Emerging Trends in Phone Scams

FVRO

THE FRAUD VICTIM RIGHTS ORGANIZATION

Introduction

Since 2013, phone scams effecting Americans have primarily involved Voice over IP (VoIP) calls. These calls come in two types.

1. Outbound calls where the originating number is spoofed.
2. Distribution of VoIP Direct Inward Dial (DID) or toll-free numbers that allow potential victims to self-select by calling back in response to calls, texts, e-mails, or computer pop-up ads.

In mid-2024, transnational fraud groups appear to have started migrating to using prepaid SIM cards from U.S. wireless carriers for both of the above types of scams.

Impacts of Outbound Voice Call Scams

Outbound voice calls are used in a variety of scams. The most frequently reported voice call scams are business and government impersonation.

Americans reported $1.48 billion in business and government impersonation loss to the FBI and FTC in 2023.

By Complaint Loss ▼ ▲ = Trend from previous Year			
Crime Type	*2023*	*2022*	*2021*
Government Impersonation	$394,050,518 ▲	$240,553,091 ▲	$142,643,253 ▲

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf; page 23.

Subcategory	# of Reports	Total $ Lost
Business Imposters	315,270	$632.6M
Government Imposters	148,430	$444.2M

Source: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts > Subcategory Payment & Contact Methods > 2023

FVRO

Outbound Caller ID Spoofing

While use of DID and toll-free numbers is more common in most phone scams since mid-2021, outbound caller ID spoofing via VoIP is still common—especially for law enforcement impersonation calls.

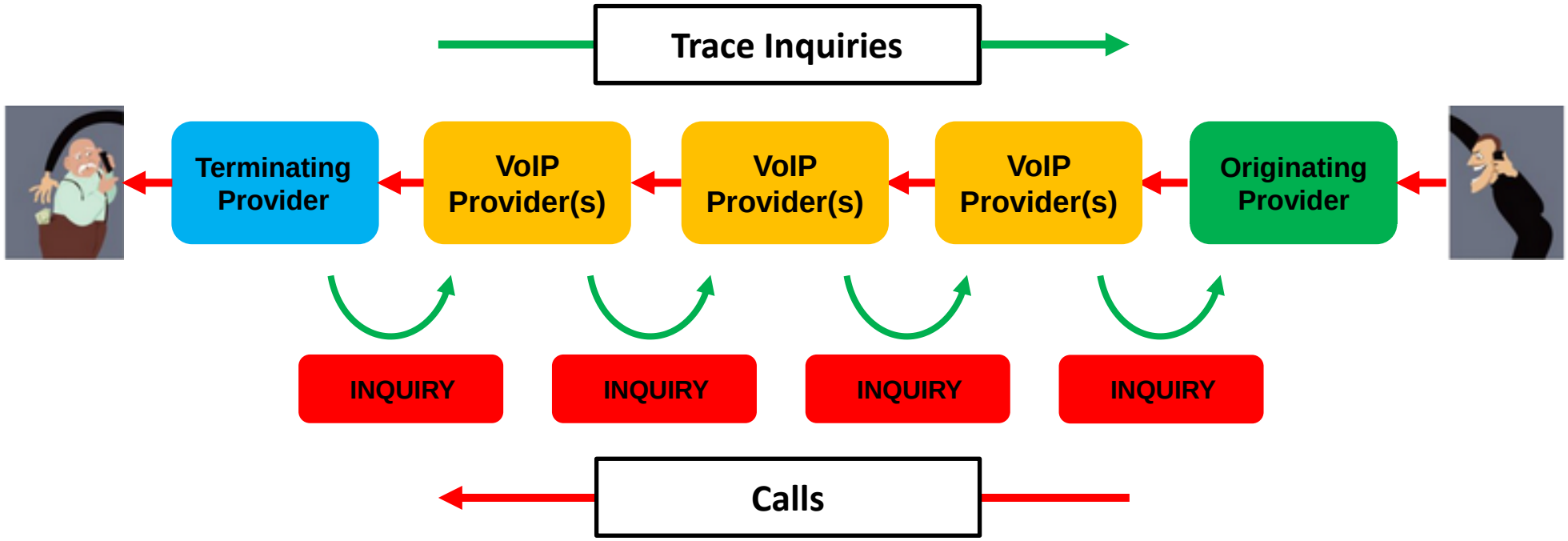
LOS ANGELES COUNTY SHERIFF – SCAM ALERT

Los Angeles County Sheriff's Department would like to warn the public of phone call scammers Impersonating L.A. County Deputies using spoofing apps that show their number on the victim's caller ID as the Sheriff's office or local police agencies.

FVRO

Tracing Spoofed Calls

While outbound spoofed calls are harder to trace than call back numbers, it is still relatively easy to trace spoofed calls.



FVRO

Wireless Numbers Used for Call Scams

While most scam voice calls originate via wholesale VoIP from overseas, beginning in Q2 2024 FCC traceback data has indicated that transnational fraud groups—pressured and deterred by industry traceback efforts—have started using prepaid wireless numbers.

Scam groups can do this by having third-parties purchase and activate prepaid SIMs. These SIMs can then be loaded into SIM boxes. Calls can then be made from U.S. wireless networks even if the SIMs and scam call centers are in other locations anywhere in the world.

Unlike VoIP calls, calls from SIM gateways cannot be traced to the call originator without physical access to the actual equipment used. The physical equipment, however, can be geolocated and seized.

FVRO

FCC Traceback Data

Every quarter the FCC issues a traceback transparency report with statistics about suspected scam calls traced by the telecom industry. The Q3 2024 traceback report indicated 23% of traced calls originated from U.S. wireless providers.

Provider	Traced Calls	First Trace	Last Trace
T-Mobile USA, Inc.	151	07/02/24	09/30/24
Ananya traders llc	59	07/01/24	09/30/24
Verizon	37	07/02/24	09/23/24
Sipphony, LLC	24	07/10/24	09/24/24
Vonage	21	07/01/24	09/26/24
SK TELECO LLC	19	07/09/24	07/19/24
Stacy Newsome LNCC	19	07/22/24	09/03/24
Voice Fetch	18	09/11/24	09/23/24
AT&T	17	07/02/24	09/30/24
Voip Torque	17	08/06/24	09/19/24
191 Other Providers	500	07/01/24	09/30/24

Source: https://www.fcc.gov/document/fcc-releases-traceback-transparency-report-3

FVRO

Wireless Numbers Used for Call Scams (Cont.)

Descriptions of traced calls in the FCC transparency report indicate calls are primarily coming from India (e.g. Amazon and authorized order calls).

Provider	Traced Calls	First Trace	Last Trace	Call Description
T-Mobile	124	07/02/24	09/30/24	Authorized-Order-P2 Order Scam
Verizon	31	07/02/24	09/23/24	Authorized-Order-P2 Order Scam
AT&T	15	07/02/24	09/30/24	Authorized-Order-P2 Order Scam
T-Mobile	12	07/31/24	09/16/24	Amazon-AuthorizeOrder-P3 Amazon
T-Mobile	8	07/19/24	09/17/24	Amazon-Various-P1 Amazon
Verizon	3	07/02/24	09/10/24	Amazon-Various-P1 Amazon
T-Mobile	3	07/11/24	07/19/24	Authorized-Order-P1 Order Scam
T-Mobile	2	08/13/24	09/18/24	Authorized-Order Order Scam
Verizon	2	08/23/24	08/23/24	Unsolicited-Calls-Spoofed-P2 Impersonation
AT&T	1	09/12/24	09/12/24	Authorized-Order Order Scam
Verizon	1	07/02/24	07/02/24	Authorized-Order-P1 Order Scam
AT&T	1	09/25/24	09/25/24	Amazon-Various-P1 Amazon
T-Mobile	1	09/17/24	09/17/24	Chinese-ISP/Cable/Wireless-Impers-P1 Cable/Phone Impersonation
T-Mobile	1	08/21/24	08/21/24	Amazon-AuthorizeOrder-P2 Amazon

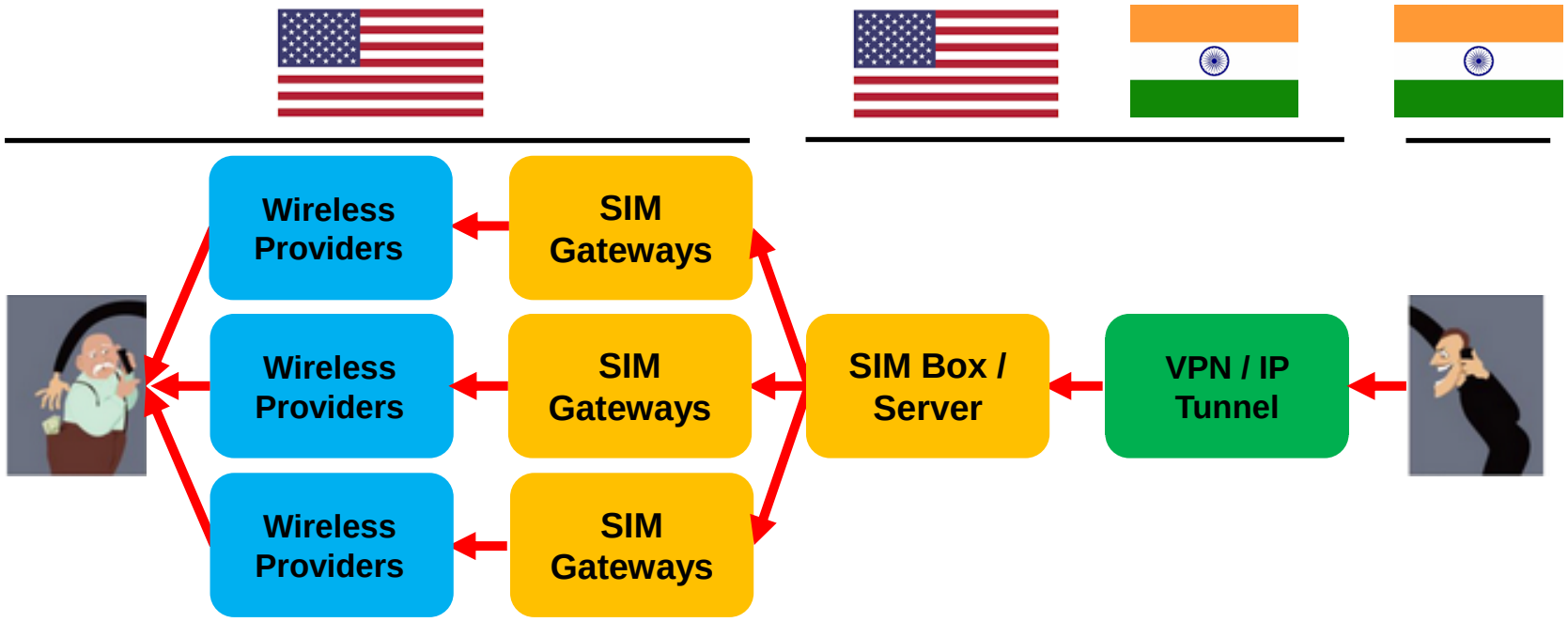
Sources: https://www.fcc.gov/document/fcc-releases-traceback-transparency-report-3
https://www.fcc.gov/document/fcc-releases-traceback-transparency-report-2

FVRO

SIM Boxes

Scam calls from foreign fraud groups that appear to come from prepaid SIM cards most likely originate from SIM boxes.

SIM boxes and SIM gateway devices allow criminals anywhere in the world to transmit calls from other locations anywhere in the world.



FVRO

Locating SIM Boxes

SIM boxes can be located though:

- CDR and IMEI analysis;
- Historical cell site analysis;
- Radio frequency triangulation;
- Data mining 7726 spam complaints (in the case of message spam);
- Examination of payment records;
- Activation records; and
- SIM shipment records.

➢ **Law enforcement agencies with questions about methods for detecting illegal SIM box activity, including specific crimes to charge, should contact the author directly.**

Impacts of Inbound Voice Call Scam Call Back Numbers

Tech support fraud scams primarily make use of DID and toll-free call back numbers distributed by computer pop-up ads and e-mail messages.

Americans reported $1.13 billion in business and government impersonation scam loss to the FBI and FTC in 2023.

By Complaint Loss ▼ ▲ = Trend from previous Year			
Crime Type	*2023*	*2022*	*2021*
Tech Support	$924,512,658 ▲	$806,551,993 ▲	$347,657,432 ▲

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf; page 23.

Subcategory	# of Reports	Total $ Lost
Tech Support Scams	56,255	$202.7M

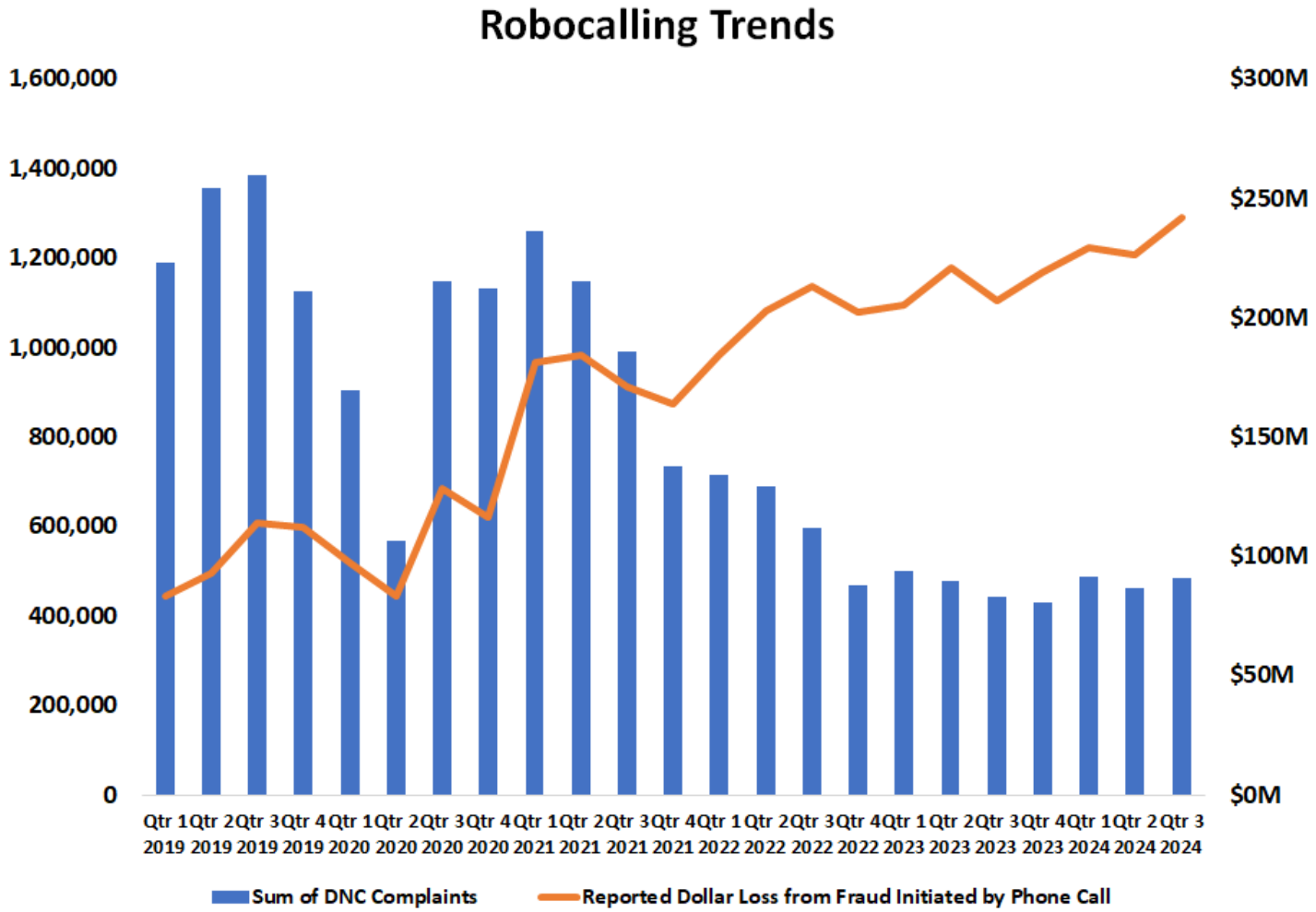
Source: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts > Subcategory Payment & Contact Methods > 2023

FVRO

Phone Fraud Trends

Since July 2021, consumer complaints about unwanted calls have declined 58% due to FCC registration requirements for VoIP providers and the deterrent effect of call tracing.

Meanwhile, reported loss from fraud initiated by telephone has increased 32% due to criminal groups in India switching from outbound spoofed calls to pop-ups and e-mails with call back numbers.



Source: https://public.tableau.com/app/profile/federal.trade.commission/viz/DoNotCallComplaints/Maps > Robocalls
https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts > Contact Methods

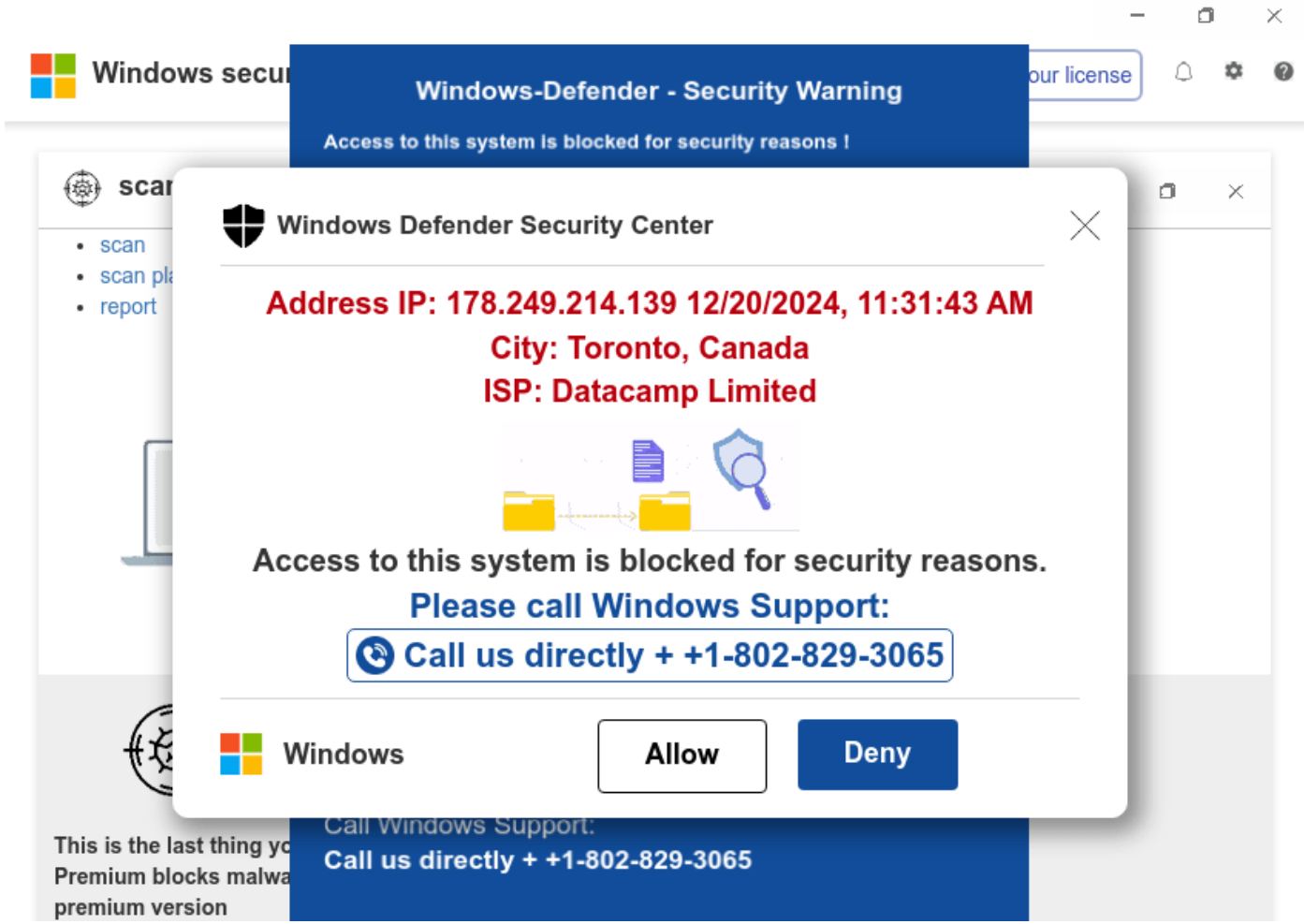
FVRO

Tech Support Fraud Computer Pop Ups

Tech support fraud is usually initiated through computer pop-up ads with toll-free or VoIP DID call back numbers.

This image was posted on the message board scammer.info on December 20, 2024.

(Note the number displayed has most likely since been recycled to a different user.)

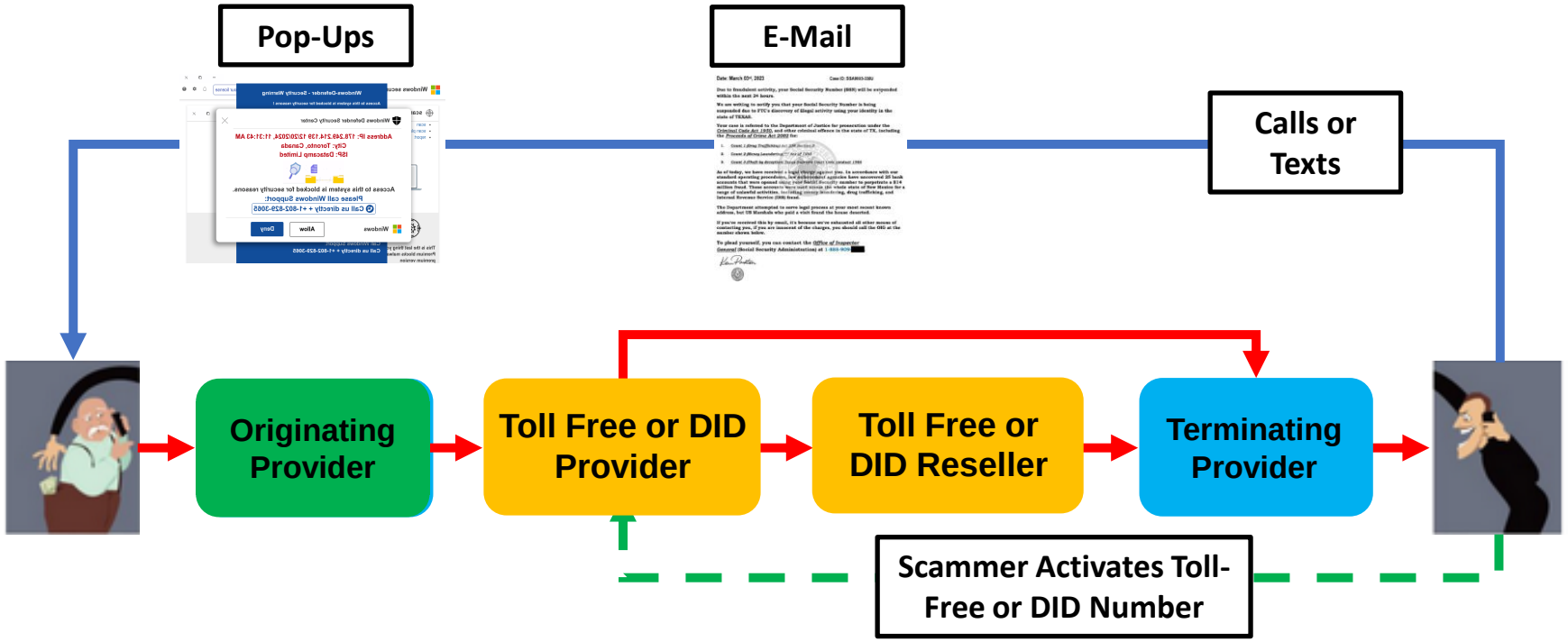


Source: https://scammer.info/t/demurrage-popup-scanner/147342/7147

FVRO

Call Back Number Routing

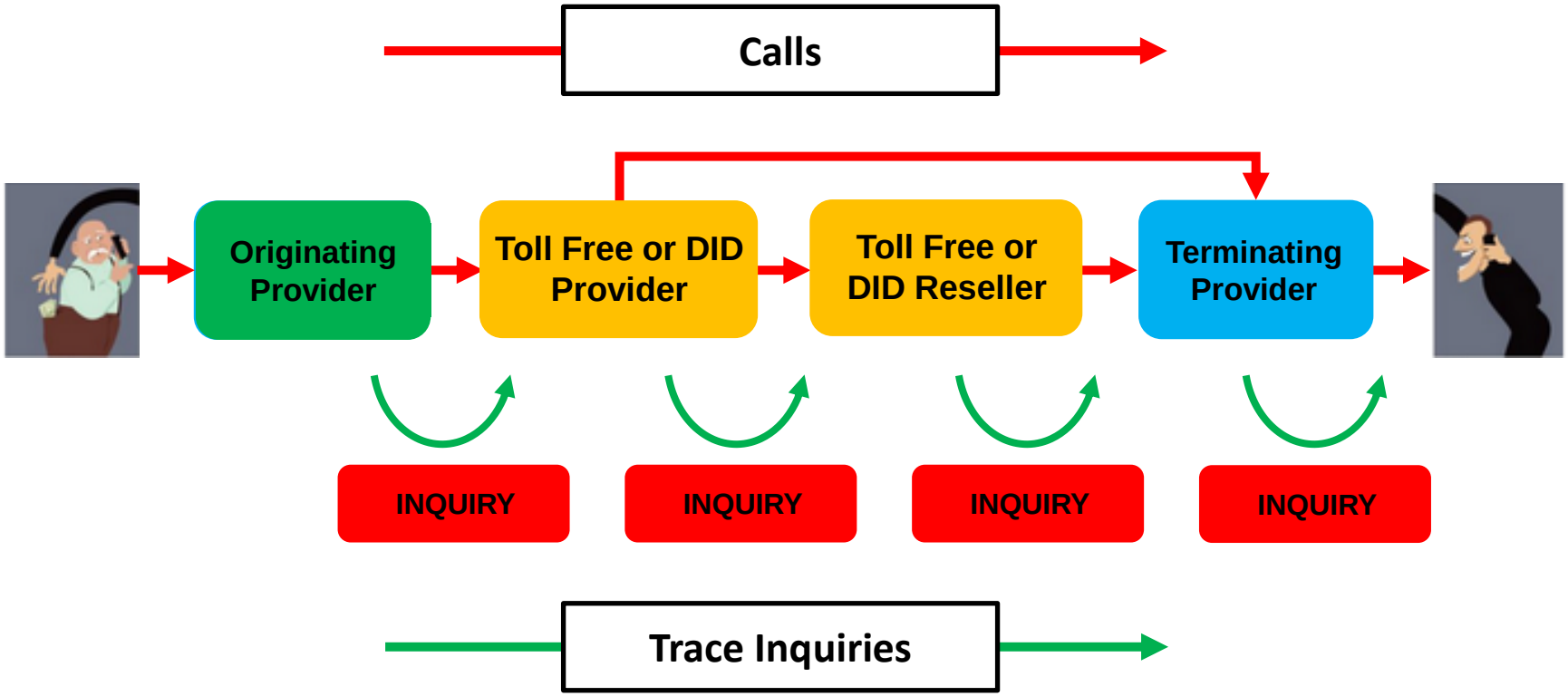
Call back numbers are distributed by computer pop-up and e-mail. Potential victims can self-select by calling back.



FVRO

Tracing Call Back Numbers

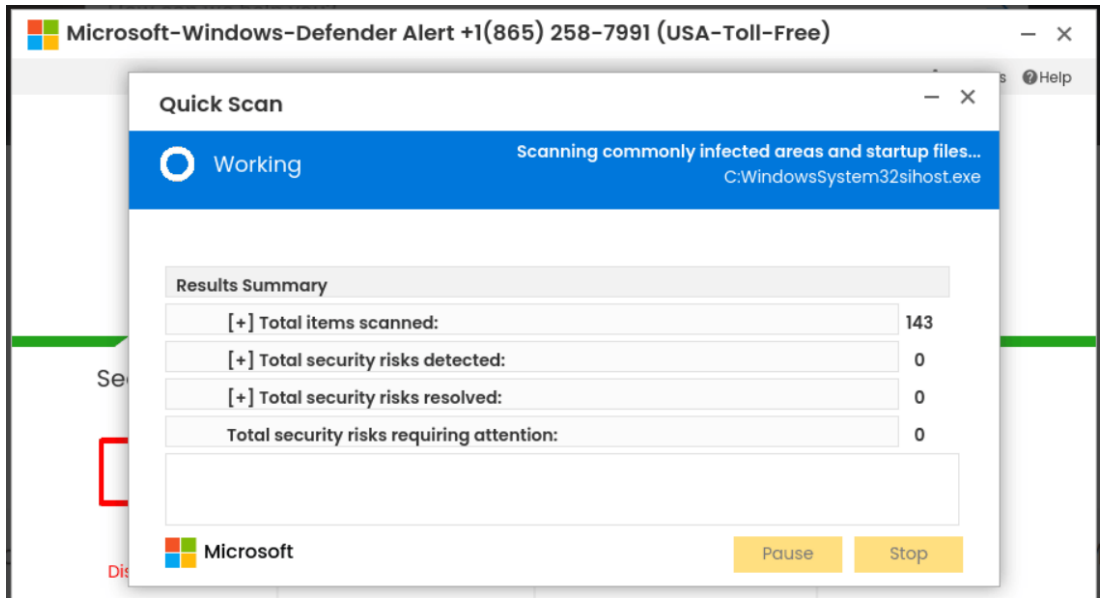
These call back numbers can be easily traced to the locations of scammers because scammers must own these numbers in order to receive calls from victims.



FVRO

Call Back Scams Using Wireless Numbers

In October 2024, a major wireless carrier appears to have been the 2nd most frequently used carrier for call back numbers appearing on tech support fraud pop-up ads.



Source: (right) https://scammer.info/t/demurrage-popup-scanner/147342/5611
(left) https://scammer.info/t/demurrage-popup-scanner/147342/5556

(Note the numbers displayed have most likely since been recycled to different users.)

FVRO

Call Back Scams Using Wireless Numbers (Cont.)

Another major wireless carriers' numbers appeared on fake tech support e-mail messages in October 2024.

McAfee

Date: Wednesday, October 23, 2024
Transaction Receipt Id: 97856-3994
Payment id: 517-20-475-1044

Your membership is now active.

Salutations, **[REDACTED]**

Payment Renewal Alert: This is to inform you that your McAfee service will automatically renew in the next 24 hours, with $657.75 set to be deducted from your account for the next 72 Months.

Continue as Normal: If you wish to keep your service active, no need to reply to this message. For cancellations or inquiries, you can reach out to our support team at **1{8O3} 381-1279**.

Sale Information
[REDACTED]

Membership Auto-Renewal:
*Your membership with McAfee has auto-renewed, and the payment is now due. Should you want to cancel or request a refund, kindly contact Billing Support at **1{8O3} 381-1279**.*

Best Sending Wishes,
The McAfee, LLC.
Operational Head: Justin Olson
Address: 3700 Highland Drive #3 Sanford Nc 27330 US

PAYPAL

Helpline Number: + 1 (806) 787-3548

Billed to: **[REDACTED]**

Invoice Number: 2410281P2EIW Date: October 28th, 2024.

Good day,

Your Transaction has been authorized by your PayPal and it's have been successful.

We're pleased that you chose Norton protection as your computer security provider. Due to the auto renewal date, your antivirus protection plan will expire today and you will be charged $246.83 as of today. It will be taken out instantly from your bank's checking account. The charges will appear on your statement in the next 48 hours.

PRODUCT DETAILS :-

Account Type:- Personal Home Subscription
Product: Norton 360 Platinum Plan
Device: Windows Computer (3 Users)
Quantity: 1
Tenure: 3 Years
Mode: Auto Debit (PayPal Wallet) Verified Checking account

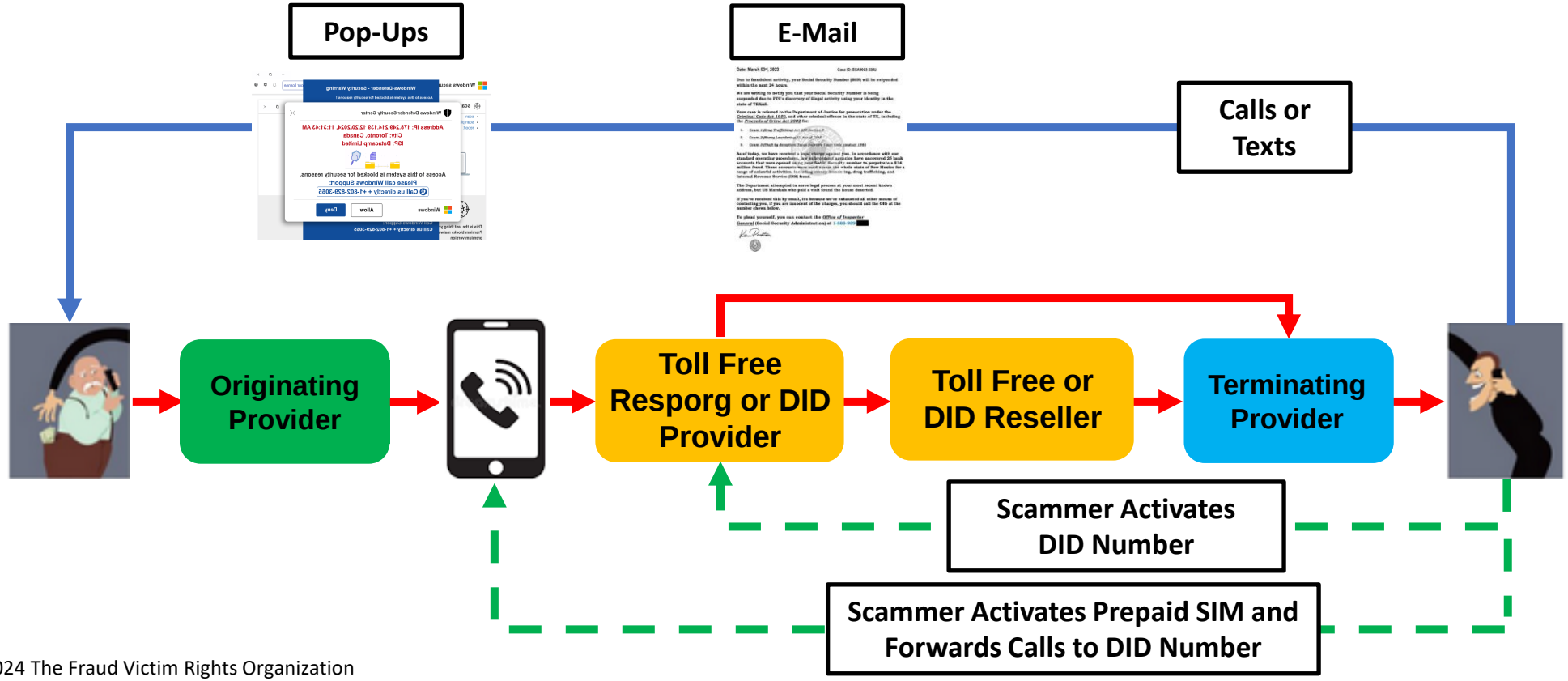
Renewal Amount - $246.83

However, you can contact us at our helpline number, **+ 1 (806) 787-3548** For you any kind of assistance or if you are having any kind of trouble regarding this transaction do reach us.

(Note the numbers displayed have most likely since been recycled to different users.)

Wireless Number Call Back Routing

These wireless numbers could indicate prepaid SIMs being used to mask call back DID numbers. Scammers can activate prepaid lines, program call forwarding to DID numbers, and then dispose of the SIM.



Driving Deterrence

DID and toll-free call back numbers, outbound spoofed calls, prepaid SIMs used to forward calls to DID numbers, and SIM gateway devices can all be traced to their source locations.

Once scammers realize any use of this technology can lead to enforcement actions in their home countries, they will be forced to abandon the most effective means of contacting potential victims.

To accomplish this, U.S. wireless carriers need to obtain attributary evidence and send it to both U.S. and foreign law enforcement as soon as possible.

- **Wireless carriers with questions about effective FMS alarms for this type of activity should contact the author directly.**

Implications for Policy Makers

1. The pipeline of criminal cases from U.S. to Indian law enforcement needs to be significantly expanded.
2. U.S. law enforcement does not need to wait years to fully develop cases before sending leads to Indian police. IP addresses that may identify the locations of scammers in India need to be sent to Indian police as soon as they are located.
3. U.S. and Indian law enforcement can then coordinate on cases based on evidence developed in India.
4. U.S. prosecutors need to make full extradition requests for defendants when appropriate. The U.S. government needs to address barriers to extradition from India.

FVRO

APPENDIX: Cryptocurrency Investment Scams

According to FBI's 2023 IC3 report, the costliest online crime in America was cryptocurrency investment fraud (*ne* "pig butchering"), with $3.96 billion in reported loss. (Again, actual loss is estimated at 8-10 times reported loss.)

This fraud primarily originates from scam compounds in southeast Asia that utilize forced labor.

Until mid-2023, the initial social contact in a pig butchering scheme was usually made from a retail VoIP DID number provided by a large social media company. This company cracked down on bulk activation of accounts.
Pig butchering later migrated to prepaid U.S. SIM cards in SIM boxes.

APPENDIX: Cryptocurrency Investment Scams (Cont.)

In or about May 2023, initial pig butchering contacts began gravitating back to retail VoIP DID numbers. However, contacts using prepaid cell wireless numbers are still seen.

(Note the numbers displayed have most likely since been recycled to different users.)

FVRO