charge.

These tactics also have no effect on the many pop-up scams impersonating Microsoft on the internet, claiming that one's personal device has been infected with a virus and one must call the toll-free number for bogus tech support.

Timeline & Migration Patterns

Following the publication of the previous report, Demurrage continued to identify toll-free numbers on the RingCentral network being used for tech support fraud throughout the remainder of 2024.

Beginning in May 2025, a steady decline in activity became apparent, with only two toll-free numbers linked to RingCentral identified that month. This trend persisted through December 2025, when just two toll-free numbers tied to similar scams were again traced back to the network.

In January 2026, a third wave of RingCentral-linked toll-free numbers emerged with notable changes in volume: 8 numbers were identified in January, followed by 6 in February.

All of these toll-free numbers were once again linked to fraudsters operating out of illegal call centers in India.

A complete history of toll-free numbers used by scammers on the RingCentral network is available in the accompanying spreadsheet at:

- https://drive.google.com/file/d/1KEyhCYMGqHmSsXRI_U-h1hnDdD8NIlzg/view

Disclaimer & Concerns

While Demurrage recognizes that SOMOS deals strictly with the distribution of U.S. toll-free numbers, it is important to note that RingCentral's lack of action against scammers abusing its network has been consistent regardless of whether toll-free or non-toll-free numbers are involved. This is now the third report in three years documenting this pattern, with the previous two focused exclusively on toll-free number data. Notably, this inaction extends beyond RingCentral's own toll-free inventory.

Unlike toll-free numbers, which RingCentral owns directly, the residential numbers on its network are supplied by three different carriers. This lack of action has been documented with at least one of those carriers, while another remains difficult to assess due to its longstanding refusal to communicate with complainants.

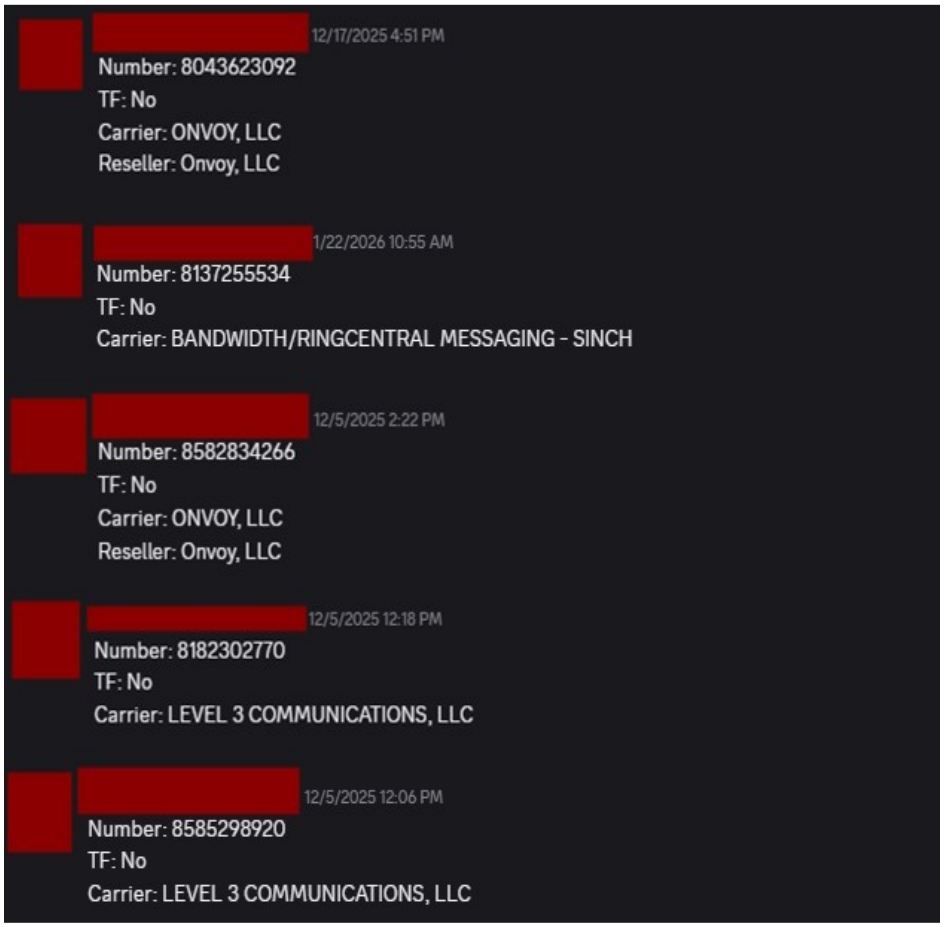
This will be examined further in the sections that follow, but it must be stated that this is a consistent problem across multiple aspects of the RingCentral network.

Residential Numbers Over Toll-Free Numbers

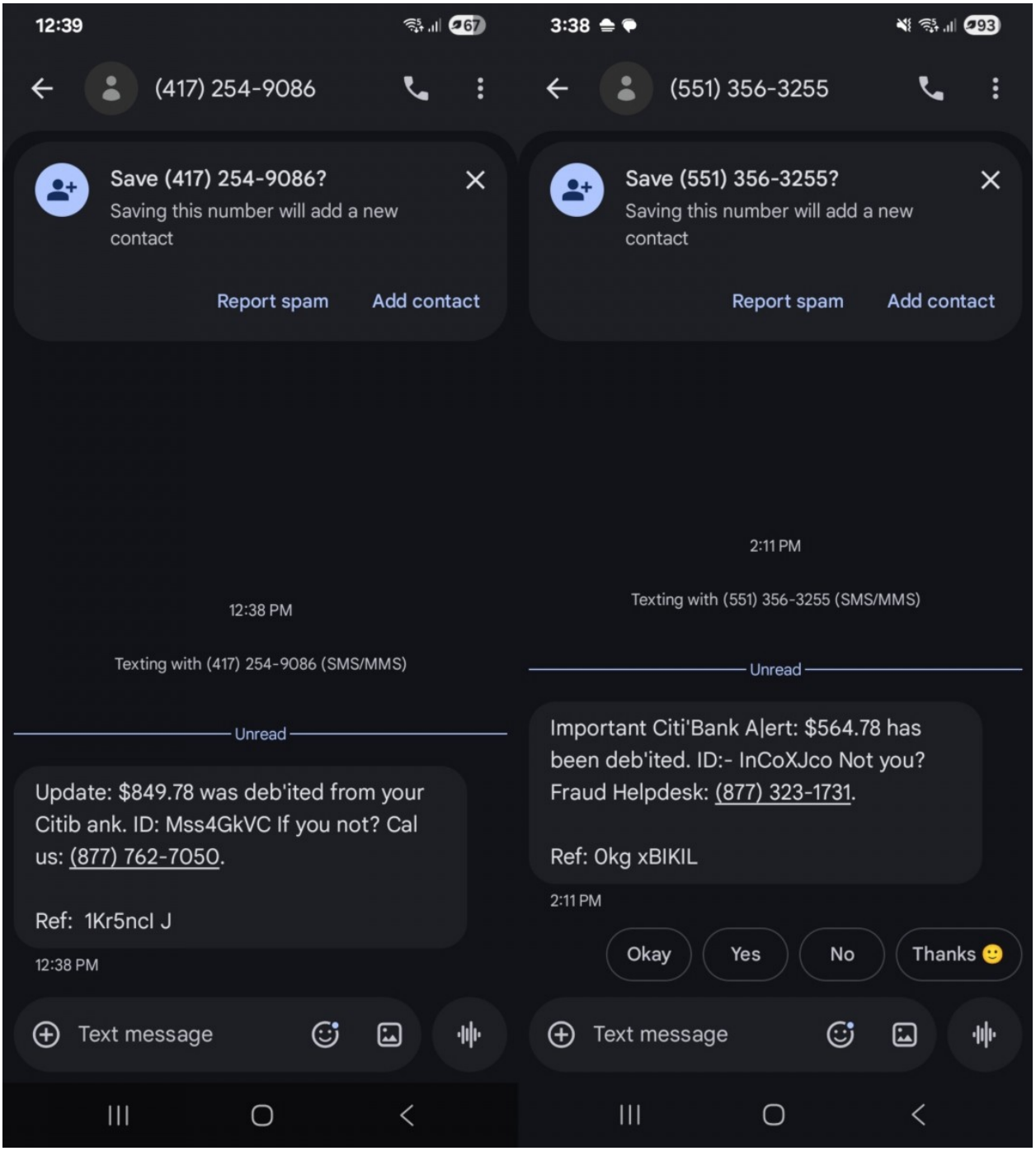
In mid-2025, Demurrage began observing a shift in scammer behavior, with more call centers moving away from toll-free numbers in favor of non-toll-free U.S. residential numbers, particularly those with 805 area codes.

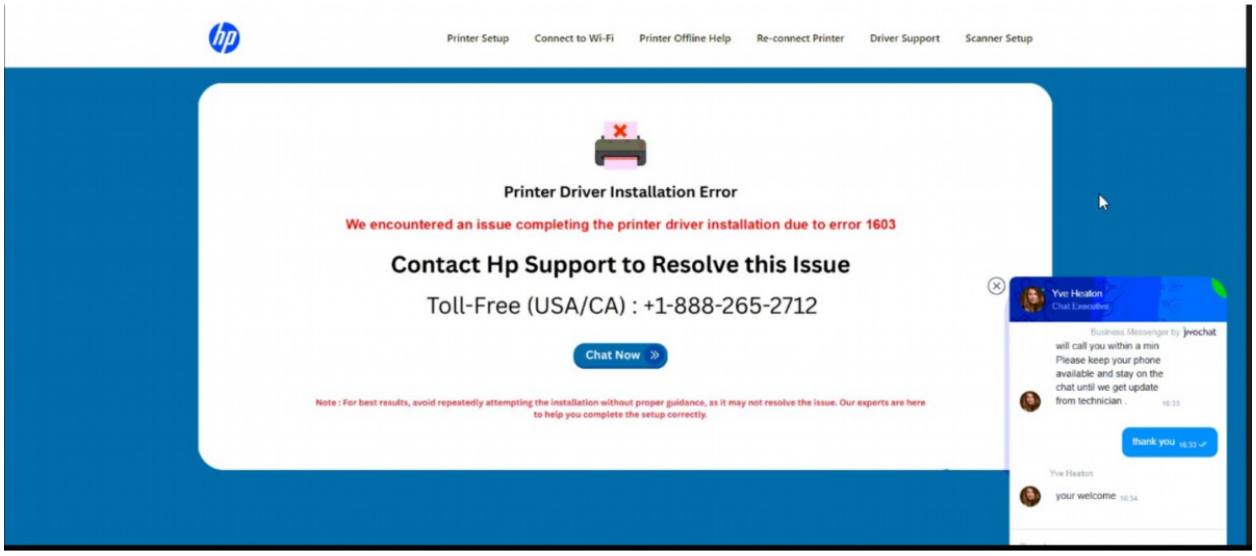
The 805 or similar area codes are often presented as "toll-free" numbers in certain scam invoices linked to refund scams, as they appear similar to the toll-free format. This shift coincided with a broader rise in the abuse of T-Mobile prepaid numbers and SIMs, which eventually overtook toll-free numbers as the primary choice for tech support fraud.

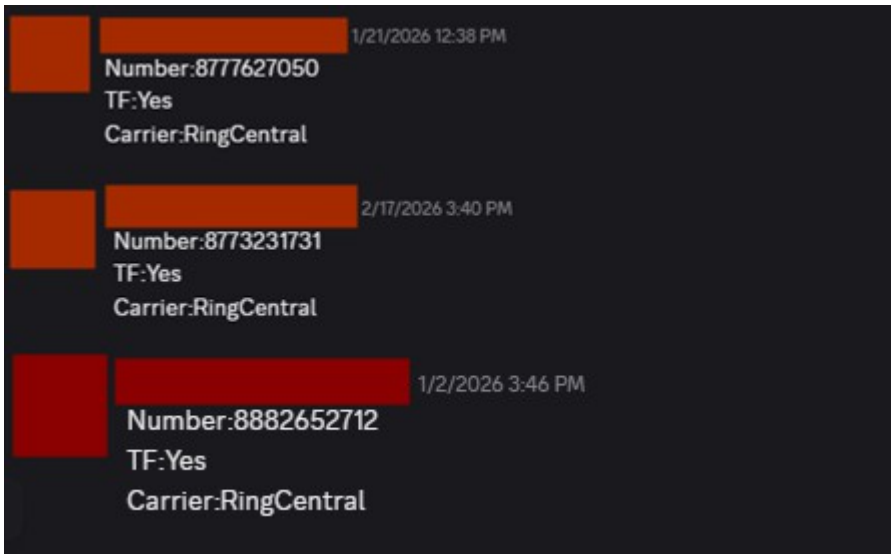
Scammers then transitioned further to non-toll-free residential numbers on other VoIP providers, namely Microsoft Teams numbers via Sinch and similar numbers on RingCentral through three different telecom networks: Lumen (through its Level 3 network), Sinch, and Bandwidth, provided SMS services are enabled on those non-toll-free residential numbers.



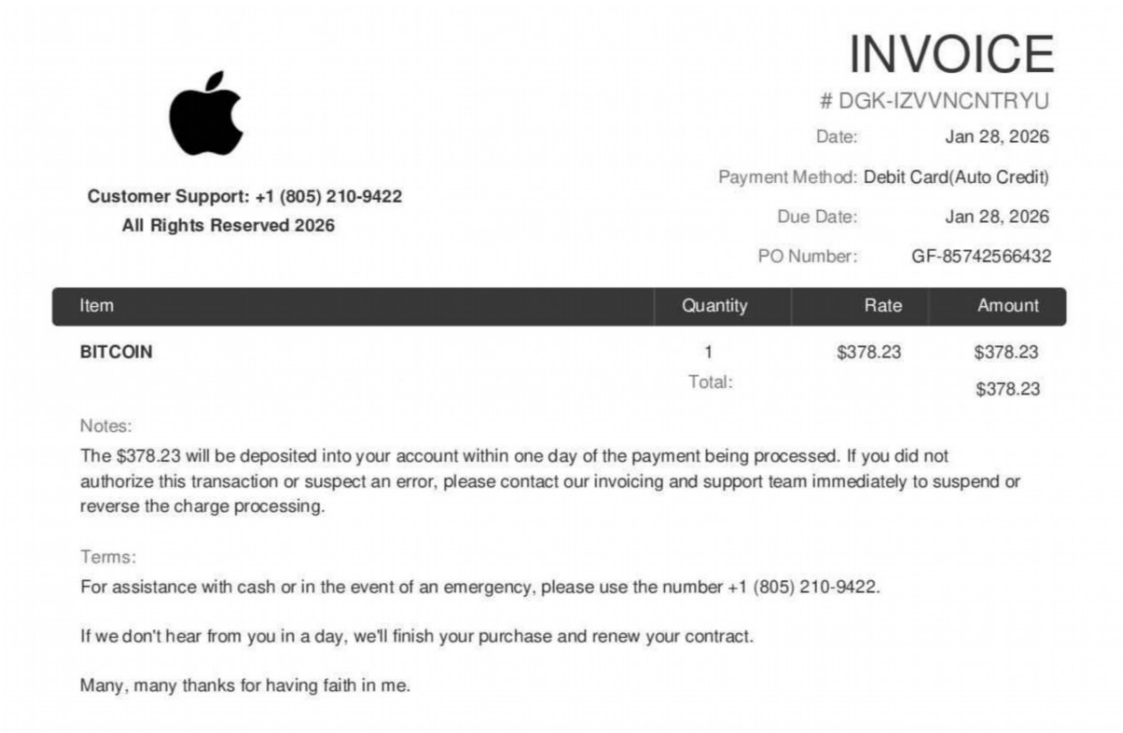
Demurrage also concludes that data pertaining to current toll-free numbers on RingCentral linked with tech support fraud shows they are used for printer technical support and Citibank or similar refund related scams.


12:39
(417) 254-9086
Save (417) 254-9086?
Saving this number will add a new contact
Report spam
Add contact
12:38 PM
Texting with (417) 254-9086 (SMS/MMS)
Unread
Update: $849.78 was deb'ited from your Citib ank. ID: Mss4GkVC If you not? Cal us: (877) 762-7050.
Ref: 1Kr5ncl J
12:38 PM
Text message
3:38
(551) 356-3255
Save (551) 356-3255?
Saving this number will add a new contact
Report spam
Add contact
2:11 PM
Texting with (551) 356-3255 (SMS/MMS)
Unread
Important Citi'Bank A|ert: $564.78 has been deb'ited. ID:- InCoXJco Not you? Fraud Helpdesk: (877) 323-1731.
Ref: 0kg xBIKIL
2:11 PM
Okay
Yes
No
Thanks
Text message


Printer Setup
Connect to Wi-Fi
Printer Offline Help
Re-connect Printer
Driver Support
Scanner Setup
Printer Driver Installation Error
We encountered an issue completing the printer driver installation due to error 1603
Contact Hp Support to Resolve this Issue
Toll-Free (USA/CA) : +1-888-265-2712
Chat Now
Note : For best results, avoid repeatedly attempting the installation without proper guidance, as it may not resolve the issue. Our experts are here to help you complete the setup correctly.
Yve Heaton
Chat Executive
Business Messenger by jivochat
will call you within a min
Please keep your phone available and stay on the chat until we get update from technician .
thank you
Yve Heaton
your welcome


[redacted] 1/21/2026 12:38 PM
Number:8777627050
TF:Yes
Carrier:RingCentral
[redacted] 2/17/2026 3:40 PM
Number:8773231731
TF:Yes
Carrier:RingCentral
[redacted] 1/2/2026 3:46 PM
Number:8882652712
TF:Yes
Carrier:RingCentral

As of early 2026, the majority of telephone numbers linked to tech support fraud, both VoIP and prepaid, are non-toll-free U.S. residential numbers.



INVOICE

DGK-IZVVNCNTRYU

Date: Jan 28, 2026

Payment Method: Debit Card(Auto Credit)

Due Date: Jan 28, 2026

PO Number: GF-85742566432

Customer Support: +1 (805) 210-9422

All Rights Reserved 2026

Item	Quantity	Rate	Amount
BITCOIN	1	$378.23	$378.23
	Total:		$378.23

Notes:

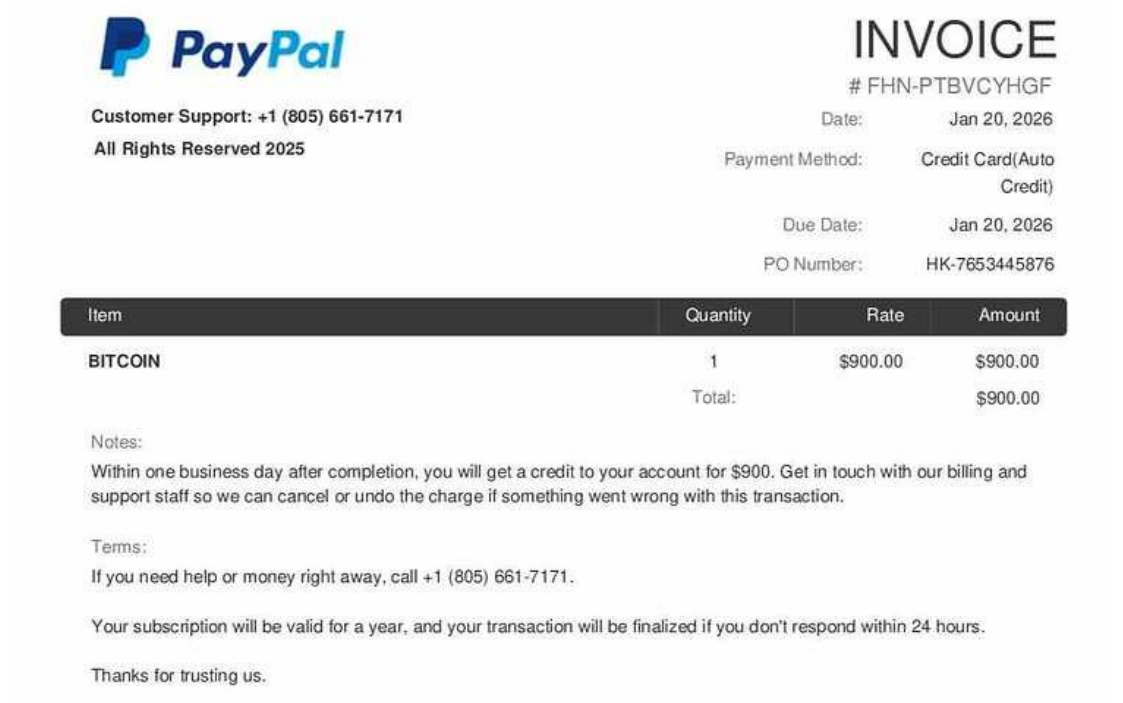
The $378.23 will be deposited into your account within one day of the payment being processed. If you did not authorize this transaction or suspect an error, please contact our invoicing and support team immediately to suspend or reverse the charge processing.

Terms:

For assistance with cash or in the event of an emergency, please use the number +1 (805) 210-9422.

If we don't hear from you in a day, we'll finish your purchase and renew your contract.

Many, many thanks for having faith in me.



PayPal

INVOICE

FHN-PTBVCYHGF

Date: Jan 20, 2026

Payment Method: Credit Card(Auto Credit)

Due Date: Jan 20, 2026

PO Number: HK-7653445876

Customer Support: +1 (805) 661-7171

All Rights Reserved 2025

Item	Quantity	Rate	Amount
BITCOIN	1	$900.00	$900.00
	Total:		$900.00

Notes:

Within one business day after completion, you will get a credit to your account for $900. Get in touch with our billing and support staff so we can cancel or undo the charge if something went wrong with this transaction.

Terms:

If you need help or money right away, call +1 (805) 661-7171.

Your subscription will be valid for a year, and your transaction will be finalized if you don't respond within 24 hours.

Thanks for trusting us.

PayPal

Customer Support: +1 (810) 259-6546

All Rights Reserved 2025

INVOICE

FBE-KJVCETRYYU

Date:	Jan 15, 2026
Payment Method:	Credit Card(Auto Credit)
Due Date:	Jan 15, 2026
PO Number:	VF-76553257543

Item	Quantity	Rate	Amount
iPhone Max Pro	1	$1,599.00	$1,599.00
	Total:		$1,599.00

Notes:

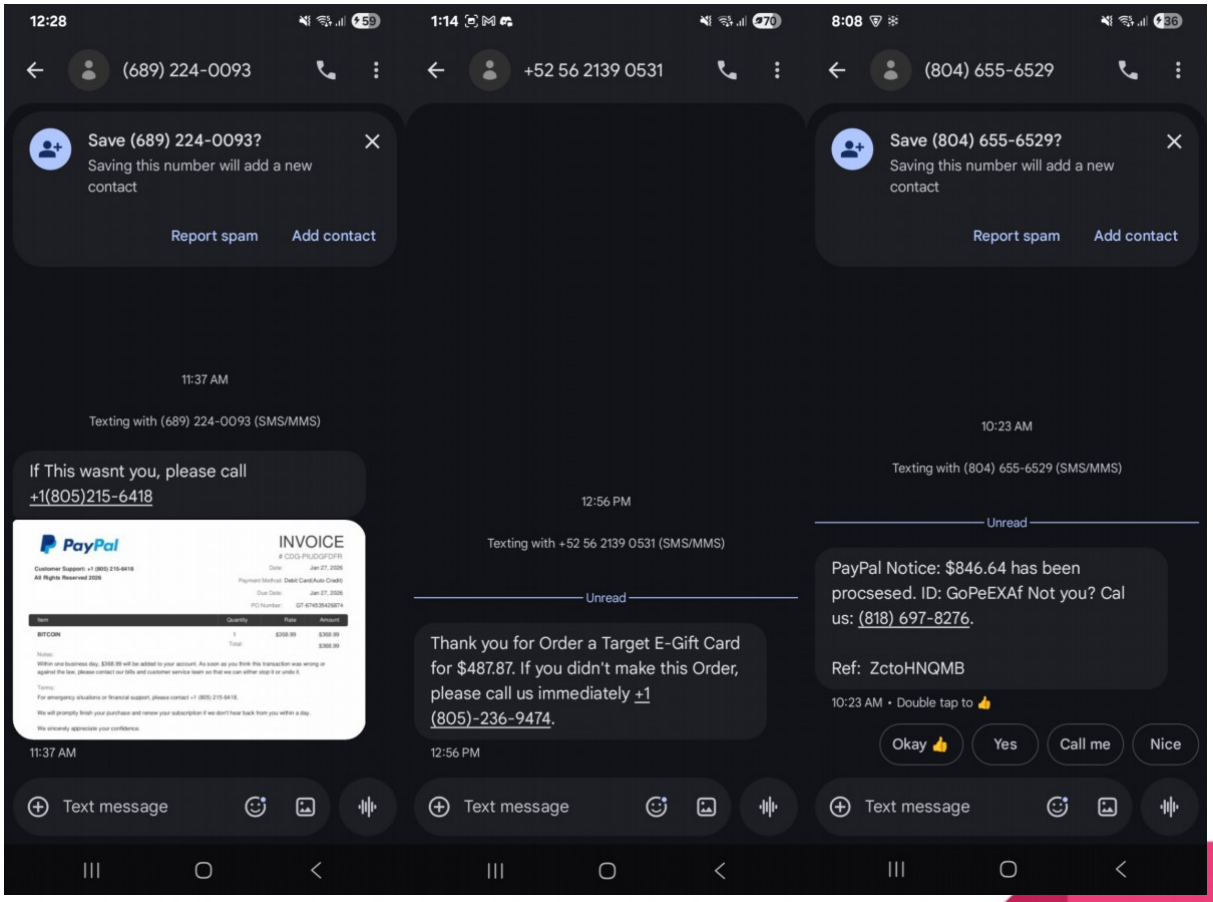
Your $1599 payment is being handled right now. You'll be able to see the changes to your account the next business day. Please get in touch with our billing and support team if you need more information or if you have any concerns about this purchase.

Terms:

For immediate assistance or to request a reimbursement, please contact us at +1 (810) 259-6546

Your purchase will be irrevocable, and your subscription will stay active for one year if you do not respond within 24 hours.

We value your trust in us.

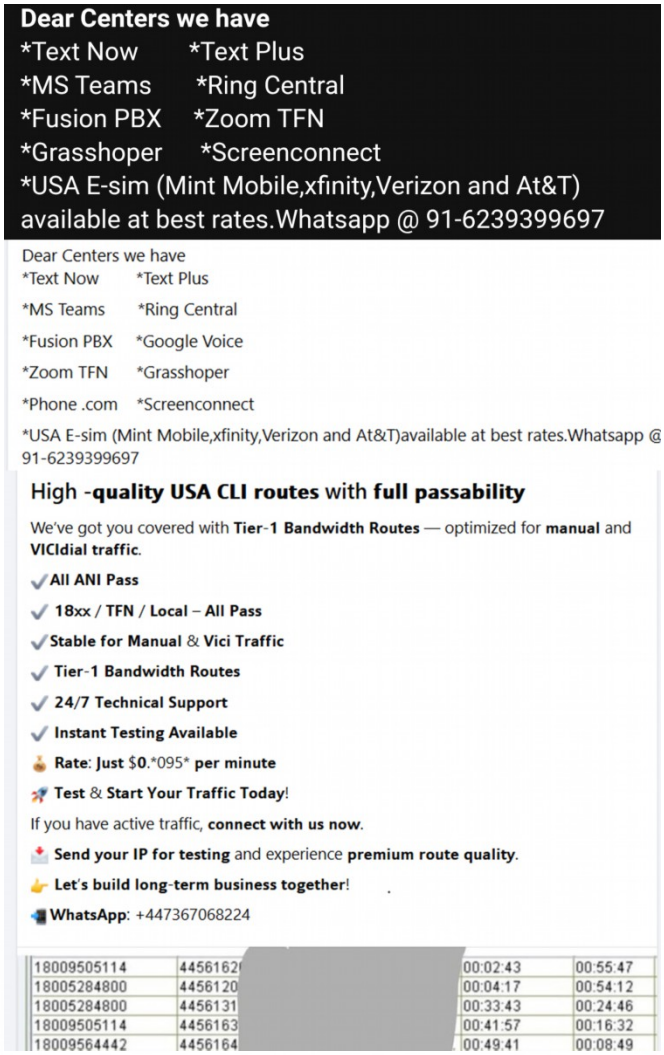


Defeating KYC Through The Use of "Marks"

The sudden switch from toll-free to non-toll-free numbers coincided with VoIP companies implementing stricter KYC policies to combat fraud. Though many telecoms claim to have "robust KYC policies," scammers have already defeated these checks through the use of intermediaries referred to as "marks" by the Demurrage team, along with switching to U.S. non-toll-free residential numbers.

Demurrage defines a "mark" as a complicit wholesaler who exploits telecom reseller programs by selling pre-verified VoIP accounts directly to scammers operating out of illegal call centers in India and elsewhere.

These wholesalers typically operate through Facebook, Telegram, and WhatsApp groups, charging a premium because the buyer is not required to submit any personal information for KYC verification.

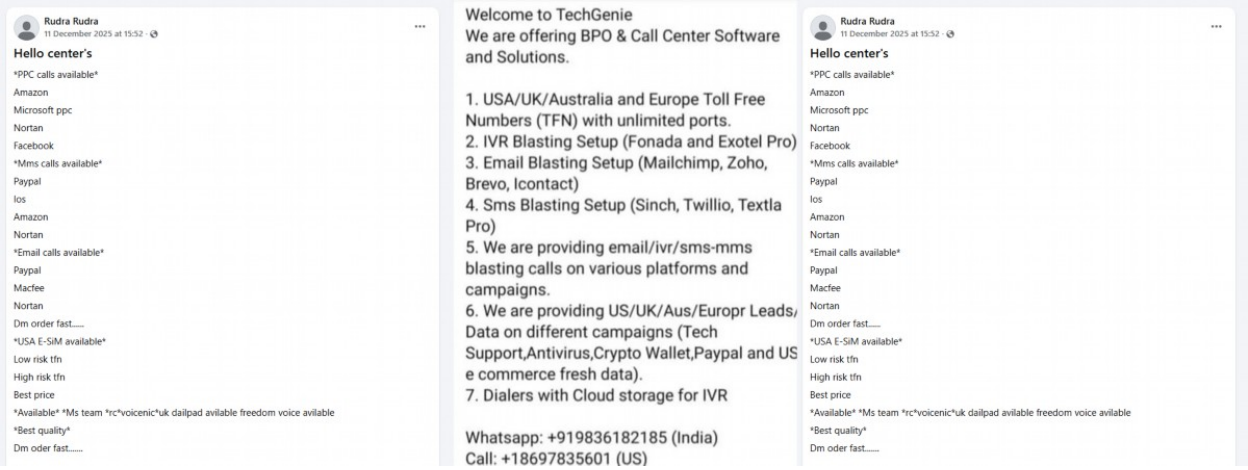


In the case of VoIP numbers, stricter KYC policies, now requiring identification, proof of address, and proof of business through a registered LLC, have pushed scammers toward non-toll-free residential numbers, as they lack the credentials needed to comply.

Residential numbers demand far less, typically only an ID, address, and phone number, as they are designed for the general consumer market.

Some telecoms require video confirmation, but “marks” have also defeated this by supplying that evidence themselves through the use of AI-generated videos or by paying complicit individuals to submit evidence for the scammers. “Marks” create the accounts, allow them to age for a few weeks, and then sell them to scammers for use in tech support fraud.

Though residential numbers are now preferred, the same scheme to bypass KYC checks applies equally to toll-free numbers, an approach some scammers continue to use across various VoIP providers, including RingCentral.



Because Demurrage reports fraudulent numbers to carriers on an ongoing basis, “marks” have adapted by retaining direct control of the accounts themselves, providing scammers only with the login credentials needed to receive calls rather than full account access.

This means that should a report be sent by Demurrage or the average consumer, the report will be forwarded to the “mark” by the telecom that facilitates that number and

traffic through its networks.

This problem is not unique to RingCentral. Multiple telecoms are currently being exploited in the same way. The more pressing concern is not which networks harbor the most “marks”, but how telecoms respond when fraud is reported to them.

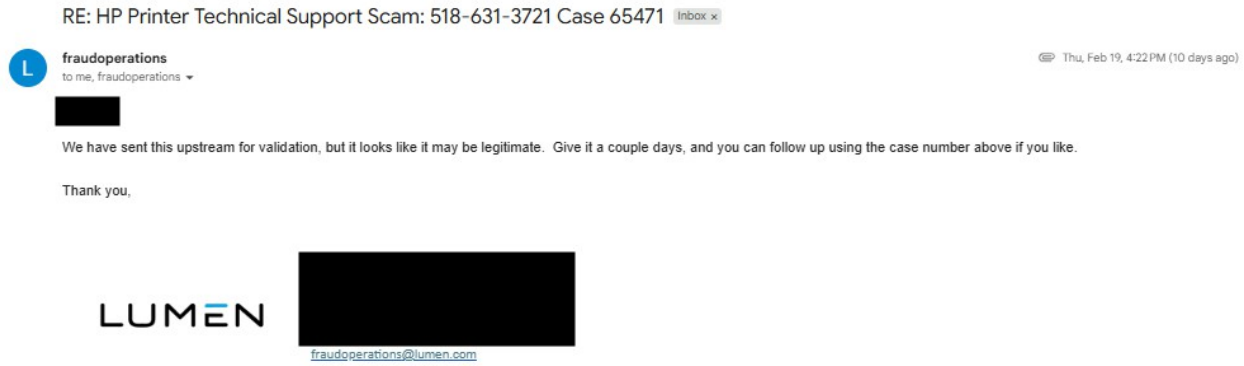
In RingCentral's case, that response has been nearly nonexistent.

Concerning Adaptation Tactics & Telecoms Not Holding “Marks” Accountable

The VoIP accounts created by “marks” have become a growing concern, as they increasingly appear legitimate even to diligent telecoms.

In one notable case, a residential non toll-free VoIP number being used as a callback number by a scammer was traced to RingCentral via Lumen's Level 3 network. A Lumen support agent reviewed the account, determined it appeared legitimate, and was therefore hesitant to apply Lumen's standard fraud response: placing a temporary block on the reported number while forwarding the report to the wholesaler for investigation.

Based on data collected over a six-year period, Demurrage ranks Lumen as the most effective telecom when it comes to removing fraudulent traffic from its network, which is why this specific case has raised severe concerns within the Demurrage team. It suggests that “marks” are rapidly adapting to keep these scam accounts and this market open for the sole purpose of supplying numbers for use in tech support fraud.


RE: HP Printer Technical Support Scam: 518-631-3721 Case 65471 Inbox ×

fraudoperations
to me, fraudoperations

Thu, Feb 19, 4:22 PM (10 days ago)

[redacted]

We have sent this upstream for validation, but it looks like it may be legitimate. Give it a couple days, and you can follow up using the case number above if you like.

Thank you,

LUMEN [redacted]

fraudoperations@lumen.com

The Problem with Telecoms Not Taking Direct Action Against “Marks” & The Fraudulent Traffic On Their Networks

The current response method for dealing with scammers and fraud reports across multiple VoIP providers and telecoms with large infrastructures is to forward the complaint to the wholesaler associated with the account or that sold the account to the person or scammer making and receiving those calls.

Rather than taking direct action themselves, such telecoms expect their wholesalers to be honest and take action against the reported number. In reality, it is becoming increasingly clear that many of these wholesalers are in fact “marks” and have been shown to ignore reports altogether.

Unlike Lumen, which temporarily blocks reported numbers while investigations are pending, providers such as Sinch and Bandwidth typically forward complaints directly to the wholesaler and rely on that wholesaler to investigate, despite all traffic being routed through their own networks and infrastructure.

Neither has demonstrated a willingness to intervene directly by blocking reported numbers from sending or receiving calls. In Sinch's case, the company avoids direct communication of any kind with consumers and complainants alike, a behavior long established and documented by the Demurrage team.

In Bandwidth's case, reports often go unanswered by wholesalers, yet Bandwidth will not hold its wholesalers accountable for ignoring reports. A simple response from the

wholesaler is sufficient for Bandwidth to close the ticket, regardless of content or claims made in the response.

RingCentral normally does not respond at all, regardless of where calls are being routed, something Lumen discovered after stating that its wholesalers, whom it confirmed as customers, were honest and would respond. Those wholesalers ignored the reports for days.

Round 3: Reporting Fraudulent Activity to RingCentral's Fraud Department.

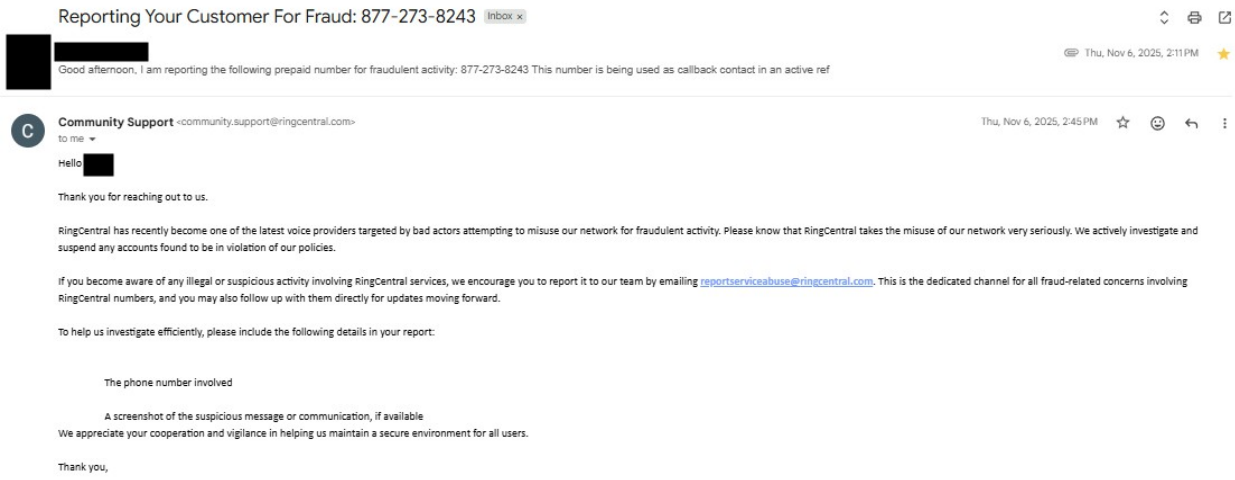
On November 6, 2025, at 2:11 PM, Demurrage again attempted to report a toll-free number linked to RingCentral that was being used in a Citibank refund scam, submitting the report to ***Community.Support@ringcentral.com***, the address previously provided by RingCentral. At 2:45 PM the same day, RingCentral responded and, for the first time, acknowledged the presence of "bad actors" on its network.

> Hello [redacted],
>
> Thank you for reaching out to us.
>
> RingCentral has recently become one of the latest voice providers targeted by bad actors attempting to misuse our network for fraudulent activity. Please know that RingCentral takes the misuse of our network very seriously. We actively investigate and suspend any accounts found to be in violation of our policies.
>
> If you become aware of any illegal or suspicious activity involving RingCentral services, we encourage you to report it to our team by emailing ***reportserviceabuse@ringcentral.com***. This is the dedicated channel for all fraud-related concerns involving RingCentral numbers, and you may also follow up with them directly for updates moving forward.
>
> To help us investigate efficiently, please include the following details in your report:

The phone number involved
A screenshot of the suspicious message or communication, if available

We appreciate your cooperation and vigilance in helping us maintain a secure environment for all users.

Thank you,
Best regards,



Reporting Your Customer For Fraud: 877-273-8243 Inbox ×

[redacted]
Thu, Nov 6, 2025, 2:11 PM
Good afternoon, I am reporting the following prepaid number for fraudulent activity: 877-273-8243 This number is being used as callback contact in an active ref

C **Community Support** <community.support@ringcentral.com>
Thu, Nov 6, 2025, 2:45 PM
to me

Hello [redacted]

Thank you for reaching out to us.

RingCentral has recently become one of the latest voice providers targeted by bad actors attempting to misuse our network for fraudulent activity. Please know that RingCentral takes the misuse of our network very seriously. We actively investigate and suspend any accounts found to be in violation of our policies.

If you become aware of any illegal or suspicious activity involving RingCentral services, we encourage you to report it to our team by emailing reportserviceabuse@ringcentral.com. This is the dedicated channel for all fraud-related concerns involving RingCentral numbers, and you may also follow up with them directly for updates moving forward.

To help us investigate efficiently, please include the following details in your report:

The phone number involved

A screenshot of the suspicious message or communication, if available

We appreciate your cooperation and vigilance in helping us maintain a secure environment for all users.

Thank you,

As previously stated, the majority of emails in the previous two reports went unanswered entirely, yet in this instance a reply was issued within 34 minutes, suggesting that RingCentral is capable of responding to fraud reports in a timely manner but has consistently chosen not to.

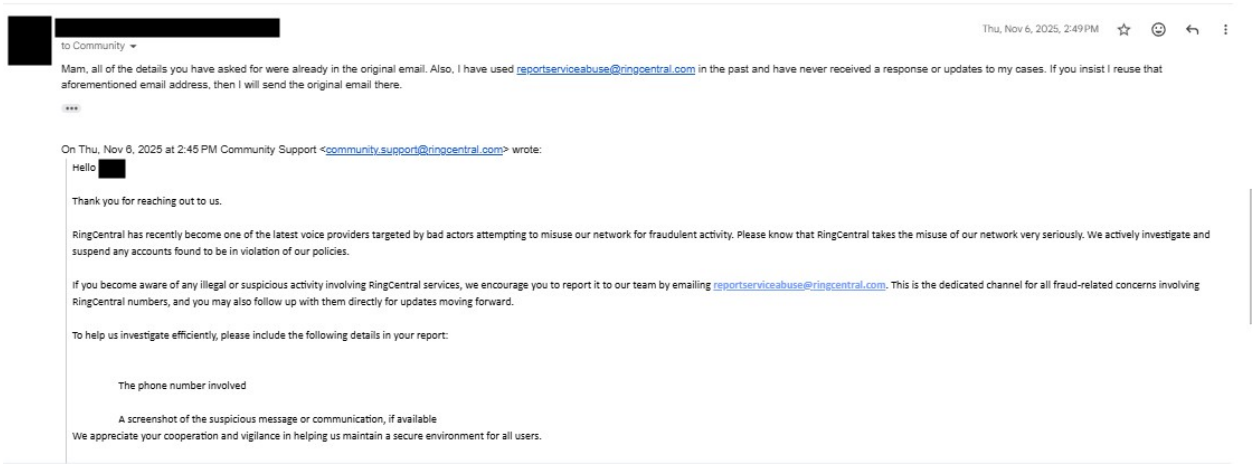
While the response did acknowledge the presence of bad actors on its network, RingCentral directed Demurrage to yet another email address: ***reportserviceabuse@ringcentral.com***, making this the sixth address purportedly dedicated to fraud reporting on RingCentral's network and the fourth provided directly to Demurrage by a RingCentral agent.

The full list of addresses supposedly associated with fraud reporting at RingCentral is as follows:

1. ***fraudresponse@ringcentral.com***
2. ***fraudalert@ringcentral.com***

3. ***serviceabuse@ringcentral.com***
4. ***support@ringcentral.com***
5. ***Community.Support@ringcentral.com***
6. ***reportserviceabuse@ringcentral.com***

Despite Demurrage's original report containing detailed evidence, including two recordings of the scammer answering calls and claiming to represent the "fraud department" at Citibank, along with call timestamps, the agent requested that those details be resubmitted within the same reply chain while simultaneously directing Demurrage to a different email address supposedly dedicated to fraud reports.


[redacted] [redacted] Thu, Nov 6, 2025, 2:49 PM

to Community

Mam, all of the details you have asked for were already in the original email. Also, I have used reportserviceabuse@ringcentral.com in the past and have never received a response or updates to my cases. If you insist I reuse that aforementioned email address, then I will send the original email there.

...

On Thu, Nov 6, 2025 at 2:45 PM Community Support <community.support@ringcentral.com> wrote:

Hello [redacted]

Thank you for reaching out to us.

RingCentral has recently become one of the latest voice providers targeted by bad actors attempting to misuse our network for fraudulent activity. Please know that RingCentral takes the misuse of our network very seriously. We actively investigate and suspend any accounts found to be in violation of our policies.

If you become aware of any illegal or suspicious activity involving RingCentral services, we encourage you to report it to our team by emailing reportserviceabuse@ringcentral.com. This is the dedicated channel for all fraud-related concerns involving RingCentral numbers, and you may also follow up with them directly for updates moving forward.

To help us investigate efficiently, please include the following details in your report:

The phone number involved

A screenshot of the suspicious message or communication, if available

We appreciate your cooperation and vigilance in helping us maintain a secure environment for all users.

Demurrage replied, stating that the requested evidence had already been included in the original email. No further response was received from RingCentral at ***Community.Support@ringcentral.com***, and the case was never updated.

Demurrage used this opportunity to test the newly provided email address, ***reportserviceabuse@ringcentral.com***, beginning the third investigation into RingCentral.

The Investigation - Part 1: Toll-Free Numbers & Contacting RingCentral Directly

For this phase of the investigation, Demurrage reported 20 toll-free numbers confirmed to have been used in tech support fraud directly to RingCentral via ***reportserviceabuse@ringcentral.com***. The following statistics reflect RingCentral's

response, or lack thereof, when contacted directly regarding fraudulent use of its services.

Statistics

Of the 20 emails sent to RingCentral, only 5 reports received any response from RingCentral's fraud team, stating that fraud is taken seriously and that they would investigate the accounts associated with the reported numbers and take action based on their findings. No further updates were provided on the status of these cases.

In 1 case, the Demurrage team followed up after confirming the reported number remained active after three days and was still answering as "support." RingCentral did not respond to this follow-up, leaving the case unresolved.

In 1 case, the mailbox associated with ***reportserviceabuse@ringcentral.com*** was full and returned an error, leaving that case unresolved.

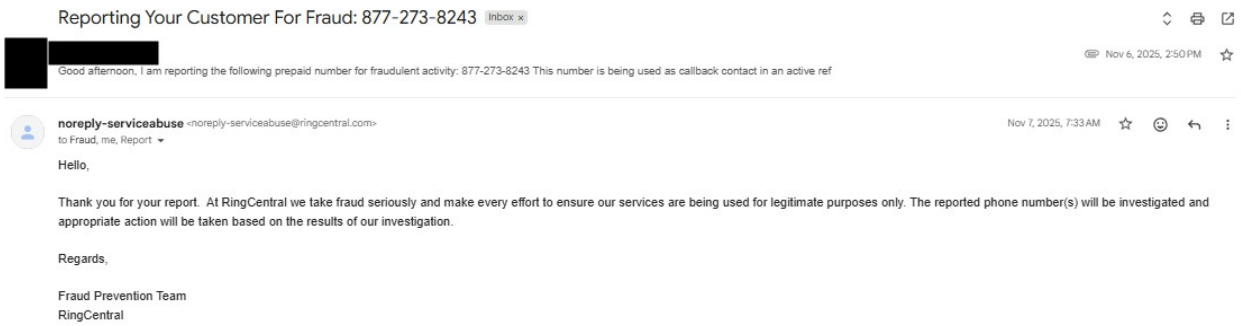
The remaining 14 cases received no replies from RingCentral, not even the standard response mentioned previously.

None of the 20 cases involving toll-free numbers were confirmed to have been shut down for fraud by RingCentral.

Case #1: Citibank Refund Scam

RingCentral responded by stating that it takes fraud seriously and would investigate the reported toll-free number, with appropriate action to follow based on its findings. No further updates were provided, and RingCentral has not disclosed what action, if any, was taken, though the number appears to have since been disconnected.

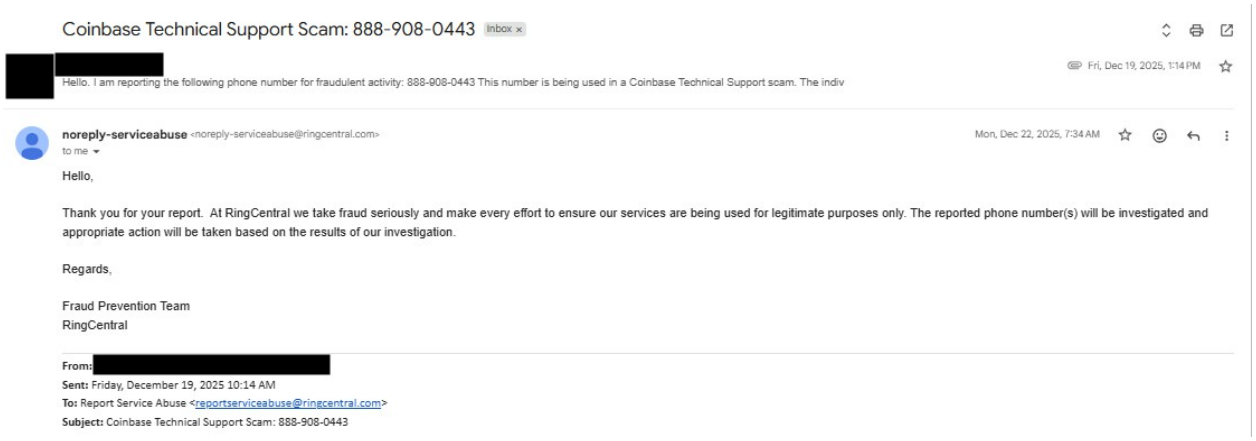
- **Toll-Free Number:** 877-273-8243
- **Recordings:** Yes
    - https://drive.google.com/file/d/1RK2vrCxjZejOh2oDiecpNIR7g45rPHxJ/
    - https://drive.google.com/file/d/1B3b7gdx3rNpfQgZEFUG1bRL0L9Ww2eL_
- **Reported:** Wed, November 6, 2025, 2:50 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** No



Case #2: Coinbase Technical Support Scam

RingCentral responded by stating that it takes fraud seriously and would investigate the reported toll-free number, with appropriate action to follow based on its findings. No further updates were provided, and RingCentral has not disclosed what action, if any, was taken.

- **Toll-Free Number:** 888-908-0443
- **Recordings:** Yes
  - https://drive.google.com/file/d/1ybnjyDIqhkG71Lx7DoacUisAGw63Klkj/
- **Reported:** Fri, December 19, 2025, 1:14 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Call Back)

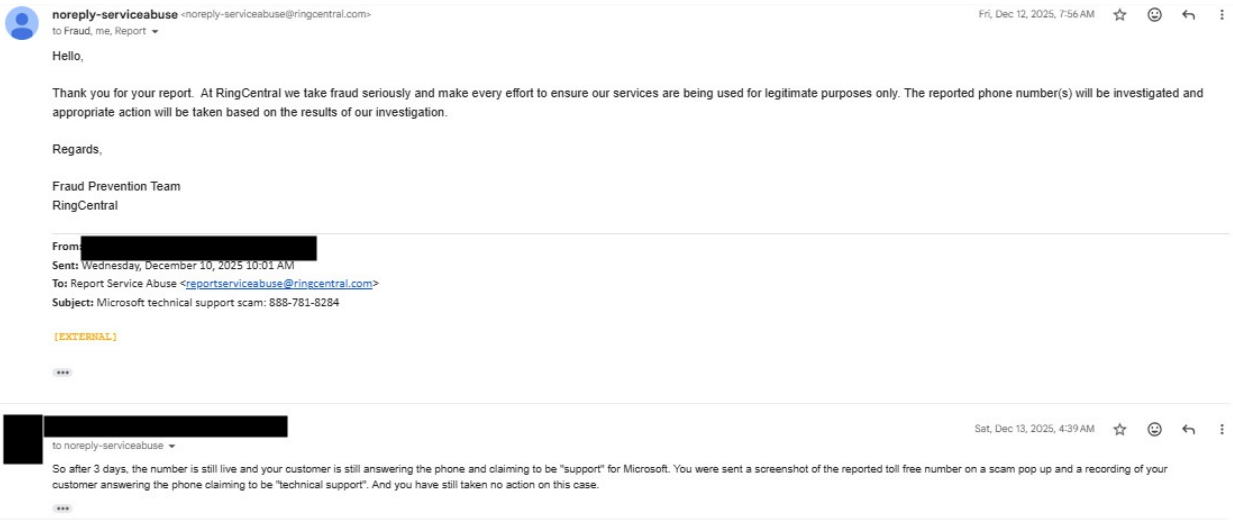




Case #3: Microsoft Technical Support Scam

RingCentral responded by stating that it takes fraud seriously and would investigate the reported toll-free number, with appropriate action to follow based on its findings. However, the number remained active for at least three days after the report was filed, continuing to answer as "support." Demurrage followed up on the original complaint, but no further updates were provided and RingCentral has not disclosed what action, if any, was taken.

- **Toll-Free Number:** 888-781-8284
- **Recordings:** Yes
    - https://drive.google.com/file/d/1_QT9vIT1sBgHiIloF1Kjw3MRjAZz2F9R/
- **Reported:** Wed, December 10, 2025, 1:01 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Pop-Up)



noreply-serviceabuse <noreply-serviceabuse@ringcentral.com> Fri, Dec 12, 2025, 7:56 AM
to Fraud, me, Report

Hello,

Thank you for your report. At RingCentral we take fraud seriously and make every effort to ensure our services are being used for legitimate purposes only. The reported phone number(s) will be investigated and appropriate action will be taken based on the results of our investigation.

Regards,

Fraud Prevention Team
RingCentral

From: [redacted]
Sent: Wednesday, December 10, 2025 10:01 AM
To: Report Service Abuse <reportserviceabuse@ringcentral.com>
Subject: Microsoft technical support scam: 888-781-8284

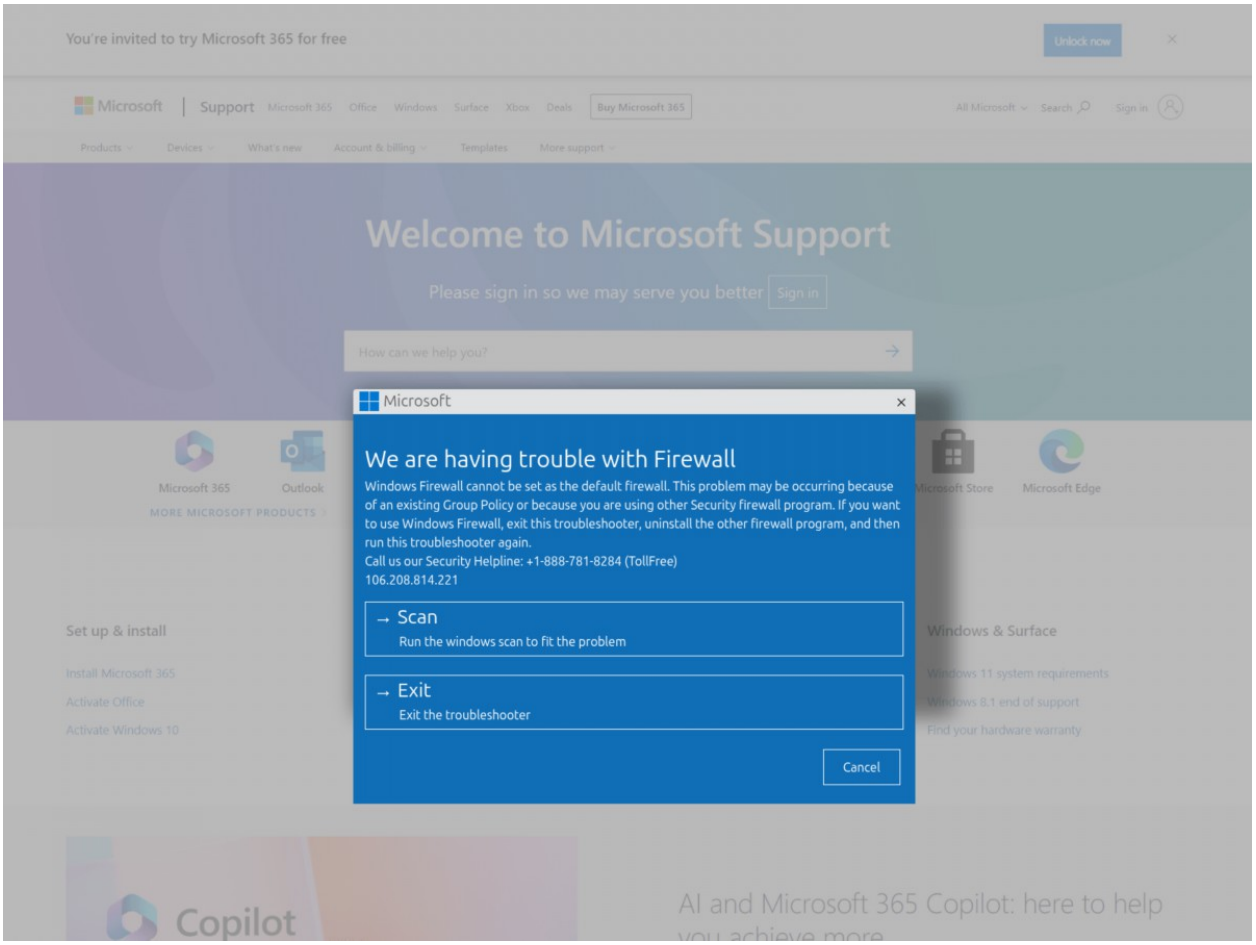
[EXTERNAL]

...

[redacted] Sat, Dec 13, 2025, 4:39 AM
to noreply-serviceabuse

So after 3 days, the number is still live and your customer is still answering the phone and claiming to be "support" for Microsoft. You were sent a screenshot of the reported toll free number on a scam pop up and a recording of your customer answering the phone claiming to be "technical support". And you have still taken no action on this case.

...

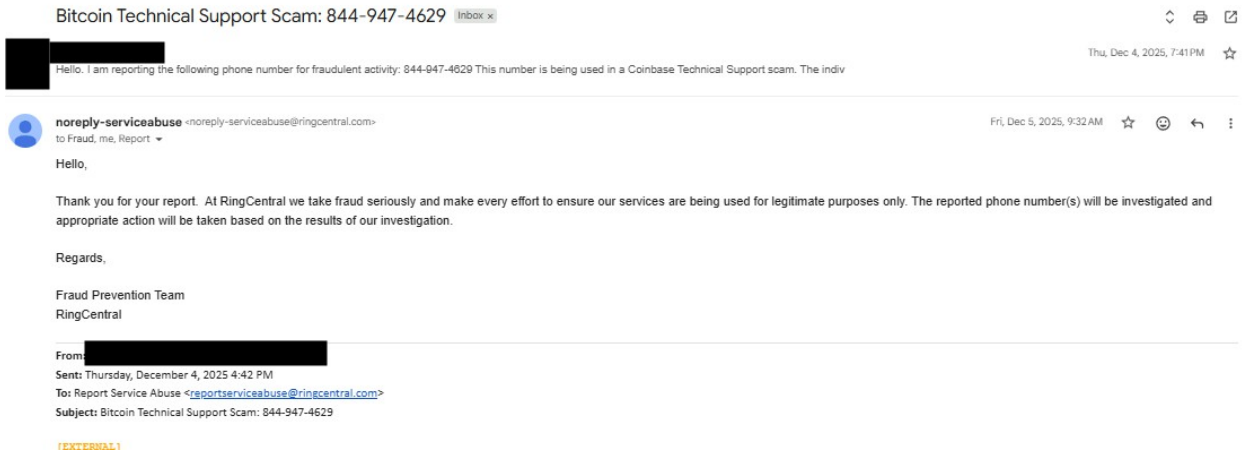


Case #4: Bitcoin Technical Support Scam

RingCentral responded by stating that it takes fraud seriously and would investigate the reported toll-free number, with appropriate action to follow based on its findings. No further updates were provided, and RingCentral has not disclosed what action, if any, was taken.

- **Toll-Free Number:** 844-947-4629

- **Recordings:** None
- **Reported:** Thu, December 4, 2025, 7:41 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Scam Google Ad)



Bitcoin Technical Support Scam: 844-947-4629 Inbox ×

[redacted]

Hello. I am reporting the following phone number for fraudulent activity: 844-947-4629 This number is being used in a Coinbase Technical Support scam. The indiv

Thu, Dec 4, 2025, 7:41 PM

noreply-serviceabuse <noreply-serviceabuse@ringcentral.com>
to Fraud, me, Report

Fri, Dec 5, 2025, 9:32 AM

Hello,

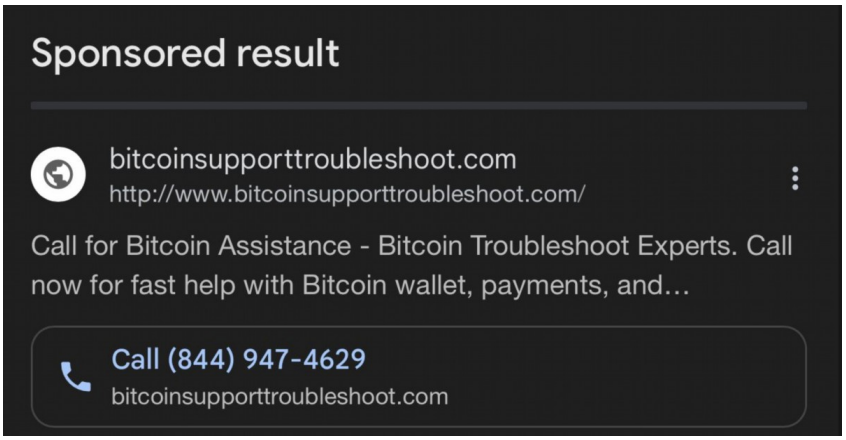
Thank you for your report. At RingCentral we take fraud seriously and make every effort to ensure our services are being used for legitimate purposes only. The reported phone number(s) will be investigated and appropriate action will be taken based on the results of our investigation.

Regards,

Fraud Prevention Team
RingCentral

From: [redacted]
Sent: Thursday, December 4, 2025 4:42 PM
To: Report Service Abuse <reportserviceabuse@ringcentral.com>
Subject: Bitcoin Technical Support Scam: 844-947-4629

[EXTERNAL]

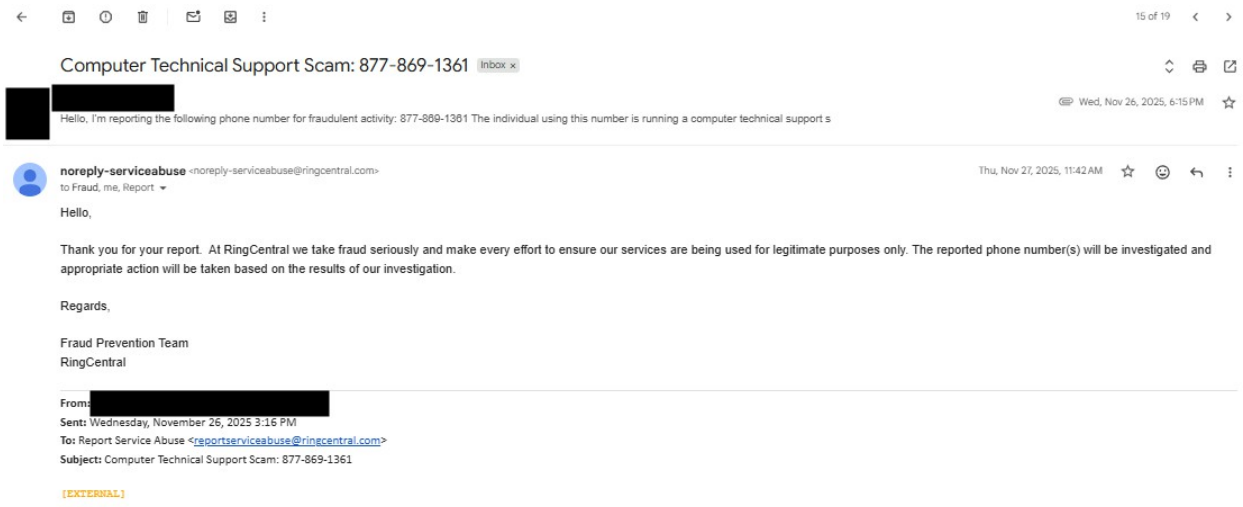


Case #5: Computer Technical Support Scam

RingCentral responded by stating that it takes fraud seriously and would investigate the reported toll-free number, with appropriate action to follow based on its findings. No further updates were provided, and RingCentral has not disclosed what action, if any, was taken

- **Toll-Free Number:** 877-869-1361

- **Recordings:** Yes
    - https://drive.google.com/file/d/1Mq8rIlaN2yO_d4wJCQDrw4fN0DKfYVYU/
- **Reported:** Wed, Nov 26, 2025, 6:15 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Call Back)



Computer Technical Support Scam: 877-869-1361 Inbox ×

[redacted]

Hello, I'm reporting the following phone number for fraudulent activity: 877-869-1361 The individual using this number is running a computer technical support s

Wed, Nov 26, 2025, 6:15 PM

noreply-serviceabuse <noreply-serviceabuse@ringcentral.com>
to Fraud, me, Report

Thu, Nov 27, 2025, 11:42 AM

Hello,

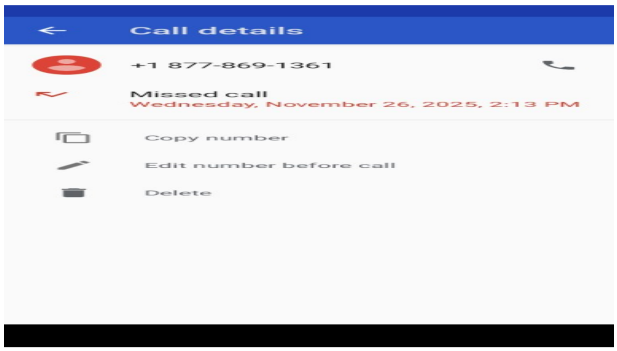
Thank you for your report. At RingCentral we take fraud seriously and make every effort to ensure our services are being used for legitimate purposes only. The reported phone number(s) will be investigated and appropriate action will be taken based on the results of our investigation.

Regards,

Fraud Prevention Team
RingCentral

From: [redacted]
Sent: Wednesday, November 26, 2025 3:16 PM
To: Report Service Abuse <reportserviceabuse@ringcentral.com>
Subject: Computer Technical Support Scam: 877-869-1361

[EXTERNAL]

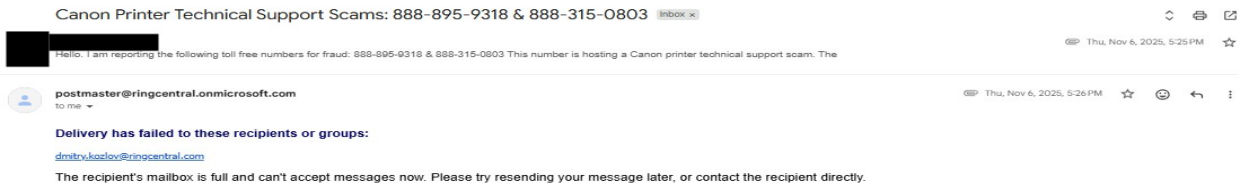


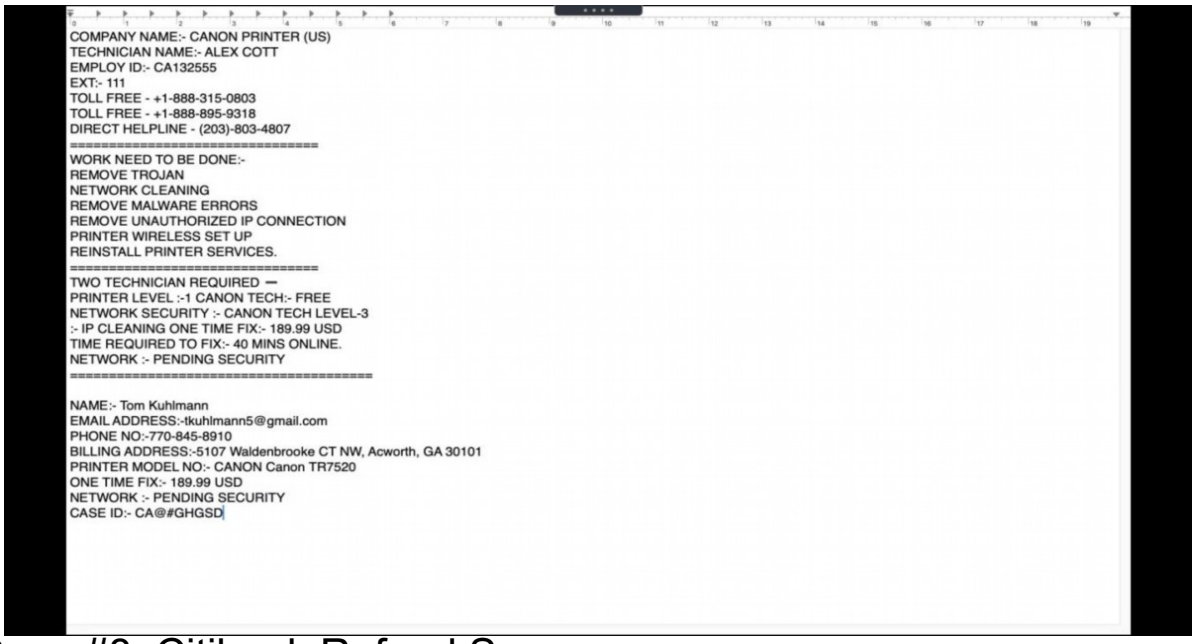
Case #6 & #7: Canon Printer Technical Support Scams

Although Demurrage sent a detailed report, the email address returned an error, stating that the email could not be received due to the recipient's mailbox being full, leaving this case unresolved.

- **Toll-Free Numbers:** 888-895-9318, 888-315-0803
- **Recordings:** Yes

    - https://drive.google.com/file/d/10Aqo53Gz93Dxkk37NpBRuwIQ5PB_Z_ha
    - https://drive.google.com/file/d/1VCf6AIUHhrqnmeke53VnIkOeXa50H2iY/
- **Reported:** Thu, November 6, 2025, 5:25 PM
- **Action Taken:** None
- **Screenshot:** Yes (Scammer Invoice)



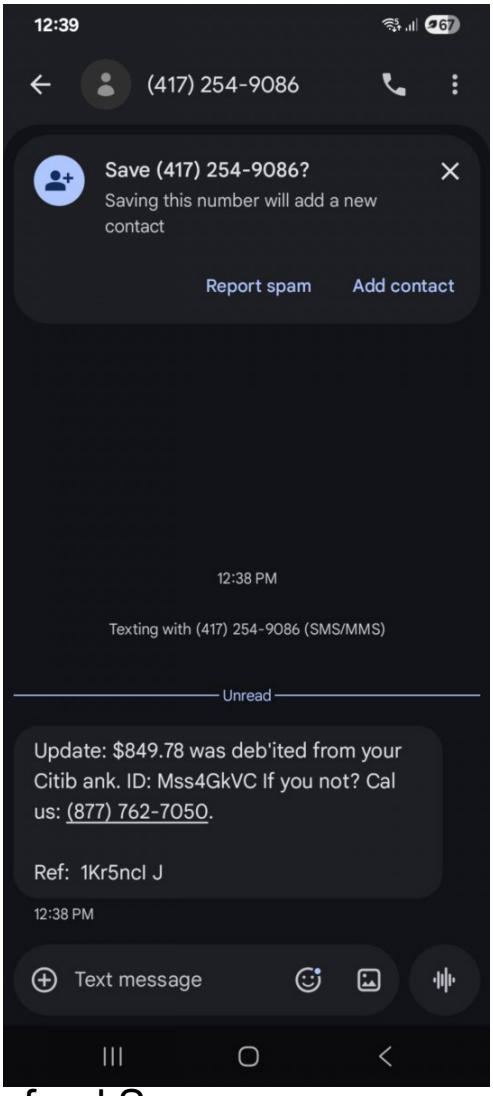


Case #8: Citibank Refund Scam

Despite submitting a detailed report to RingCentral, Demurrage received no response about the status of this case. As of this writing, no further updates or responses have been provided by RingCentral's fraud department.

- **Toll-Free Numbers:** 877-762-7050
- **Recordings:** Yes
    - https://drive.google.com/file/d/1WDmq3dBnCKmQXw5x_flfNYPDIeIJHvoH

- **Reported:** Wed, January 21, 1:45 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Scam SMS)

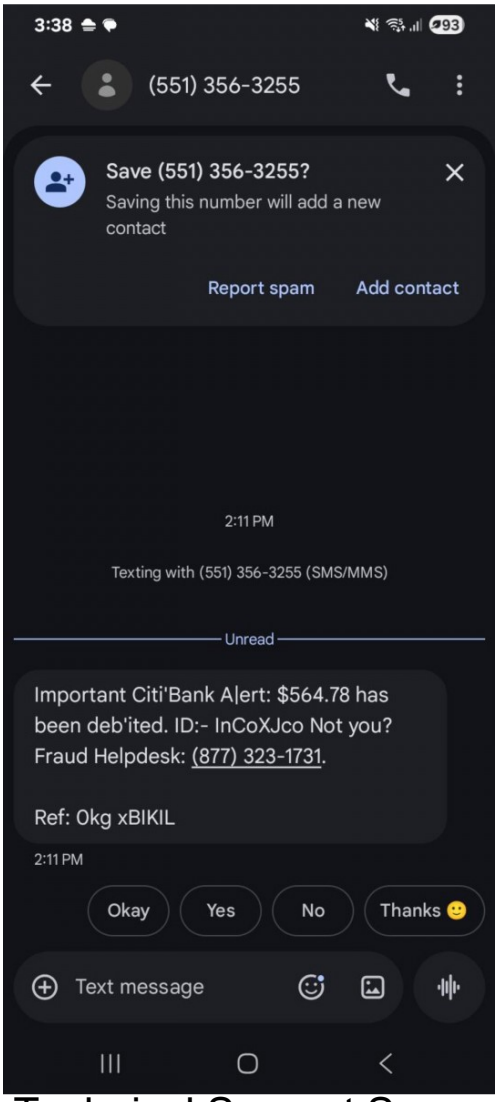


Case #9: Citibank Refund Scam

Despite submitting a detailed report to RingCentral, Demurrage received no response about the status of this case. As of this writing, no further updates or responses have been provided by RingCentral's fraud department.

- **Toll-Free Numbers:** 877-762-7050
- **Recordings:** Yes
    - https://drive.google.com/file/d/1v6a90Kjv-I5bYBFkab60DpSxZlx5Cs9o/

- **Reported:** Tue, February 17, 2026, 3:49 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Scam SMS)

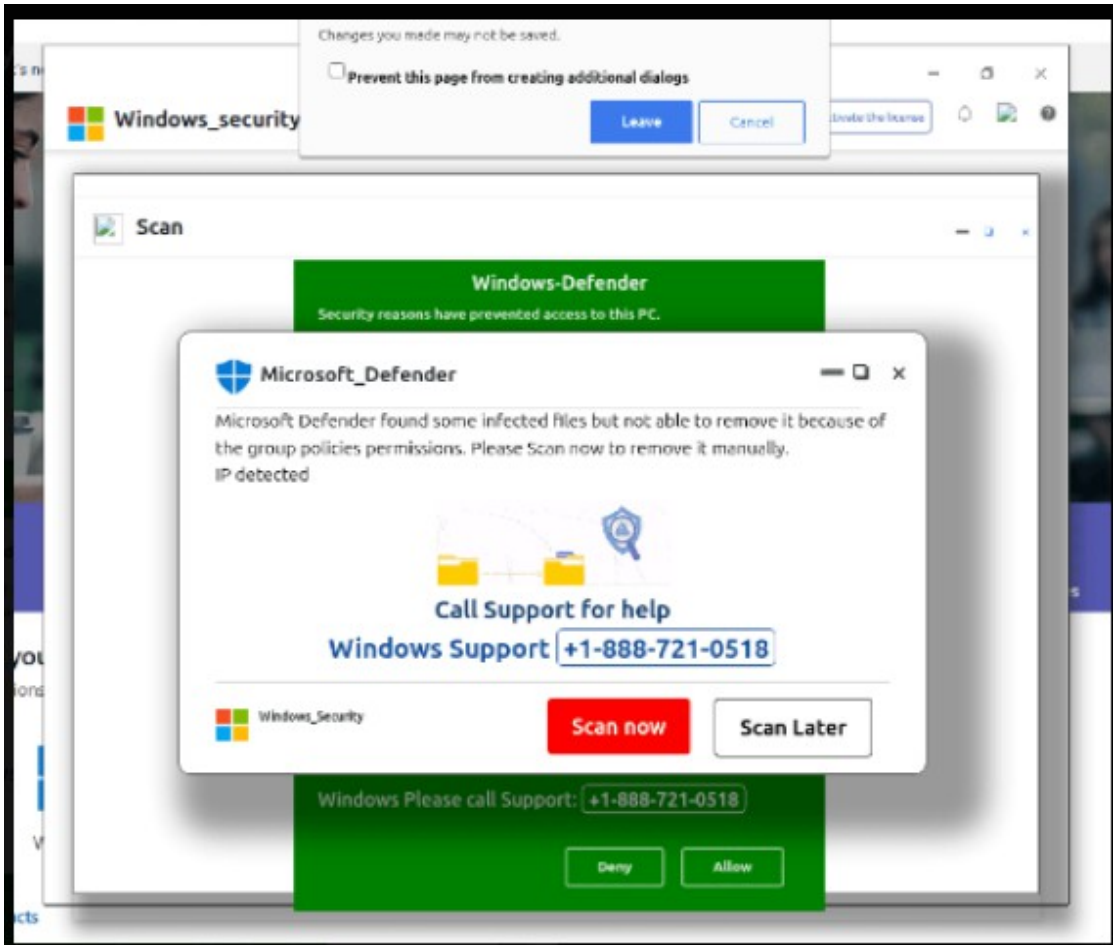


Case #10: Microsoft Technical Support Scam

Despite submitting a detailed report to RingCentral, Demurrage received no response about the status of this case. As of this writing, no further updates or responses have been provided by RingCentral's fraud department.

- **Toll-Free Numbers:** 888-721-0518
- **Recordings:** Yes
    - https://drive.google.com/file/d/142eHZkM-mQYHBIMCjnhm-9yq-fm-0T87/

- **Reported:** Tue, February 17, 2026, 3:49 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Pop-Up)

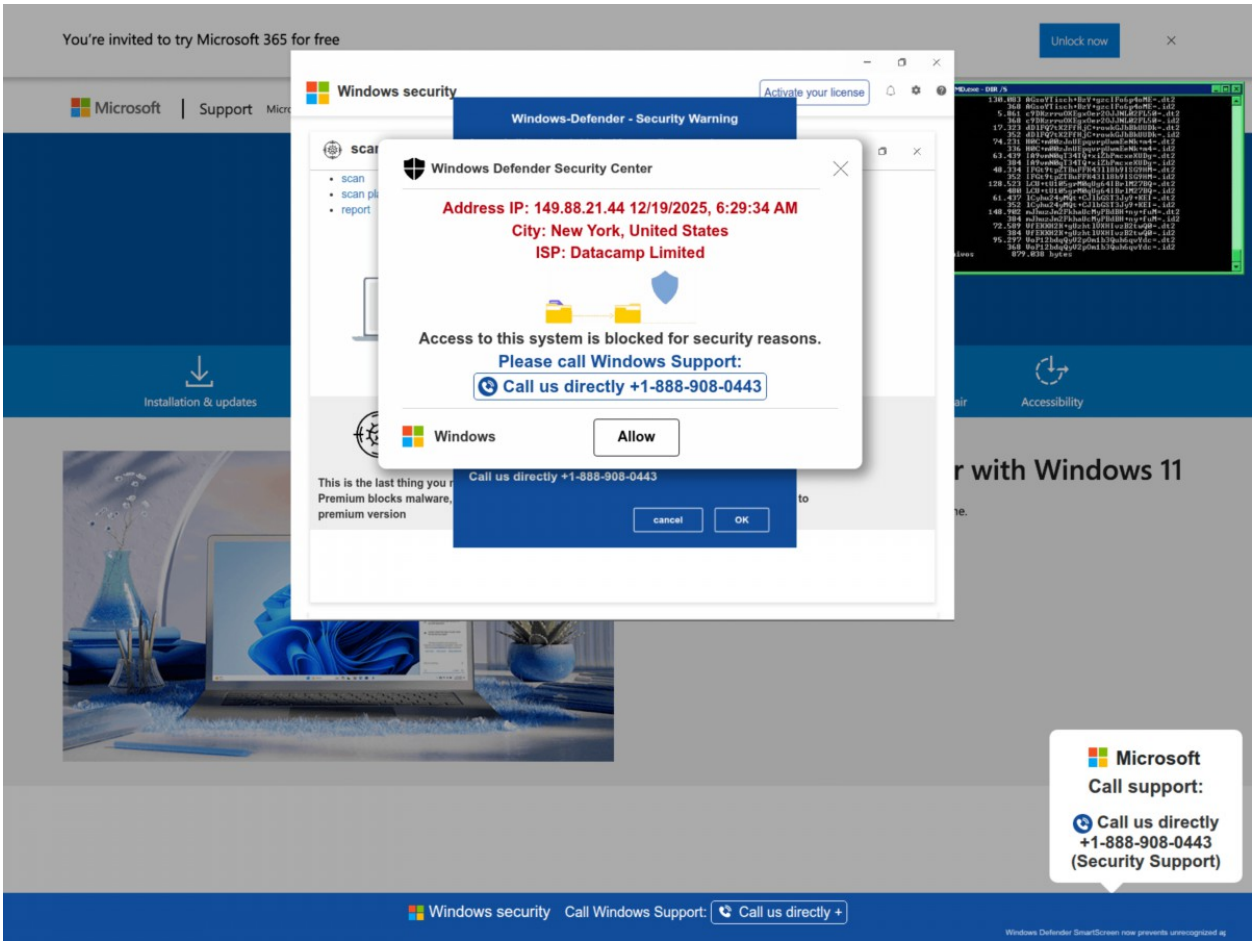


Case #11: Microsoft Technical Support Scam

Despite submitting a detailed report to RingCentral, Demurrage received no response about the status of this case. As of this writing, no further updates or responses have been provided by RingCentral's fraud department.

- **Toll-Free Numbers:** 888-415-7056
- **Recordings:** None
- **Reported:** Tue, February 17, 2026, 3:49 PM

- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Pop-Up)

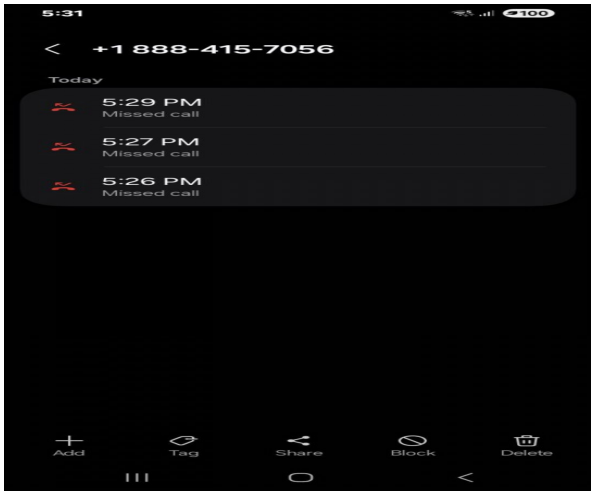


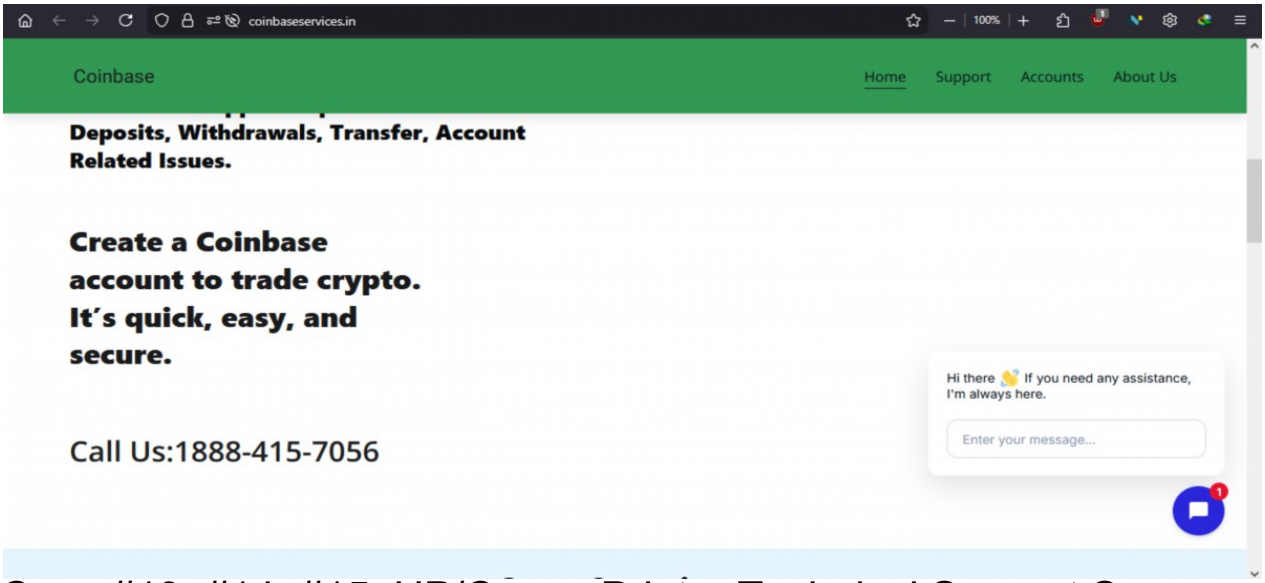
Case #12: Coinbase Technical Support Scam

Despite submitting a detailed report to RingCentral, Demurrage received no response about the status of this case. As of this writing, no further updates or responses have been provided by RingCentral's fraud department.

- **Toll-Free Numbers:** 888-415-7056
- **Recordings:** Yes
    - https://drive.google.com/file/d/1uWWii21XFk5t-8NQKNSdahCs7xpg_bpi/

- **Reported:** Wed, December 3, 2025, 5:38 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Call Back & Phishing Website)





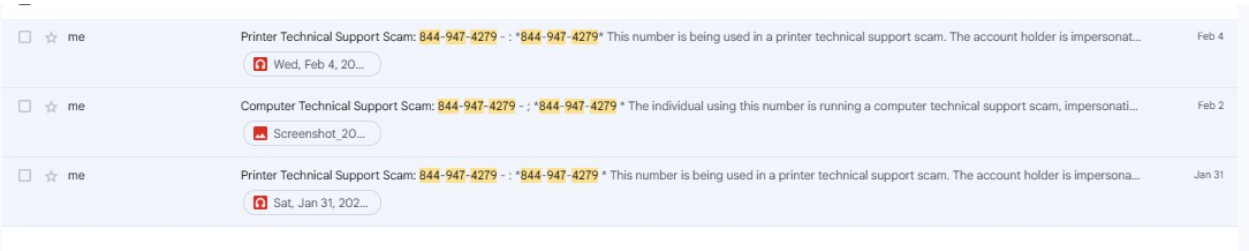
Case #13, #14, #15: HP/Canon Printer Technical Support Scam

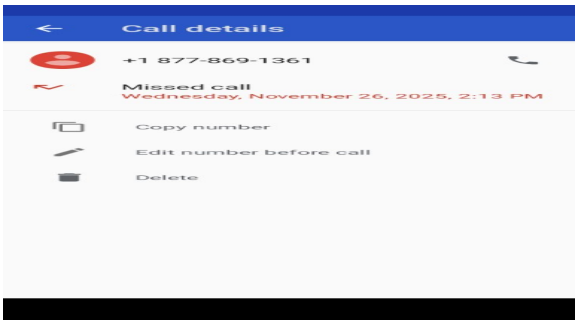
This number was reported three times to RingCentral. Despite submitting detailed reports, Demurrage received no responses about the status of this case. As of this writing, no further updates or responses have been provided by RingCentral's fraud department.

This case is linked to a specific call center in India that specializes in the impersonation of Canon and HP by claiming to be certified "Printer Support" for each brand and has

been known to illegally use each company's logos in the invoices they send to victims. This call center has numbers spanning across several toll-free and non-toll-free numbers on RingCentral.

- **Toll-Free Numbers:** 844-947-4279
- **Recordings:** Yes
    - https://drive.google.com/file/d/1V8Q-GgVp9GjpmVwqVrjel4tIAhnI4SJf/
    - https://drive.google.com/file/d/1vdIDausCdiTiqYZZVW9uBuUrbV847TpW/
- **Reported:** Sat, January 31, 2:04 PM & Mon, February 2, 12:59 PM & Wed, February 4, 1:54 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Call Back)





Case #16, #17, #18, #19: HP Printer Technical Support Scam

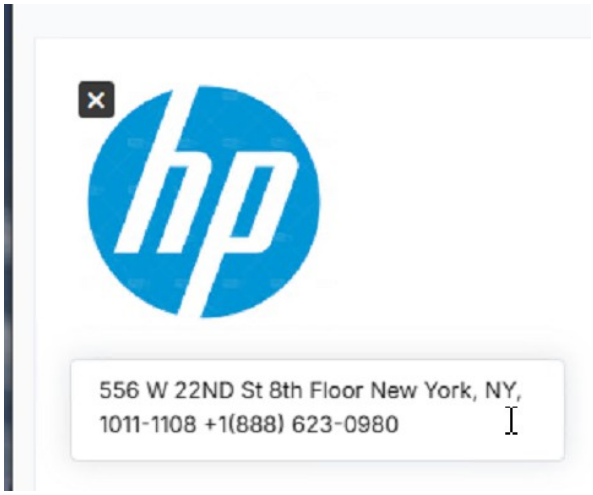
This number was reported four times to RingCentral. Despite submitting detailed reports, Demurrage received no responses about the status of this case. As of this writing, no further updates or responses have been provided by RingCentral's fraud department.

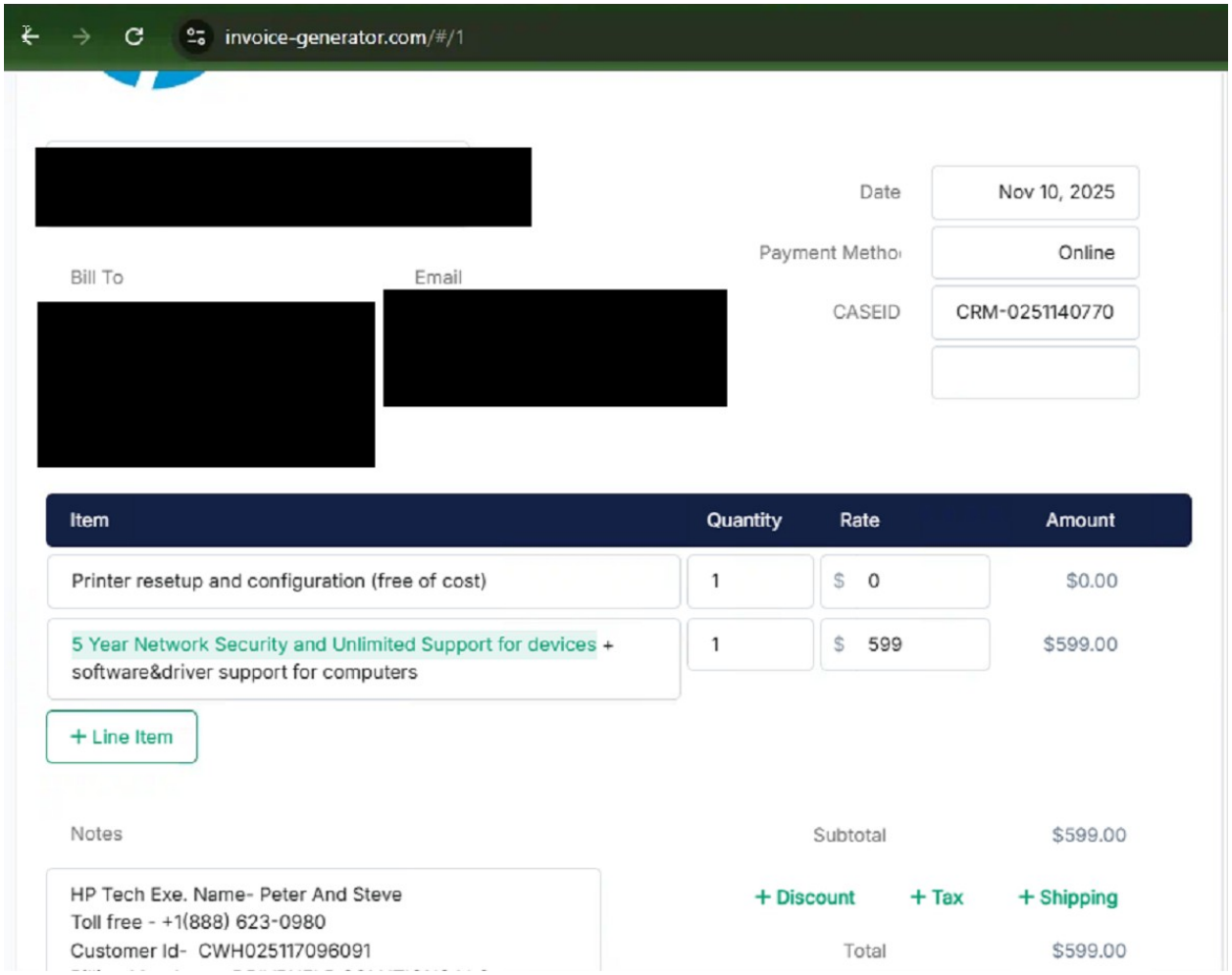
Like the previous cases, this toll-free number is linked to the same call center in India that specializes in the impersonation of Canon and HP by claiming to be certified

"Printer Support" for each brand and has been known to illegally use each company's logos in the invoices they send to victims. This call center has numbers spanning several toll-free and non-toll-free numbers on RingCentral.

- **Toll-Free Numbers:** 888-623-0980
- **Recordings:** Yes
    - https://drive.google.com/file/d/1vXGpl7B3enIU6-hB_m1cXKCIL9ueuzsG/
    - https://drive.google.com/file/d/18vbuH-WaRZ5GWgBwlUslSBX3MhZGJ231/view?usp=sharing
- **Reported:** Mon, November 10, 2025, 7:31 PM & Tue, November 11, 2025, 3:40 PM & Sat, February 14, 3:37 PM & Wed, February 11, 7:17 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Phishing Logo & Scammer Invoice)




556 W 22ND St 8th Floor New York, NY,
1011-1108 +1(888) 623-0980

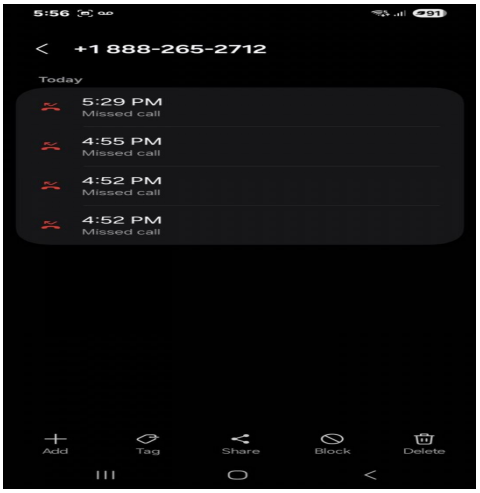

invoice-generator.com/#/1
[redacted]
Date
Nov 10, 2025
Payment Metho
Online
CASEID
CRM-0251140770
Bill To
[redacted]
Email
[redacted]
Item
Quantity
Rate
Amount
Printer resetup and configuration (free of cost)
1
$ 0
$0.00
5 Year Network Security and Unlimited Support for devices + software&driver support for computers
1
$ 599
$599.00
+ Line Item
Notes
Subtotal
$599.00
HP Tech Exe. Name- Peter And Steve
Toll free - +1(888) 623-0980
Customer Id- CWH025117096091
+ Discount
+ Tax
+ Shipping
Total
$599.00

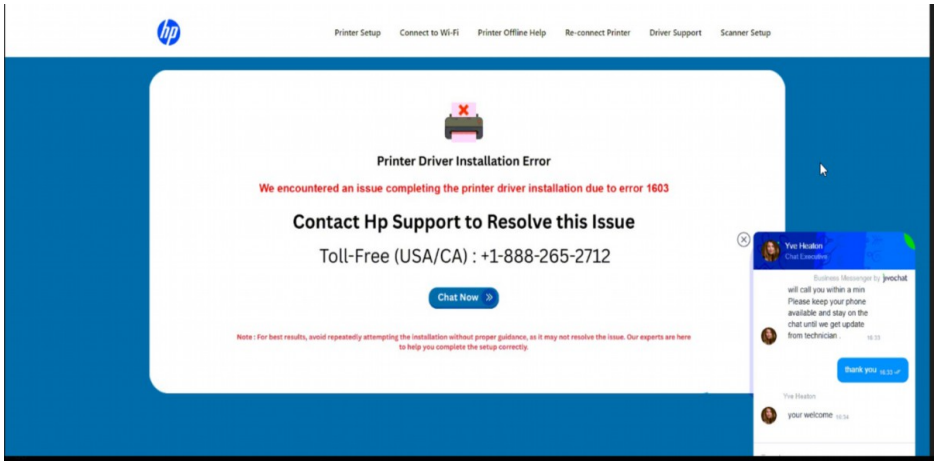
Case #20: HP Printer Technical Support Scam

Despite submitting a detailed report to RingCentral, Demurrage received no response about the status of this case. As of this writing, no further updates or responses have been provided by RingCentral's fraud department, despite the number appearing to have been disconnected.

Like the previous cases, this toll-free number is linked to the same call center in India that specializes in the impersonation of Canon and HP by claiming to be certified "Printer Support" for each brand and has been known to illegally use each company's logos in the invoices they send to victims. This call center has numbers spanning several toll-free and non-toll-free numbers on RingCentral.

- **Toll-Free Numbers:** 888-265-2712
- **Recordings:** Yes
    - https://drive.google.com/file/d/1XmqEQ_0ui5JkgDKcoh42FtJQjMM3X4cW
- **Reported:** Tue, February 24, 2026, 5:58 PM
- **Action Taken:** Unconfirmed
- **Screenshot:** Yes (Phishing Website & Call Backs)



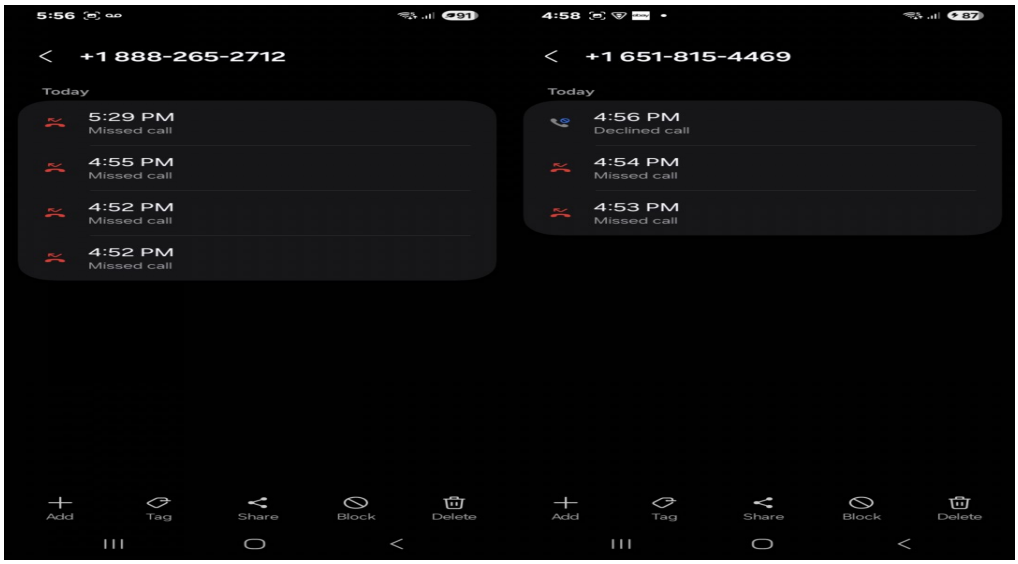


The Investigation - Part 2: The Toll-Free / NonToll-Free Number Connection

The second half of the report begins with the last toll-free number of 888-265-2712 on RingCentral, reported on February 24, 2026. Before this report, Demurrage came across multiple non-toll-free residential RingCentral numbers that were all being used for printer technical support scams, often impersonating HP, Canon and other generic technical support entities, all of which spanned across the aforementioned three telecoms of Bandwidth, Lumen and Sinch, leaving Demurrage to believe that this call center acquired all of its numbers for each scammer operating the phone through the same "mark" who was deep within RingCentral's reseller/wholesaler program.

Timeline

Demurrage called and reported the toll-free number 888-265-2712 on February 24, 2026. However, after calling that number and acquiring the recording, the U.S. non-toll-free residential number 651-815-4469 called Demurrage back three times, leaving voicemail claiming to be "HP technical support." The scammers also used 888-265-2712 to call back after receiving no response on 651-815-4469.



Recording:

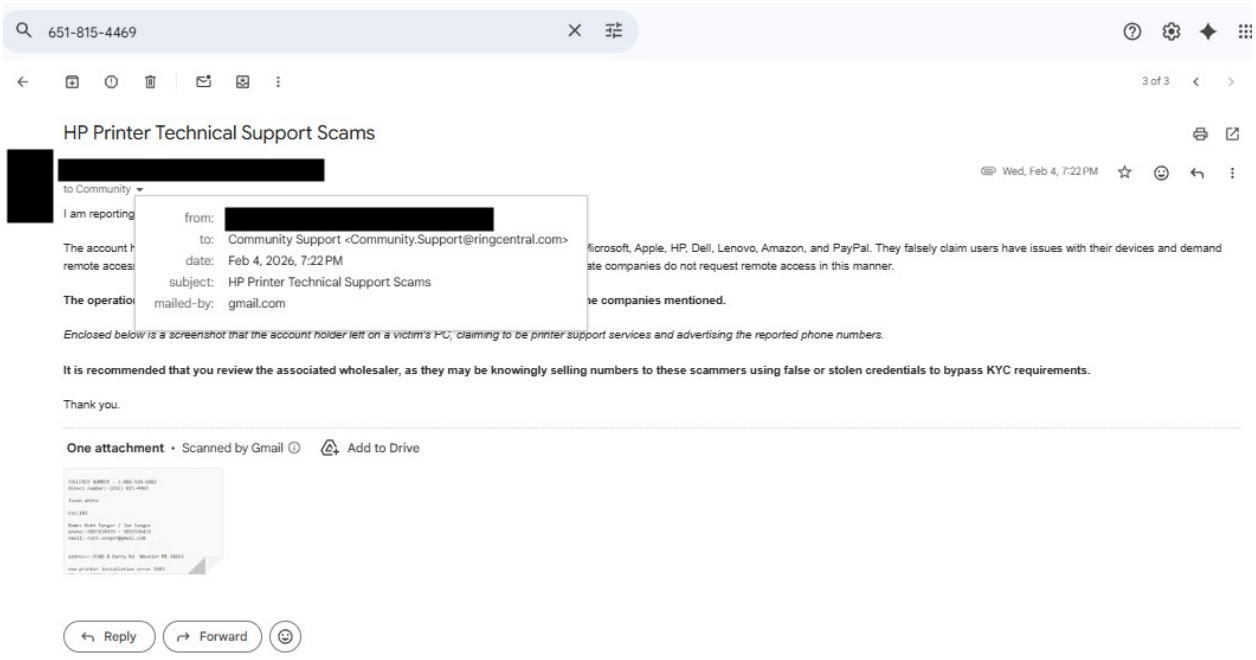
- https://drive.google.com/file/d/175BMbQUzo6NFhR5oROyw3bYv2RBgfKZJ/

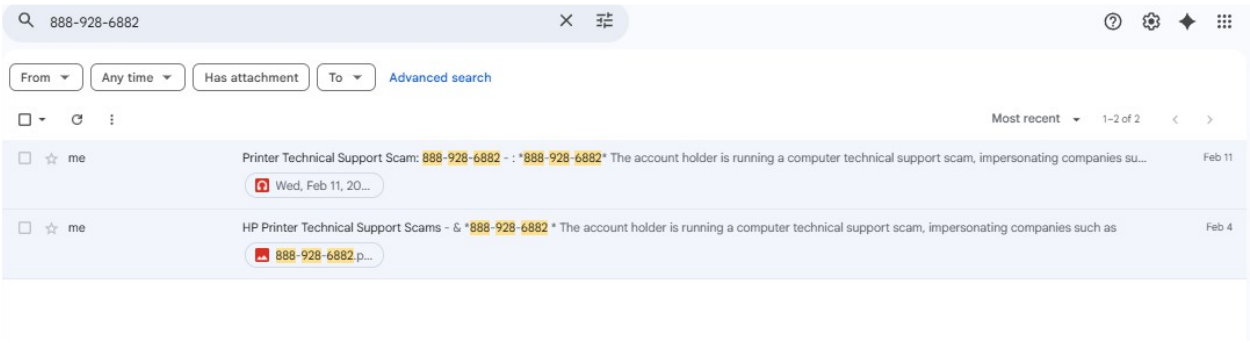
The number 651-815-4469 traced back to Bandwidth's network. Upon examining our records further, Demurrage had actually reported this number before on February 4, 2026, at 7:22 PM, prior to receiving the aforementioned callback on the dedicated cell phone.

That same report also included another toll-free number that traced back to RingCentral and was used by the same call center: 888-928-6882

This number had also been reported twice to RingCentral previously based on records. Demurrage sent RingCentral copies of the scam invoices that the scammers created using Windows Notepad after gaining access to victims' PCs, a common scammer tactic, after claiming that work was done on their printers and therefore charging the victims for bogus tech support.

Recordings were also sent to RingCentral of the scammers answering the phone, claiming to be "support."





TOLLFREE NUMBER - 1-888-928-6882
Direct number:-(651) 815-4469

Jason white

Ext:102

Name:-[redacted]
phone:-[redacted]
email:-[redacted]

address:-9300 N Barry Rd Wheeler MI 48662

new printer installation error 1603
HP envy 6155e all in one

clean up the both computer

saleby:Bhanu

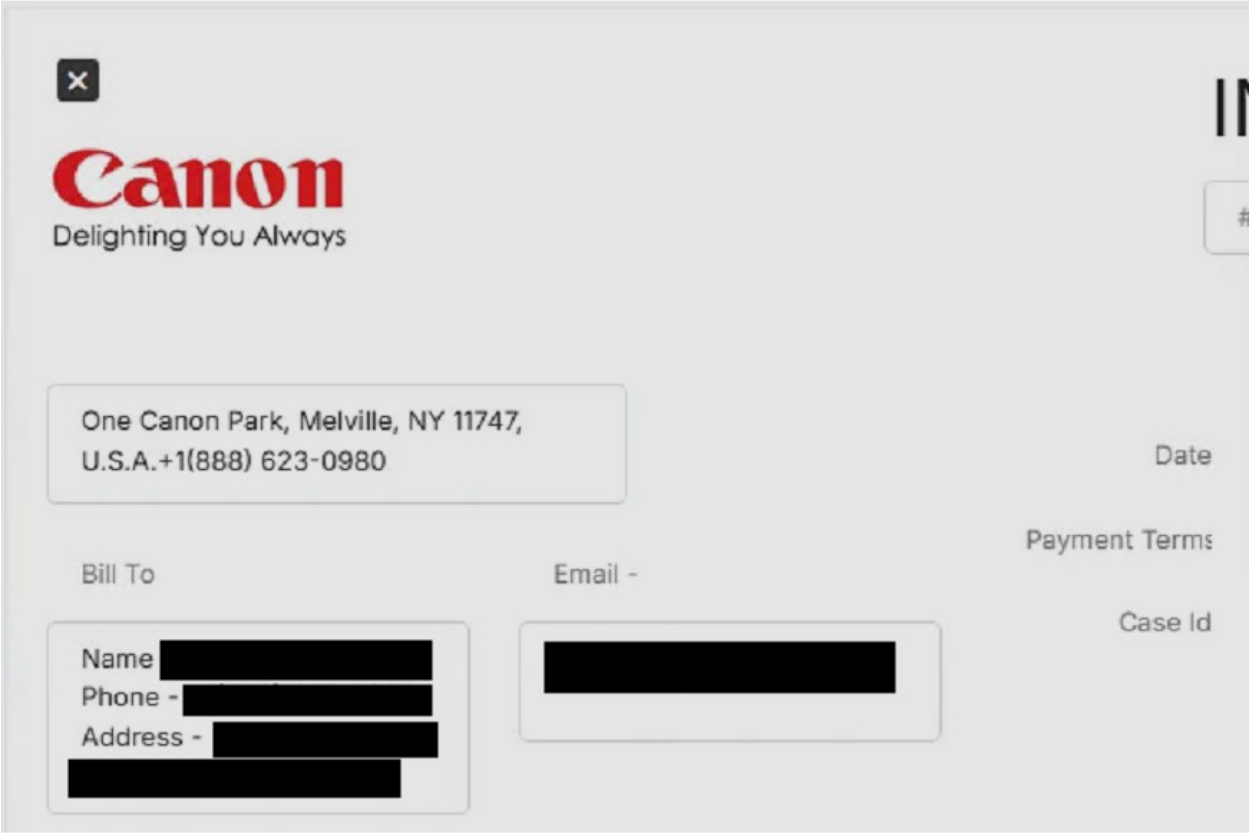
Recording:

- https://drive.google.com/file/d/1BHxfl46sio_SRCdwKgJdRxhYyUethnEL/view

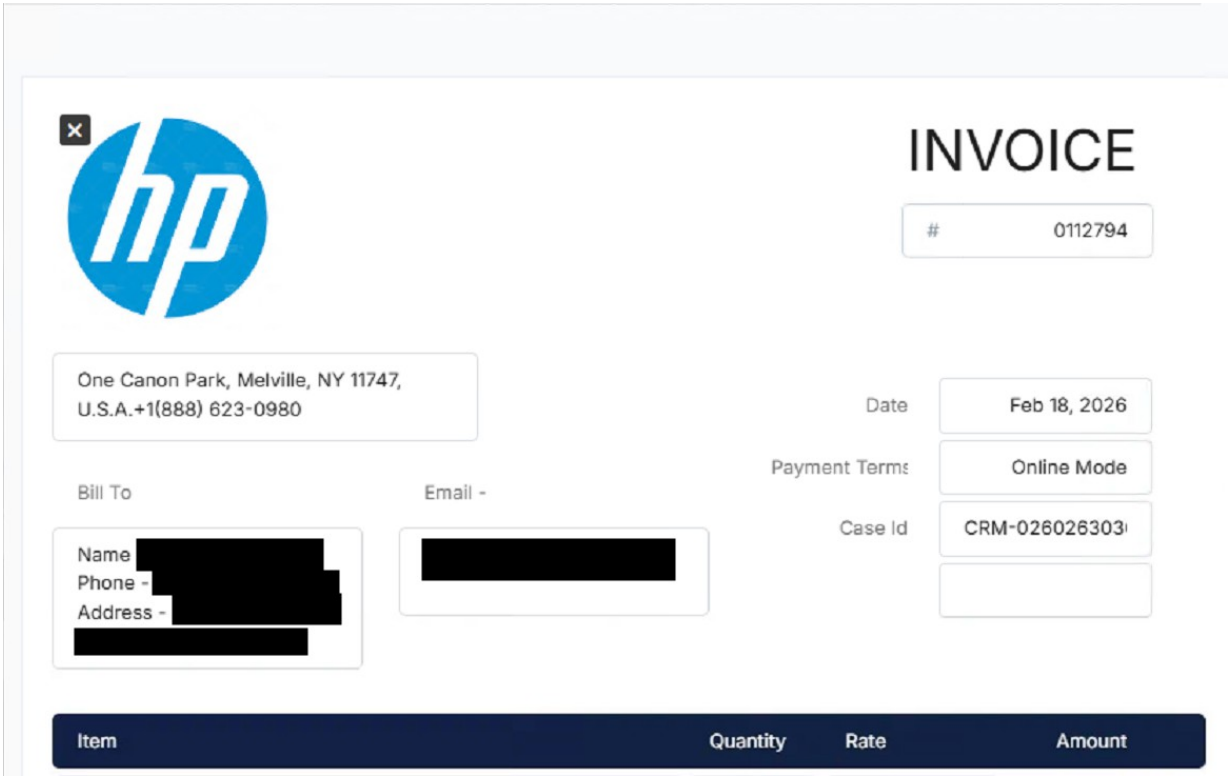
Scam Invoices, the Impersonation of HP and Canon, and help from Victim Advocate Group: AVAHS

The following series of scam invoices used by this call center were sent to Demurrage by anonymous sources along with victim advocate groups, such as AVAHS.

All of the numbers that appear within these invoices traced back to RingCentral. The victims' names, phone numbers, and email addresses have been redacted to protect their privacy.



In the first invoice, the scammers are impersonating Canon using the toll-free number 888-623-0980, which was reported four times to RingCentral on November 10, 2025, at 7:31 PM; November 11, 2025, at 3:40 PM; February 14, 2026, at 3:37 PM; and February 11, 2026, at 7:17 PM.



INVOICE

0112794

One Canon Park, Melville, NY 11747,
U.S.A.+1(888) 623-0980

Date Feb 18, 2026

Payment Terms Online Mode

Case Id CRM-026026303

Bill To

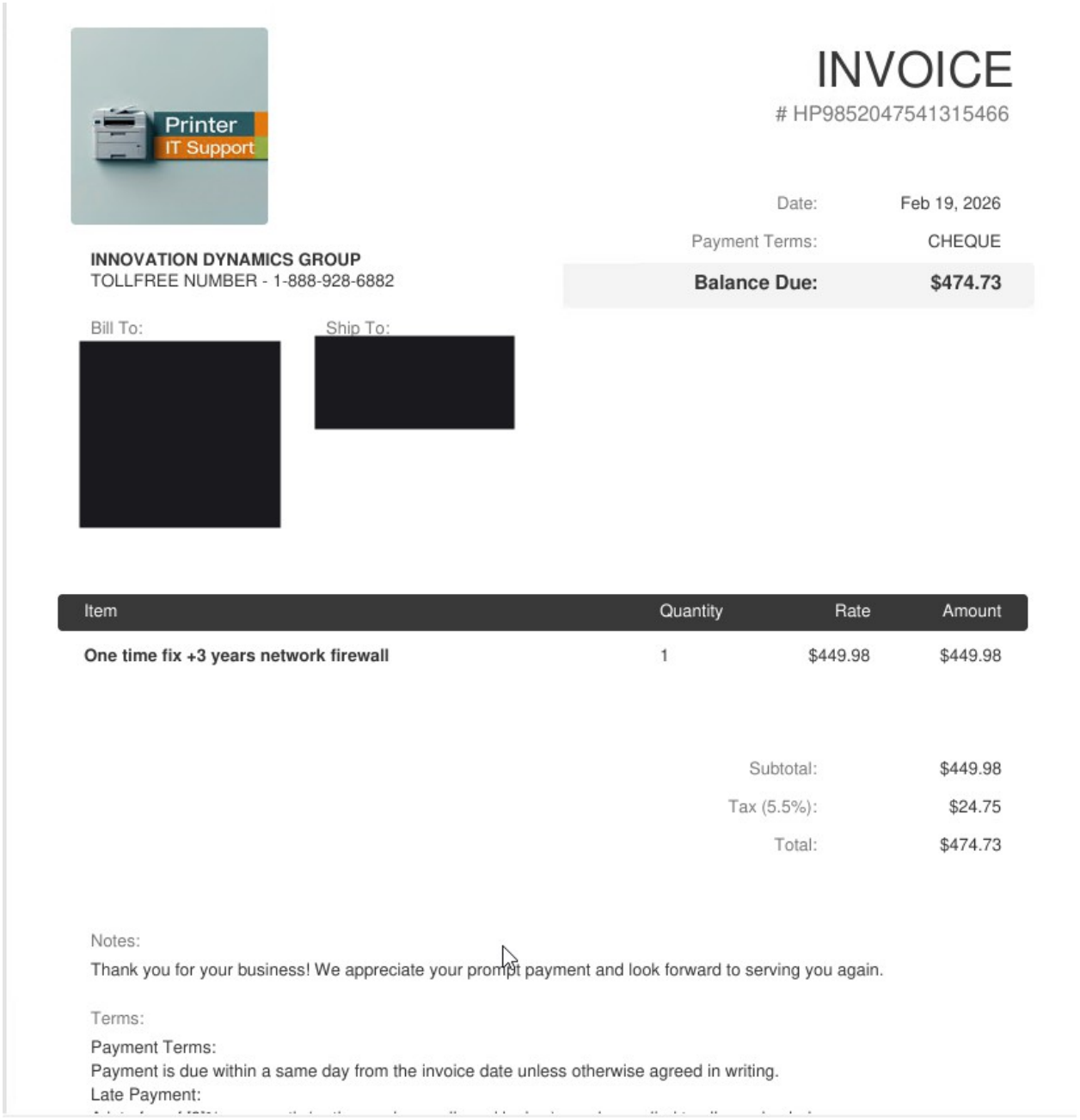
Email -

Name [redacted]
Phone - [redacted]
Address - [redacted]

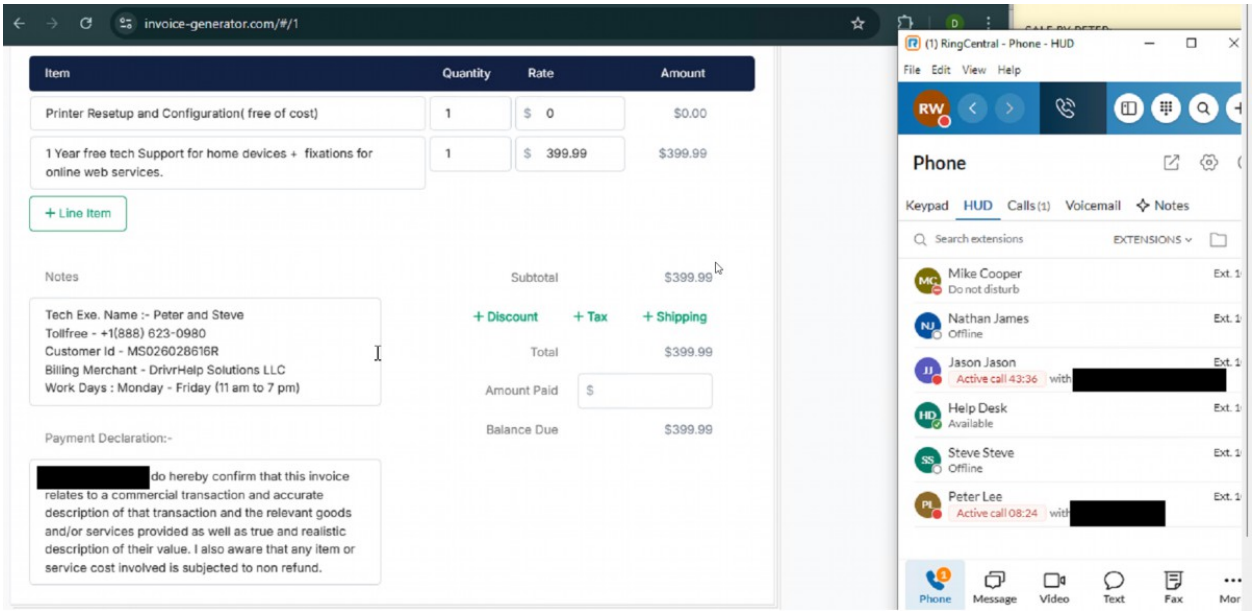
[redacted]

Item	Quantity	Rate	Amount

In the second invoice, the scammers are impersonating HP and once again using the toll-free number 888-623-0980 to receive calls under the guise of impersonating HP and Canon.



In the third invoice, the scammers list their company name as "Innovation Dynamics Group," once again using the toll-free number 888-928-6882 to receive calls under the guise of being legitimate printer IT support. The victim in this case was scammed out of $474 USD for bogus tech support, charging the victim for a "one time fix +3 years network firewall," both of which have nothing to do with printer-related problems.



In the final invoice, which was sent to AVAH anonymously and later forwarded to Demurrage, the scammers can be seen using both the RingCentral app to receive and make calls as well as a website called ***invoice-generator.com*** to create a bogus invoice for the victim who was eventually scammed for $399 USD.

Once again, if these accounts were genuine, why would they need to create invoices from such a website if they are legitimate Canon and HP support?

More concerning still, because the scammers lost some of their callback numbers after Demurrage reported them to Lumen, the scammers began including a declaration at the bottom of these invoices, which they made the victims accept to avoid having their accounts and merchant, which is listed as "**DrivrHelp Solutions LLC**", flagged and to avoid chargebacks due to refunds after victims were contacted by AVAH and notified that they were scammed.

Testimony By AVAHS

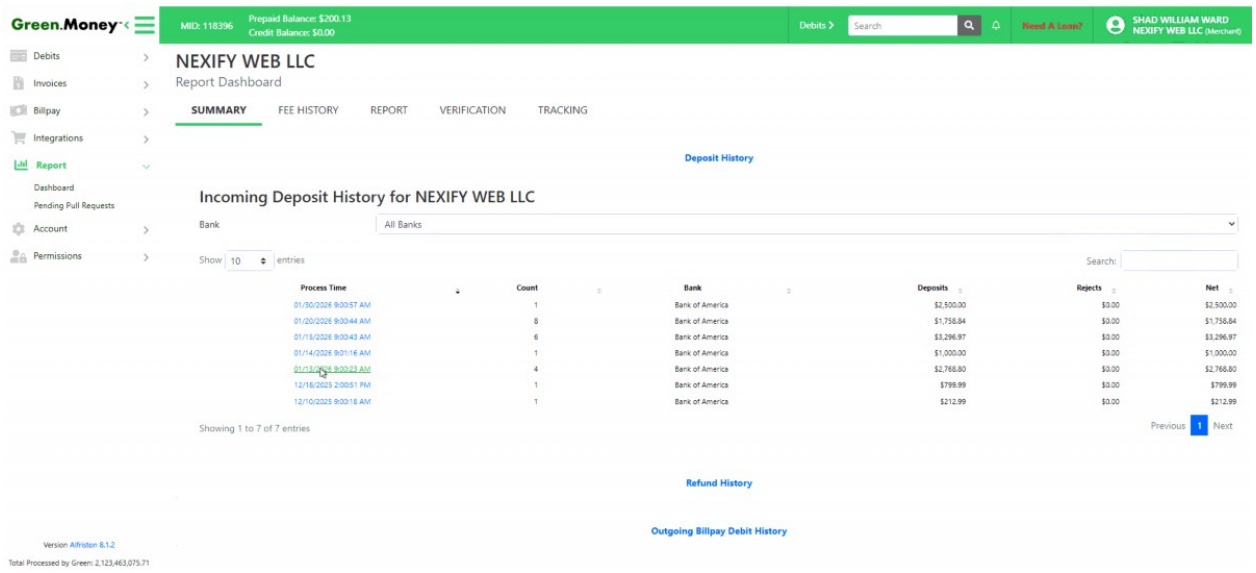
A member of Demurrage contacted AVAHS on February 18, 2026, after receiving the invoices and the various numbers used by the scammers.

AVAHS Outreach Group is an all-volunteer organization providing certified assistance and free victim advocacy for all scam victims.

AVAHS concluded that they had spoken to 157 victims from the beginning of February to the 18th and that 75% were victims of these printer support scammers, or possibly even higher. The numbers that Demurrage found were also linked to the same call center that scammed victims AVAH had spoken to during the month of February. AVAHS also shared toll-free numbers, such as 888-265-2712, during the time of this investigation, corroborating Demurrage's data in the process.

AVAHS also concluded that this same call center was running insurance-type scams but had moved to printer support scams. While several other victims did not answer AVAHS' calls, they were left detailed voicemails by AVAHS on how to proceed after being scammed along with being provided with outreach support.

More concerning still, AVAHS shared the scammers' intake data on these scams, which they received anonymously, and the results were very concerning. Once again, RingCentral has done little to nothing about the numbers and traffic that were reported to them.



Demurrage would like to thank AVAHS for their help in this investigation. While many news outlets have an idea of what scambaiting is, and while Demurrage itself is not a scambaiting group, there is not enough attention given to groups like AVAHS, which talk to real victims who were scammed by these criminals. AVAHS work with victims deserves not only praise but more attention, as they deal directly with the fallout of the scams. Their work is just as important, if not more so, than what groups like Demurrage and other scambaiters are doing. AVAHS contact information can be found below.



https://avahsoutreach.org/

Non Toll-Free Residential Numbers & The Lack of Action By Bandwidth Against Complicit Wholesalers

Before proceeding, Demurrage would like to stress that it holds no ill will toward Bandwidth's support staff. This half of the report is not meant in any way to slander them, but rather to highlight that Bandwidth as a telecom is not doing nearly enough when it comes to removing scammers from its network.

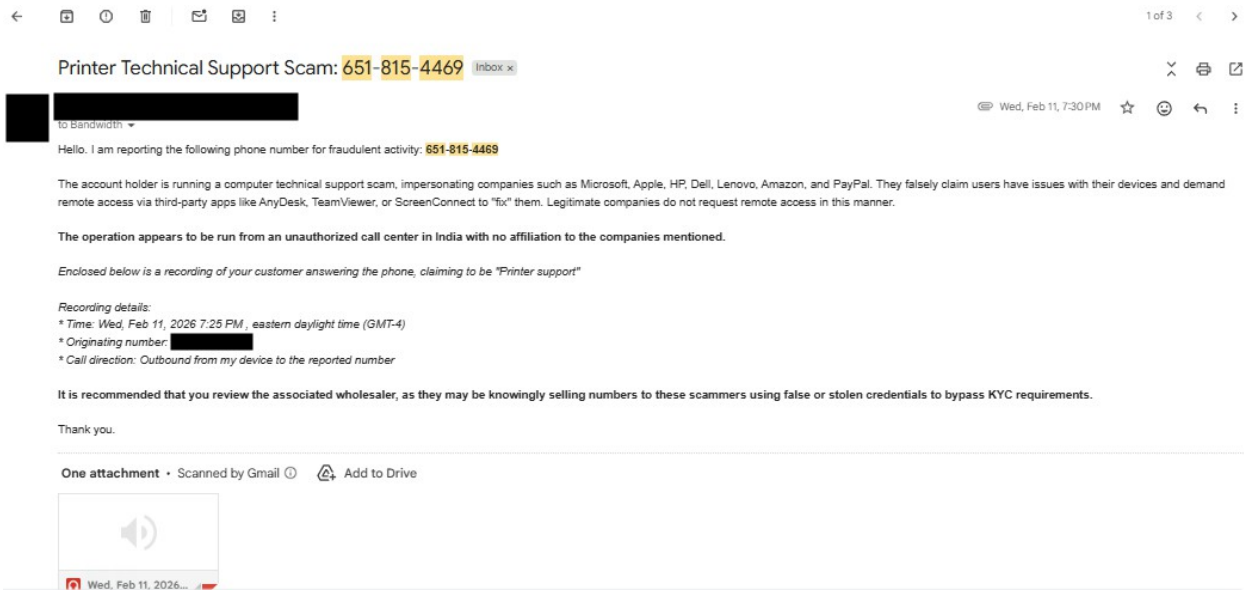
The names of the support agents have been redacted to protect their privacy. Demurrage thanks them for their time and wishes for more direct human communication for these fraud reports in the future.

Bandwidth as a telecom will continue to have problems in the future because its current practices for addressing fraud are simply inadequate and ineffective and only encourage fraud to continue on its network. As stated earlier, many telecoms refuse to take direct action against the “marks” and wholesalers on their networks, with Bandwidth having a long history of doing so.

The following cases all involve numbers traced back to RingCentral and were routed through Bandwidth's network.

Case 1: 651-815-4469

As mentioned earlier, this number was reported twice. Since RingCentral did not respond directly to the first report, Demurrage sent a second report on February 11, 2026, at 7:30 PM to Bandwidth with a recording and timestamps.



1 of 3

Printer Technical Support Scam: 651-815-4469 Inbox ×

[redacted]

to Bandwidth

Wed, Feb 11, 7:30 PM

Hello. I am reporting the following phone number for fraudulent activity: 651-815-4469

The account holder is running a computer technical support scam, impersonating companies such as Microsoft, Apple, HP, Dell, Lenovo, Amazon, and PayPal. They falsely claim users have issues with their devices and demand remote access via third-party apps like AnyDesk, TeamViewer, or ScreenConnect to "fix" them. Legitimate companies do not request remote access in this manner.

The operation appears to be run from an unauthorized call center in India with no affiliation to the companies mentioned.

Enclosed below is a recording of your customer answering the phone, claiming to be "Printer support"

Recording details:
** Time: Wed, Feb 11, 2026 7:25 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.

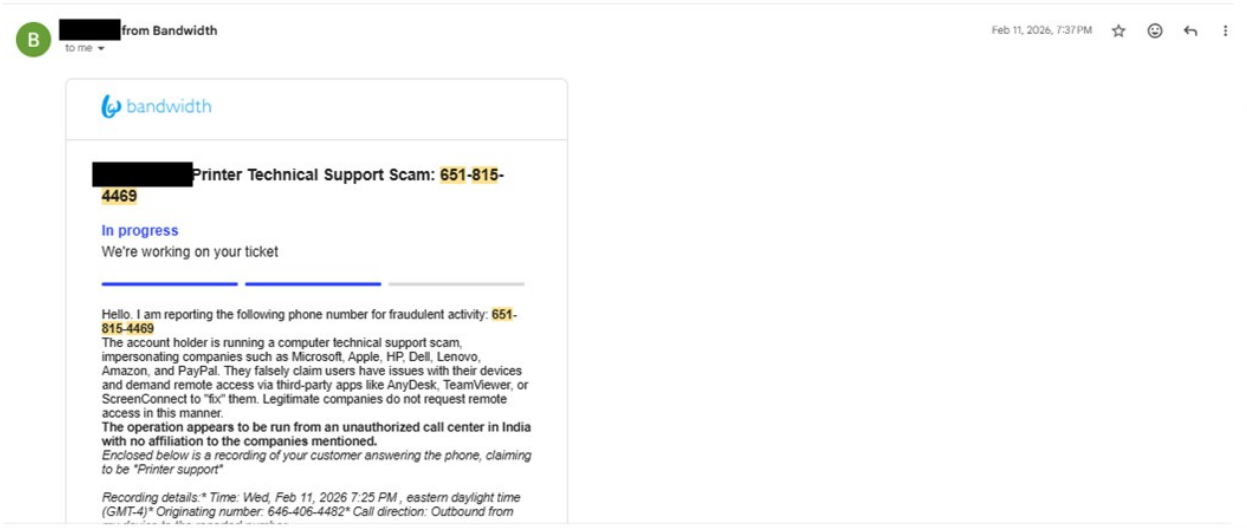
Thank you.

One attachment • Scanned by Gmail ⓘ Add to Drive

Wed, Feb 11, 2026...

Because Bandwidth now relies on an AI system called "Synthi," there is a bit of a delay between the time the report is received and sent to an actual human at Bandwidth.

There are many problems with Bandwidth's new AI and its insistence on using it, but these will not be addressed at this time.



B [redacted] from Bandwidth
to me
Feb 11, 2026, 7:37 PM

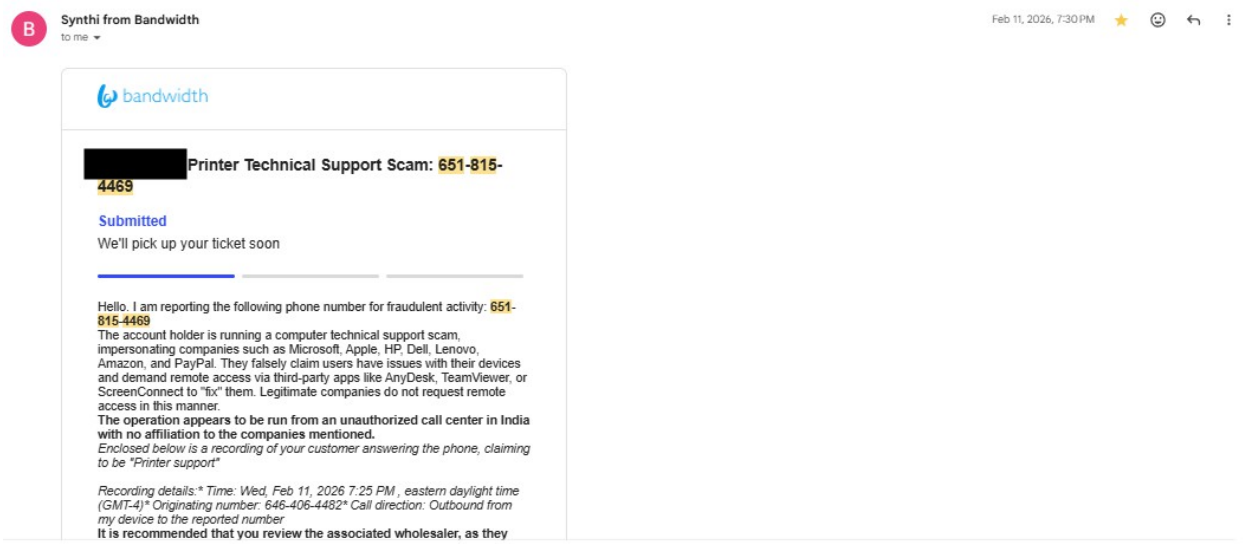
bandwidth

[redacted] Printer Technical Support Scam: 651-815-4469

In progress
We're working on your ticket

Hello. I am reporting the following phone number for fraudulent activity: 651-815-4469
The account holder is running a computer technical support scam, impersonating companies such as Microsoft, Apple, HP, Dell, Lenovo, Amazon, and PayPal. They falsely claim users have issues with their devices and demand remote access via third-party apps like AnyDesk, TeamViewer, or ScreenConnect to "fix" them. Legitimate companies do not request remote access in this manner.
The operation appears to be run from an unauthorized call center in India with no affiliation to the companies mentioned.
Enclosed below is a recording of your customer answering the phone, claiming to be "Printer support"

Recording details: Time: Wed, Feb 11, 2026 7:25 PM , eastern daylight time (GMT-4)* Originating number: 646-406-4482* Call direction: Outbound from*



B Synthi from Bandwidth
to me
Feb 11, 2026, 7:30 PM

bandwidth

[redacted] Printer Technical Support Scam: 651-815-4469

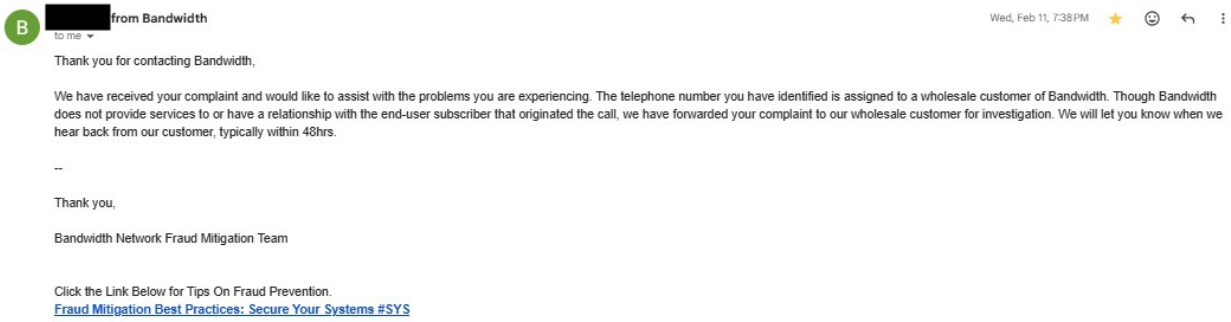
Submitted
We'll pick up your ticket soon

Hello. I am reporting the following phone number for fraudulent activity: 651-815-4469
The account holder is running a computer technical support scam, impersonating companies such as Microsoft, Apple, HP, Dell, Lenovo, Amazon, and PayPal. They falsely claim users have issues with their devices and demand remote access via third-party apps like AnyDesk, TeamViewer, or ScreenConnect to "fix" them. Legitimate companies do not request remote access in this manner.
The operation appears to be run from an unauthorized call center in India with no affiliation to the companies mentioned.
Enclosed below is a recording of your customer answering the phone, claiming to be "Printer support"

Recording details: Time: Wed, Feb 11, 2026 7:25 PM , eastern daylight time (GMT-4)* Originating number: 646-406-4482* Call direction: Outbound from my device to the reported number*
It is recommended that you review the associated wholesaler, as they

On February 11, 2026, at 7:38 PM, a support agent at Bandwidth stated the following:

> 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

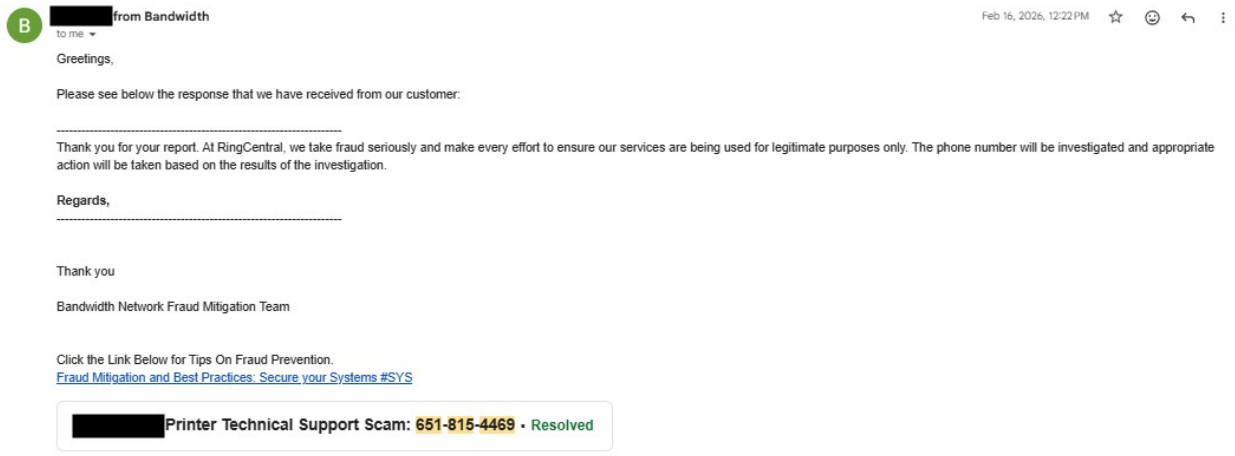


The last half of that response is key and is where the problems begin with Bandwidth, as it is not uncommon for many wholesalers to ignore the 48-hour period that Bandwidth supposedly claims is the allotted time for their customers to respond.

Nowhere is that more clear than with RingCentral and its “marks”, as it took five days for RingCentral to respond. At no point does Bandwidth make any attempts to get its customers or wholesalers to respond after 48 hours, which Demurrage considers far too long, as the scammers are literally using the number to commit tech support fraud during the entire time a person filing the report is waiting for a response.

After five days, RingCentral responded with the following, to which the agent at Bandwidth notified Demurrage via email:

> Greetings,
>
> Please see below the response that we have received from our customer:
>
> ---
> Thank you for your report. At RingCentral, we take fraud seriously and make every effort to ensure our services are being used for legitimate purposes only. The phone number will be investigated and appropriate action will be taken based on the results of the investigation.
>
> Regards,
> ---
>
> Thank you
> Bandwidth Network Fraud Mitigation Team



Demurrage then proceeded to call the number back, and the scammer once again answered the phone, claiming to be "support" and did so for days afterward, effectively proving that RingCentral took no action whatsoever. More telling still, this also proves that Bandwidth does not actually read the responses that their wholesalers send to them, as Bandwidth marked this case as "solved" and closed the ticket, despite RingCentral taking no action and not notifying Bandwidth of any actions that may have been taken.

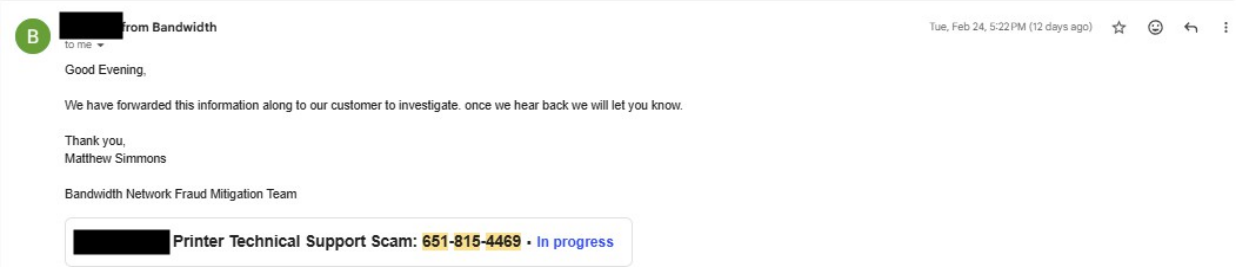
This type of behavior by Bandwidth happens far too frequently. As long as a response is sent to Bandwidth, regardless of what is said by their customers, Bandwidth will close the ticket regardless of whether actions are taken or not.

On February 24, 2026, some 11 days later, Demurrage followed up after it became clear that RingCentral had taken no action against the reported number. New data was included that was previously shown in the toll-free half of this report: the scammers called back on the dedicated cell phone, this time leaving a voicemail identifying themselves as "HP technical support."

Demurrage also requested that Bandwidth perform a traceback so that the report and the location could be verified as fraudulent and coming from India rather than the United States. Demurrage suggested this because it is most likely that the mark responsible for the creation of these accounts used U.S. credentials to create the accounts, either under false pretenses or through paid accomplices

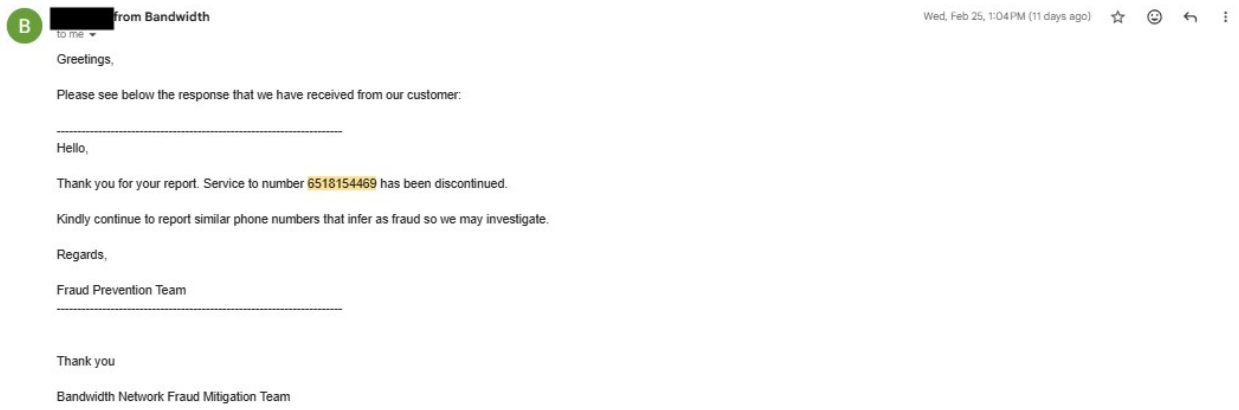
A traceback would be easy for Bandwidth to perform since the calls are routed through its network, yet Bandwidth ignored this request and once again forwarded the new data to RingCentral, avoiding direct action for the second time. Synthi, not a human, received the update and, after a bit of a delay, forwarded it to a support agent at Bandwidth who responded with the following:

> Good Evening,
>
> We have forwarded this information along to our customer to investigate. once we hear back we will let you know.
>
> Thank you,
> Matthew Simmons
> Bandwidth Network Fraud Mitigation Team



A full 24 hours later, RingCentral finally responded and confirmed for the first time since this investigation started that they had shut down a number for fraud, after 12 days.

> Greetings,
>
> Please see below the response that we have received from our customer:
>
> ---
> Hello,
>
> Thank you for your report. Service to number 6518154469 has been discontinued.
>
> Kindly continue to report similar phone numbers that infer as fraud so we may investigate.
>
> Regards,
> Fraud Prevention Team
> ---
>
> Thank you
> Bandwidth Network Fraud Mitigation Team



[redacted] from Bandwidth

to me

Wed, Feb 25, 1:04 PM (11 days ago)

Greetings,

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

Hello,

Thank you for your report. Service to number 6518154469 has been discontinued.

Kindly continue to report similar phone numbers that infer as fraud so we may investigate.

Regards,

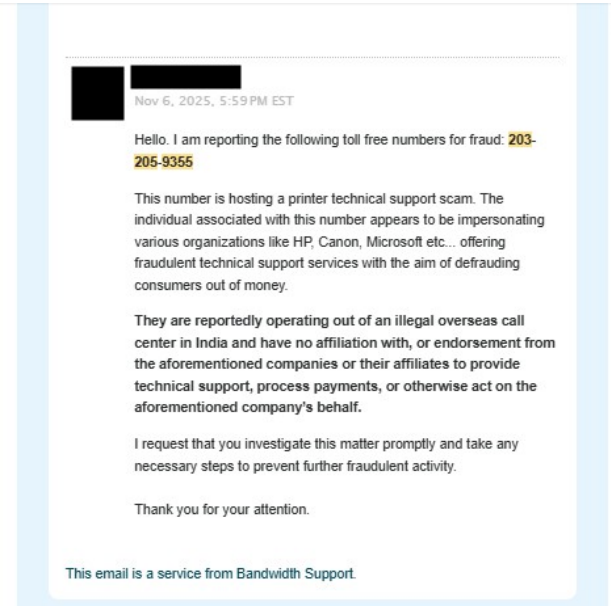
Fraud Prevention Team

Thank you

Bandwidth Network Fraud Mitigation Team

Case 2: 203-205-9355

This is an older case from November 6, 2025, that Demurrage later traced back to the same call center, before Bandwidth phased out its excellent ticketing system for "Synthi."



[redacted]
Nov 6, 2025, 5:59 PM EST

Hello. I am reporting the following toll free numbers for fraud: 203-205-9355

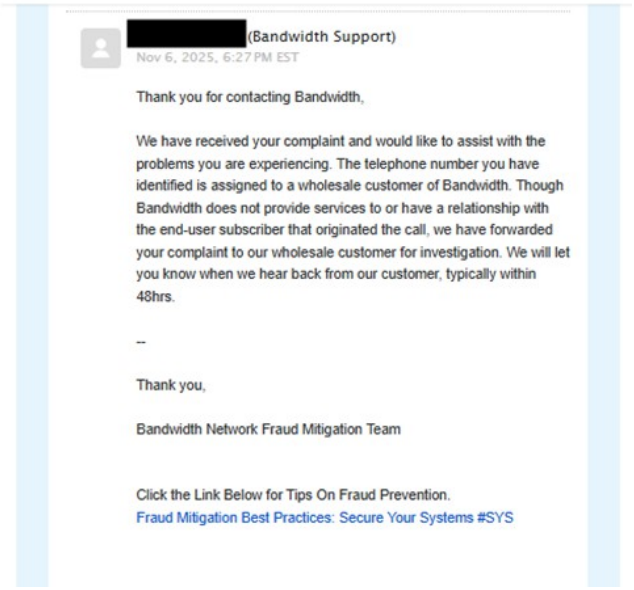
This number is hosting a printer technical support scam. The individual associated with this number appears to be impersonating various organizations like HP, Canon, Microsoft etc... offering fraudulent technical support services with the aim of defrauding consumers out of money.

They are reportedly operating out of an illegal overseas call center in India and have no affiliation with, or endorsement from the aforementioned companies or their affiliates to provide technical support, process payments, or otherwise act on the aforementioned company's behalf.

I request that you investigate this matter promptly and take any necessary steps to prevent further fraudulent activity.

Thank you for your attention.

This email is a service from Bandwidth Support.



[redacted] (Bandwidth Support)
Nov 6, 2025, 6:27 PM EST

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.

--

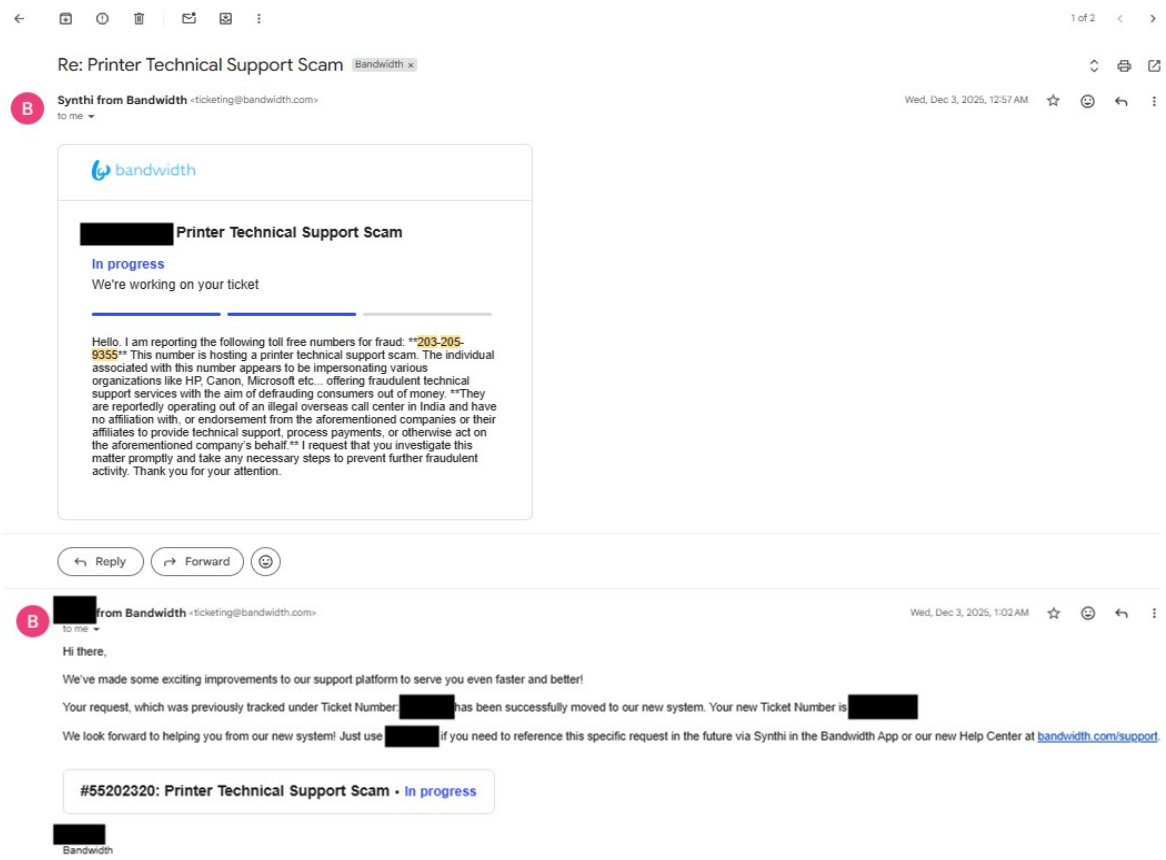
Thank you,

Bandwidth Network Fraud Mitigation Team

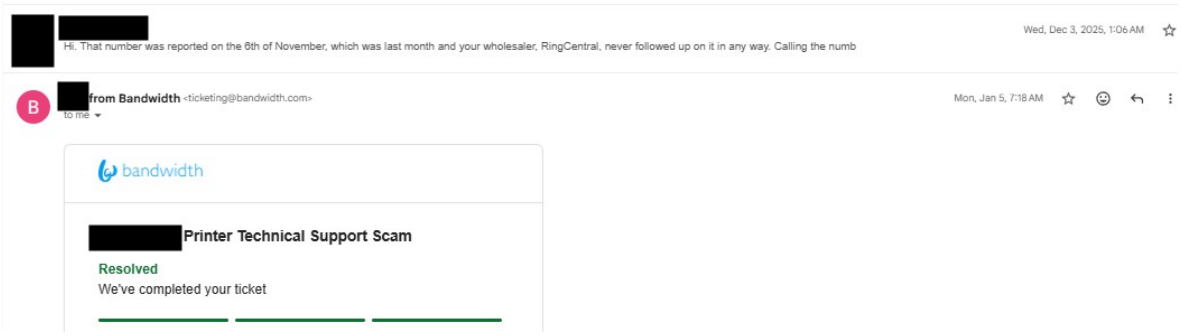
Click the Link Below for Tips On Fraud Prevention.
Fraud Mitigation Best Practices: Secure Your Systems #SYS

Demurrage received a reply from a support agent on November 6, 2025, at 6:27 PM, stating the report was forwarded to the wholesaler in question for investigation. Demurrage did not receive a single update from said wholesaler (RingCentral) or from Bandwidth until December 3, 2025, a month later, and it was from Synthi, which claimed that the ticket was being worked on.

An agent at Bandwidth later responded, stating that the previous ticket was now integrated into the Synthi AI system and was being worked on, a full month after the original report was sent and after the AI system was implemented.



Demurrage relayed this information to the agent at Bandwidth, who then closed the ticket after Demurrage confirmed that the number appeared to have been disconnected. Once again, RingCentral never updated the ticket nor responded to the complaint, to either Bandwidth or to Demurrage, for the entire month of November.



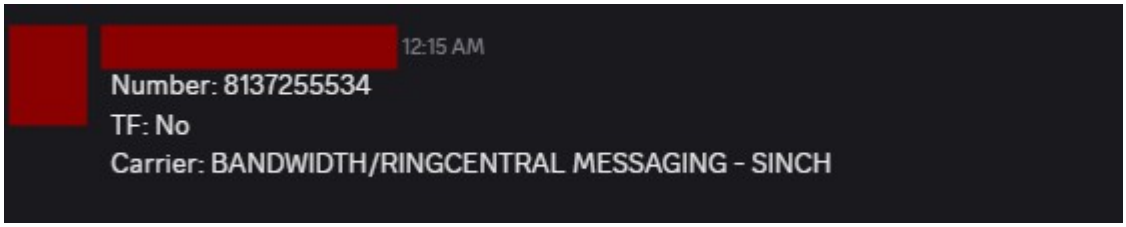
If RingCentral took action, they never claimed responsibility for it, and never once did Bandwidth ask RingCentral to follow up on the status of the case, pre-Synthi or post-Synthi.

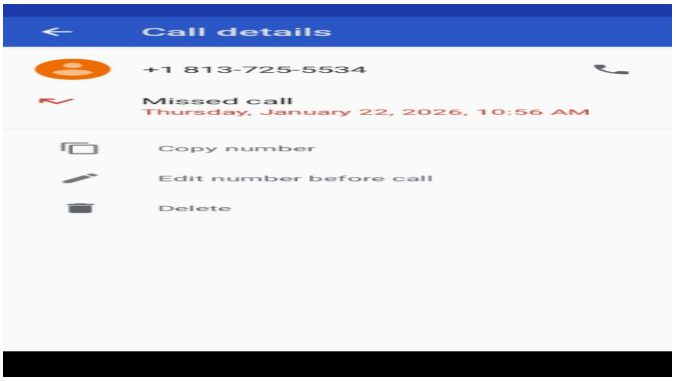
Case 3: 813-725-5534

This is a special case, as it involves SMS services and the confirmation of Demurrage's hypothesis regarding SMS services provided by either Sinch or Bandwidth for RingCentral residential numbers. In this case, Bandwidth was the supplier for this number's SMS services.

On January 22, 2026, at 11:22 AM, a scammer from the same call center called one of the dedicated Demurrage cell phones. Demurrage then returned the call, and a scammer answered the phone, claiming to be "printer support."

Both the screenshot of the call history and the recording were sent to Bandwidth after Demurrage traced the number back to "BANDWIDTH/RINGCENTRAL MESSAGING - SINCH."





Recording:

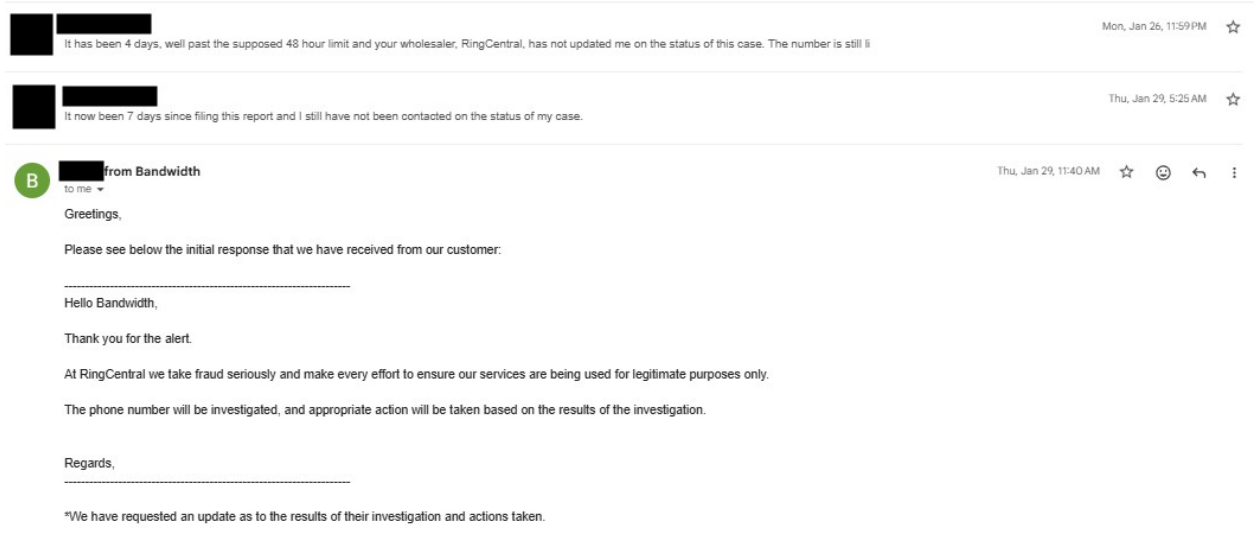
- https://drive.google.com/file/d/1VlRVbGV-eKZ41UxF-RnckBeLe3GoeRYx/view

Because Sinch was involved and has a much longer history of avoiding emails and communicating directly with people who submit fraud reports, Demurrage decided it was better to contact Bandwidth directly, even though the number was most likely having its calls routed through the Sinch network. Given that RingCentral does not reply most of the time, Demurrage did not bother reporting the number directly to them either.

After a slight delay, Synthi forwarded the report to a support agent at Bandwidth, who later forwarded the report to their wholesaler (RingCentral).

No further updates were received from Bandwidth or RingCentral. On January 26, 2026, after four days, Demurrage followed up, stating that the allotted 48-hour time limit for a response from the wholesaler had long since expired. No one at Bandwidth or at RingCentral responded to the update from Demurrage.

On January 29, 2026, after seven days, Demurrage once again followed up, stating that RingCentral had not updated the status of the case. Several hours later, RingCentral finally responded with the same stock reply shown previously, only this time, Bandwidth requested that RingCentral provide an update on the results of RingCentral's investigation.


[redacted]
It has been 4 days, well past the supposed 48 hour limit and your wholesaler, RingCentral, has not updated me on the status of this case. The number is still li
Mon, Jan 26, 11:59 PM

[redacted]
It now been 7 days since filing this report and I still have not been contacted on the status of my case.
Thu, Jan 29, 5:25 AM

B [redacted]from Bandwidth
to me
Thu, Jan 29, 11:40 AM

Greetings,

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

Hello Bandwidth,

Thank you for the alert.

At RingCentral we take fraud seriously and make every effort to ensure our services are being used for legitimate purposes only.

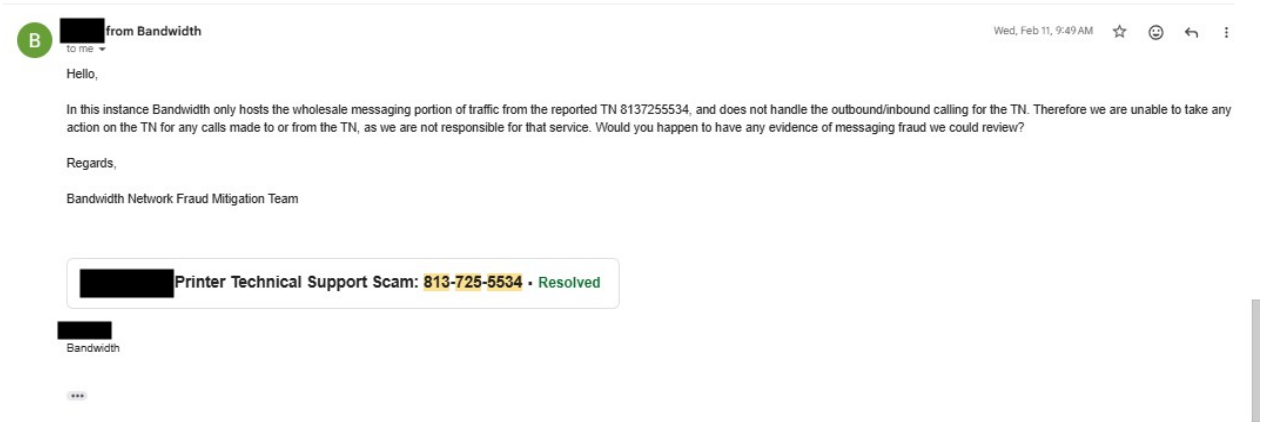
The phone number will be investigated, and appropriate action will be taken based on the results of the investigation.

Regards,

---

*We have requested an update as to the results of their investigation and actions taken.

On January 30, 2026, eight days later, the number was still live. Demurrage followed up again. This time, Bandwidth stated the following:



Because Demurrage now knows that Bandwidth can directly take action against a number if evidence of SMS fraud is occurring, it raises the question: why have they not done the same thing for the previous two cases? What makes SMS different?

The calls for the previous two cases were all being routed through Bandwidth's infrastructure and network.

Of course, Demurrage did not have a text message since the scammer did not send one. What Demurrage reported was fraudulent use of a phone number. Nevertheless, Bandwidth closed the case, and the number remains live and goes to voicemail as of this writing, with no action taken by RingCentral whatsoever.

Recording:

- https://drive.google.com/file/d/1OCsSOBSSBkhoma1FmifgcAHkrCMZSmQK/

The Most Responsible Telecom In The Industry: Lumen & The Abuse of The Level 3 Network

The actions of Bandwidth are in direct contrast to the next telecom that also routes calls for RingCentral through its infrastructure: Lumen, through the Level 3 network.

Where Bandwidth fails to step in and take direct action against the “marks” and wholesalers on its network, Lumen takes a different approach and has consistently proven to be the most effective telecom regarding eliminating fraud from its network when cases are submitted.

In fact, Lumen's track record has been so consistent that Demurrage has only ever encountered two cases where Lumen did not adequately respond in the six years that Demurrage has been active as a unit. Lumen quickly corrected these mistakes and took action immediately after receiving new data. While the first case does not involve the current batch of RingCentral numbers, it bears noting that Lumen corrected its mistake within an hour of new data being sent to them, and on the same day of receiving that data.

All the cases involving RingCentral numbers were reported to Lumen at the following address: ***fraudoperations@lumen.com***

Case 4: 518-631-3721

This number was referenced in the toll-free section of this report, in which a screenshot was presented of a support agent at Lumen believing that the account associated with the number appeared to be legitimate. The agent told Demurrage to give it some time before following up and did not place a temporary block on the number. As stated earlier, the mark responsible for making these accounts must have used extremely convincing details to fool Lumen.

Demurrage sent a report to Lumen on February 19, 2026, at 4:04 PM with the following recording of the scammer answering the phone, claiming to be "support," along with the timestamps of the call so that Lumen could verify the timestamps and trace back the call:

- https://drive.google.com/file/d/1BHxfl46sio_SRCdwKgJdRxhYyUethnEL/view

On February 19, 2026, at 4:04 PM, Lumen responded with the aforementioned response of the account looking legitimate. Although Demurrage replied, stating to Lumen that RingCentral has a long history of ignoring reports and not responding, Lumen assured Demurrage that its wholesaler, who was its customer, would respond and was responsive.

Demurrage waited until February 23, 2026, all the while the number remained live and was answered as "support" and as "printer support" by the scammer. At this point, Demurrage followed up, stating that no such reply from Lumen's wholesaler or RingCentral was received within the last five days.

Demurrage once again called the reported number, and the scammer once again answered as "support." A new recording and new timestamps so that Lumen could trace the call back were sent to Lumen in the original email chain.

Recording:

- https://drive.google.com/file/d/1KNLh1N-1giBLPsY8oLAzxZST4Ykfxrx4/view

This time, Lumen acted and placed a block on the reported number while the wholesaler allegedly investigated the claims in the report. Lumen even went as far as calling the number themselves but received a "disconnection message."

Demurrage then replied by stating that if the agent had called with a VoIP number, the calls would not go through, as scammers and marks are now blocking VoIP numbers due to what they call "prank calls" by scambaiters.

Lumen's approach to blocking the number temporarily is the most effective Demurrage has seen other than a complete disconnection of the number, as the “marks” who sell these accounts do not attempt to fight off the block. Instead, they move on and must make a new account for their scammer client list, which costs both the “mark” and the scammers more money.

As expected, the number is still blocked, and the scammers have not tried to reclaim it, marking this one of two rare instances where Lumen had to correct a mistake during this investigation.

Case 5 & 6: 818-230-2770, 858-529-8920

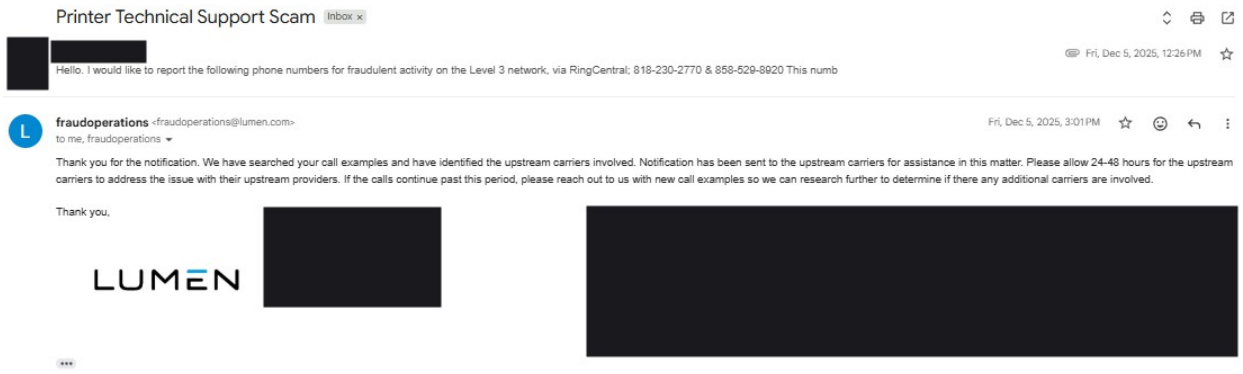
On December 5, 2025, at 12:26 PM, Demurrage reported 818-230-2770 and 858-529-8920 to Lumen after 818-230-2770 called one of Demurrage's dedicated cell phones, leaving a voicemail in which the scammer claimed to be "support." Number 858-529-8920 was sent to Demurrage by AVAHS. After calling 858-529-8920, Demurrage acquired a recording of the scammer answering the phone, claiming to be "support." Demurrage sent all of this data to Lumen, which can be found below:



Recordings:

- https://drive.google.com/file/d/1jVl6L6ybJWCX0nTMsHpA-GrVG-feWUxg/view
- https://drive.google.com/file/d/1LLKrj3TMehbeN-0Oe4WJqZa5qvxRk_Of/view

On the same day, Lumen responded by placing a temporary block on both numbers while they forwarded the report to the wholesaler in question. As of this writing, both numbers are still blocked by Lumen, and the scammers have made no attempts to reclaim the numbers.



This marks the last residential number linked with these printer scammers. The next batch of cases are unrelated yet were all traced back to RingCentral through Lumen's Level 3 network and to tech support scammers operating out of illegal call centers in India.

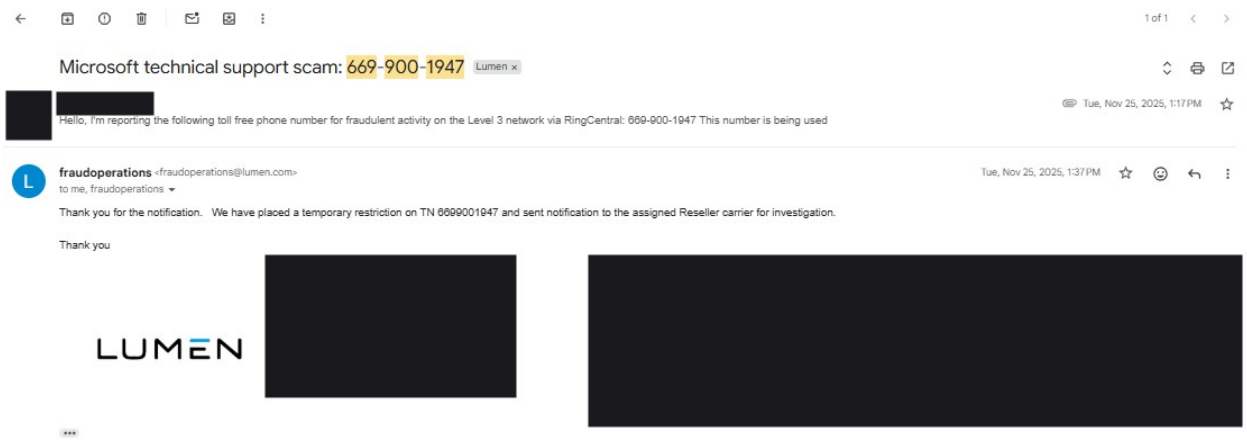
Case 7: 669-900-1947 (Microsoft Technical Support Scam)

Demurrage acquired this callback from a teammate who called a pop-up that had a toll-free number hosted on a different telecom. Using the dedicated cell phone, Demurrage called the number to verify its use and, after acquiring a recording of the scammer answering the phone claiming to be "Microsoft support," reported the number to Lumen on November 25, 2025, at 1:17 PM.

Recordings:

- https://drive.google.com/file/d/1scN1YwDZHEPKjfGPM-EoWtL81FMAaLNM/view

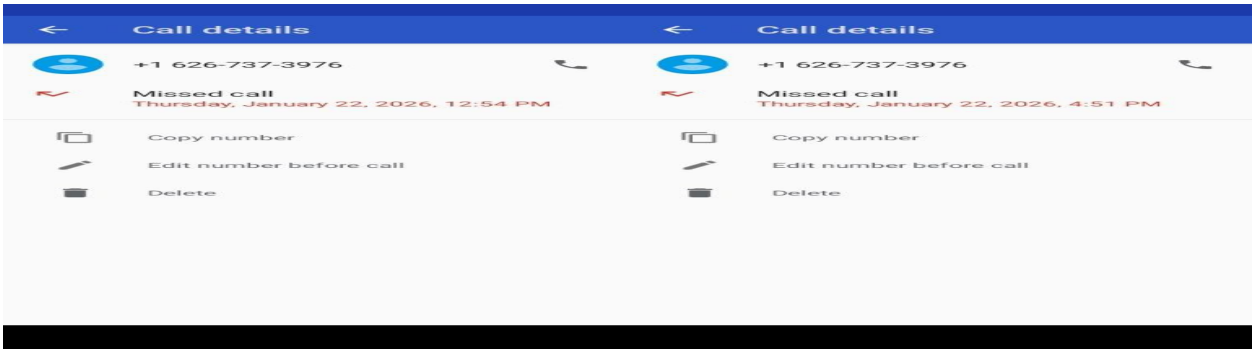
At 1:35 PM, Lumen responded to the report by placing a temporary block on the number while they forwarded the report to the wholesaler for investigation. As of this writing, the scammers have not attempted to reclaim the number, and it is still blocked by Lumen.

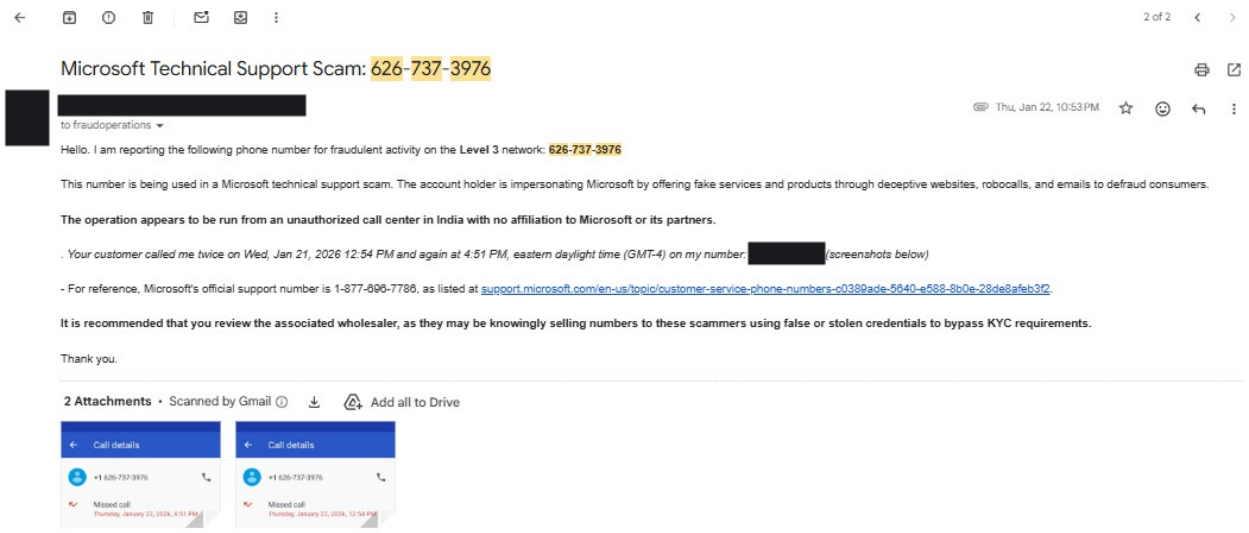


Notice how the only time RingCentral numbers can be actioned is when they fall under the Lumen umbrella. No other telecom that hosts RingCentral, including RingCentral itself, is this effective at stopping scammers from further abusing RingCentral's services.

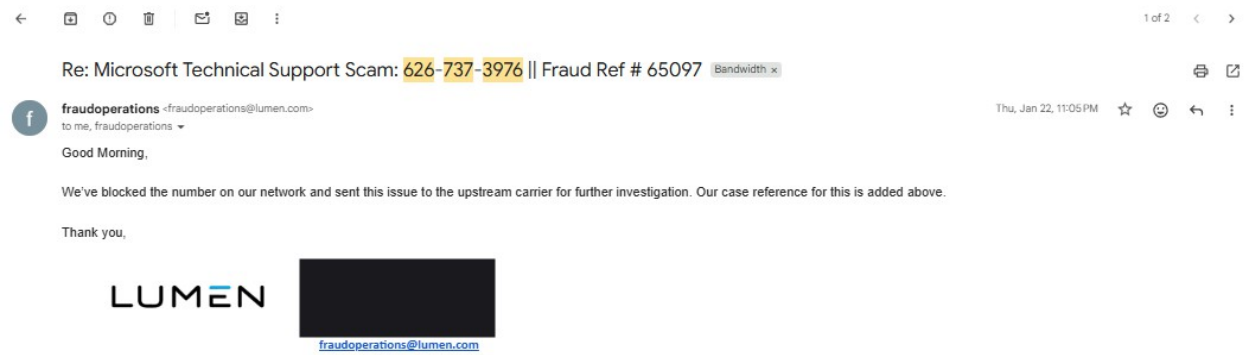
Case 8: 626-737-3976 (Microsoft Technical Support Scam)

This number was used as a callback number by scammers running a Microsoft pop-up campaign that used a toll-free number on a different telecom. After calling the toll-free number on the pop-up with one of the dedicated cell phones, Demurrage received two calls from 626-737-3976. The scammer did not leave a message, but the screenshots of the call history were sent to Lumen on January 22, 2026, at 10:53 AM.





At 11:05 AM, Lumen responded to the report by checking the account and placing a temporary block on the number while sending the report to the wholesaler for investigation. As of this writing, the number is still blocked by Lumen, and the scammers have not attempted to reclaim it.



Case 9: 424-704-5986 (Computer Technical Support Scam)

This number was used as a callback number by scammers running a generic computer pop-up campaign that listed the number as "computer technical support."

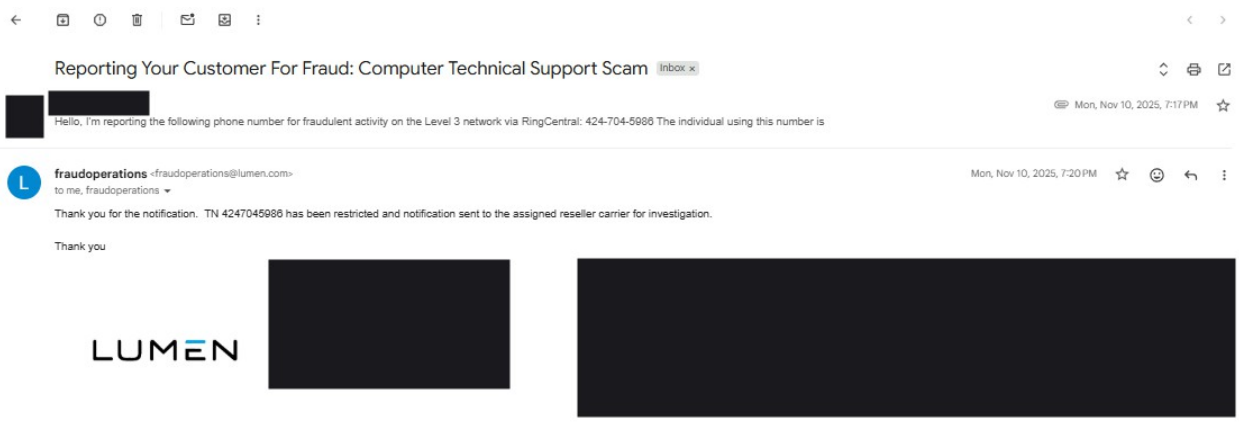
After calling the number on the pop-up with one of the dedicated cell phones, the scammer answered the phone and claimed to be "support." The recording was sent to Lumen on November 10, 2025, at 7:17 PM.

Recording:

- https://drive.google.com/file/d/1UWKkR2JISv_c7xV_LJayU0Y3sX1sv8Rj/view

Ignoring the fact that these residential numbers, which are supposed to be used by and for the general consumer market, are being answered as "support" by scammers overseas, it should be noted that scammers running technical support scams out of call centers in India almost always answer the calls as "support" to avoid being reported for impersonation.

At 7:20 PM, three minutes later, Lumen responded to the report by checking the account and placing a temporary block on the number while sending the report to the wholesaler for investigation, breaking their previous record set in 2023 of six minutes by three minutes. As of this writing, the number is still blocked by Lumen, and the scammers have not attempted to reclaim it.



Closing Statements

The data collected by Demurrage was done so independently. Demurrage is not paid by outside entities for this work and has never made any profits during its six-year tenure investigating numbers associated with tech support fraud.

Demurrage follows the data, and what has been observed so far is that many of the same RespOrgs and telcos are consistently being exploited by scammers overseas. While many governing bodies still focus solely on robocalls, it should be noted that the same problems with reporting robocalls to the telecoms that have numbers traced back to them still apply with the findings of this report.

It should not be this difficult to get a number shut down for fraud regardless of which telecom is involved. As has been seen with Lumen, it is not impossible for RespOrgs to step in directly and block a phone number reported as being used in a scam. Fines have already been sent to some telecoms more than once, yet no significant progress is being made to stop “marks” from selling these numbers to scammers overseas.

If telecoms are serious about tackling fraud, more must be done on their end. Telecoms must start taking steps to identify “marks”. Once they are identified, action must be taken by putting them on corrective plans or removing them from their networks entirely. RespOrgs must also concede that their KYC practices and policies have failed structurally and that checks are being evaded without disruption for years. The data reveals the truth: most tech scams are enabled by this systemic failure.

The governing bodies regulating the telecom industry must also step in and take direct action against telecoms (be they RespOrgs or straws) to hold them accountable for turning a blind eye to fraud on their platforms.

All telecoms, RespOrgs most of all, should have accessible and functional reporting channels. RespOrgs like Sinch and Commio refuse to look at fraud reports through email and instead redirect consumers to inadequate webforms that do not have the option to submit any evidence whatsoever and burden reporting efforts. Evidence is often demanded by downstream telcos, further squandering opportunities to help prevent victimization.

Demurrage is committed to reporting these numbers to the telecoms in question, as it truly wants to see this problem solved, but it can only happen if telecoms start to

seriously look into their own infrastructure and handle these reports firsthand. Lumen, Callture, TextNow, Go Text Me, and Vonage have dedicated people looking at these reports and taking direct action against scammers abusing their services. More RespOrgs need to adopt Lumen's model if a complete disconnection is something they do not wish to do. Tech scams operate for about three hours per popup. Any response window over 24 hours is too long, and 48 hours is ancient history. Lumen has been shown to consistently handle these abuse cases on the same day, even within minutes. In this way, they are able to consistently help prevent victimization on their network, fulfilling their duty as a RespOrg to protect the public.

No telecom should be allowed to leave reports unanswered for weeks or let alone a month on a consistent basis the way Bandwidth allows RingCentral to do, whether inadvertently or not, some corrective action must be initiated. Tracebacks must also become standard practice, as these would easily prove that U.S. residential numbers are being used by scammers overseas with accounts supposedly verified for KYC using "real" U.S. credentials and information.

All telcos exist in a position of trust in our society, and Responsible Organizations particularly so. Large RespOrg wholesalers have been granted the privilege in the US to arbitrate much of the toll free telecom industry and are its foundation, a privilege that affords them profit in exchange for their commitment to shepherd the industry. Therefore, Demurrage believes that as a moral minimum RespOrgs should investigate at least a portion of reports filed against downstream clients in-house, with capable human beings and in a timely manner.

The investigations should serve to validate that reports are in fact being handled downstream and to approximate the level of abuse with the provider. Without this groundwork, RespOrgs are fundamentally unable to do their duty to the public and prevent bad actors from exploiting their networks, but they nonetheless profit from their failure to do so. Large RespOrgs naturally should maintain practices to identify telcos on their networks primarily serving fraudsters and implement plans to place such entities on corrective action plans or terminate relationships promptly upon detection.

Demurrage urges examination of this evidence and action without delay.

Glossary

Residential numbers

These are ordinary consumer phone numbers assigned to households or individual end users. In practice, they are the kinds of numbers people expect to belong to a private person or home user, rather than to a business, call center, or telecom provider. In scam and fraud discussions, the term often matters because calls from numbers that appear "residential" may seem more trustworthy or less suspicious.

VoIP numbers

VoIP stands for Voice over Internet Protocol. A VoIP number is a phone number that works over an internet-based telephony service rather than a traditional fixed copper line or conventional mobile network. To readers in Europe and Oceania, it may help to think of these as numbers provisioned by cloud telephony providers, SIP providers, hosted PBX services, or online business calling platforms. A VoIP number can still look like a normal local, national, or toll-free number to the person receiving the call.

Wholesalers

In the telecom industry, wholesalers are base level carriers or providers that sell voice capacity, routing, numbering access, or termination services to other telecom companies rather than directly to users. These wholesalers generally hold RespOrg status and part of their capability includes registering new numbers with the NANP. Wholesale telecoms are part of the supply chain behind how calls are carried between networks, service providers, and countries. Essentially, they are the foundation of the commercial telecom industry and have strong interface with regulatory and oversight entities that reselling telecoms generally do not have.

THE END.