GLOBAL LEADERS' FORUM

GLF™

a techoraco brand

2025 GLF Fraud Report

Making fraud prevention a top priority as threats evolve

FTI CONSULTING™

This report has been commissioned by:

The Global Leaders' Forum (GLF) is a network of the leaders from the world's largest international carriers, who convene to discuss strategic issues and to agree collaborative activities with the aim of driving the next phase of growth for the industry.

This report has been supported by:

The GLF Community is a network of leaders representing the ecosystem of companies, partners, and industries that underpin global digital infrastructure.

The report has been compiled and written by:

FTI Consulting is a leading advisory and investment integrated platform globally. It is a hub for people, capital and knowledge to address challenges and opportunities in a transforming industries. We serve our TMT clients through our three business lines, Strategy, Business Transformation and Transaction Services.

For more information, please contact Silvia Peneva:

silvia.peneva@techoraco.com

For more information, please contact Anthony Pantaleo:

anthony.pantaleo@itwglf.com

TABLE OF CONTENTS


PART I
2025 GLF Fraud Report
GLOBAL LEADERS' FORUM
GLF
a techoraco brand

01

INTRODUCTION

GLOBAL LEADERS' FORUM GLF™ a techoraco brand

FOREWORD FROM

Eloy Rodriguez

At the heart of the Global Leaders' Forum is our unwavering commitment to eradicating fraudulent traffic from the wholesale telecoms industry. Since 2016, we have championed collaborative efforts to dismantle the pathways that enable fraudsters to exploit vulnerabilities, recognizing that a single weak link can sustain their illicit operations. As Chair of the GLF Trust Pillar, I am proud to introduce the 2025 GLF Fraud Report, a vital resource that charts our collective progress and illuminates the road ahead toward a resilient, fraud-free ecosystem.

Reflecting on the industry's landscape today, whilst strides have been made, the battle against fraudulent traffic demands unyielding vigilance. An increasing number of carriers are elevating fraud management to a strategic imperative, bolstering internal capabilities through advanced anti-fraud technologies, enhancing their dedicated expertise and making investments. Yet, across voice and messaging, the sophistication and scale of fraud use-cases persist: 29% and 35% of carriers report higher volumes of financial impact year-on-year of voice and messaging fraud, respectively. Carriers' investments undoubtedly enhance detection of once-elusive threats, but the true measure of success lies in proactive, consistent blocking to prevent monetization at its source.

Insights from this year's survey underscore the transformative power of collaboration, even as opportunities for deeper engagement emerge. Almost 50% of respondents indicate that a peer's adherence to the GLF Code of Conduct significantly influences their trading decisions, while over 70% advocate for an enhanced peer-review mechanism to foster greater transparency and accountability. At the GLF, we are actively pursuing initiatives to implement such a system, empowering carriers to build trust through verifiable compliance. I am particularly encouraged by the 20 carriers attested as compliant with the Code of Conduct this year, with all scoring the highest tier possible through the new peer review process we launched this year. These carriers exemplify the standards we all must pursue, and I hope they will inspire others to follow suit in the coming months.

I urge every international carrier executive to engage deeply with this report, using it as a catalyst for meaningful dialogue within your organizations. Achieving a fraudulent-traffic-free future requires relentless, unified action to seal every potential gap. In my role at the GLF, and within my own organization, I pledge to lead by example, driving innovation and partnership to safeguard our industry's integrity. Together, we can ensure that wholesale telecoms thrives on a foundation of trust and security.

- Eloy Rodriguez, Chief Wholesale Officer, Telefonica Global Solutions & Trust Pillar Lead, GLF

> ***Achieving a fraudulent-traffic-free future requires relentless, unified action to seal every potential gap.***

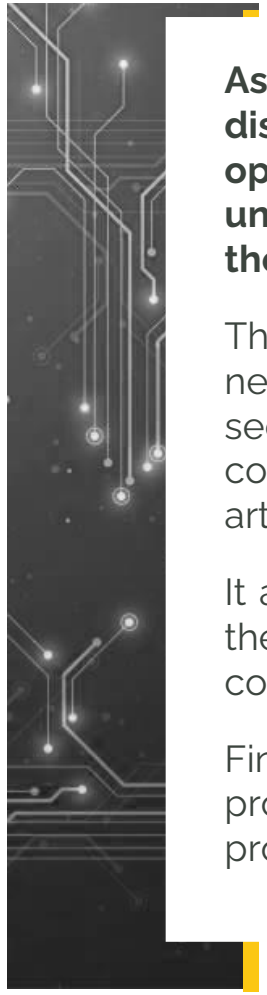
01 INTRODUCTION

Participating Organisations

MANY THANKS TO THE COMPANIES THAT CONTRIBUTED TO THE MAKING OF THIS REPORT

01 INTRODUCTION

Key Findings



As the telecom sector grows more complex, fraud tactics are advancing at an alarming pace. Fraudsters continuously discover new ways to exploit both technological innovations and existing weaknesses, placing heavy strain on operators. The consequences are extensive—ranging from financial losses to reputational damage—and they undermine customer trust in telecom providers. This report examines the escalation of fraud in telecoms, highlighting the strategies operators are using to safeguard their networks and restore confidence among customers.

This GLF fraud report is structured into six sections, each focusing on a distinct and timely issue. It opens by stressing the need to keep fraud prevention firmly on the corporate agenda, especially as schemes become harder to detect. The second section analyses international voice fraud, detailing how criminals exploit vulnerabilities in cross-border communications. The third section addresses international messaging fraud, covering methods such as smishing and artificially inflated traffic, both of which remain serious and growing risks.

It also reviews the broader issue of unwanted traffic, emphasizing its impact on infrastructure and users alike. In addition, the report underscores the rising importance of cooperation across carriers, regulators, and industry stakeholders to build collective resilience.

Finally, the report explores emerging challenges, with a special focus on the outlook for fraud detection and prevention. It provides guidance on how operators can adapt to these threats, using AI-driven tools to create more robust and future-proof fraud management frameworks.

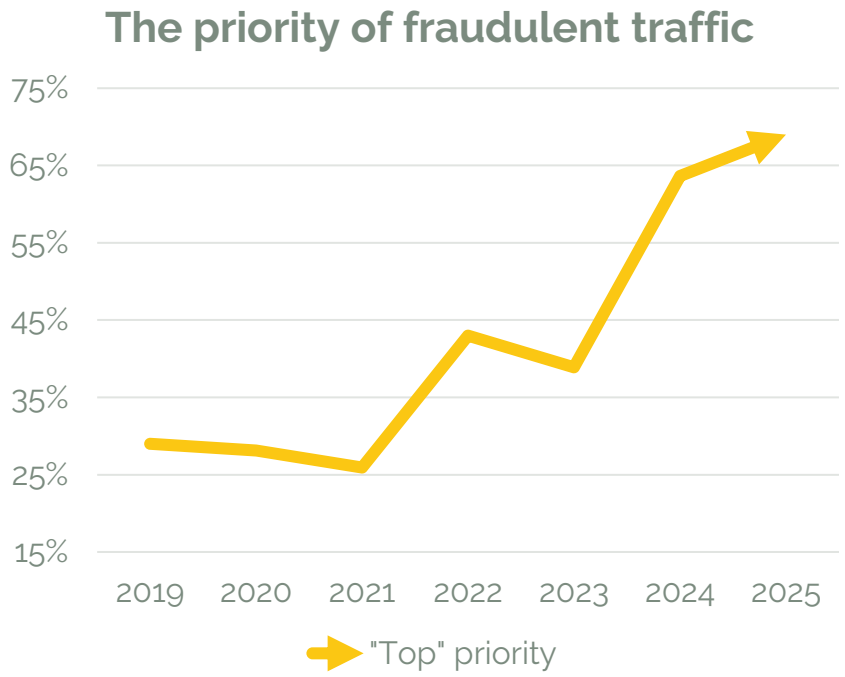
01 INTRODUCTION: KEY FINDINGS

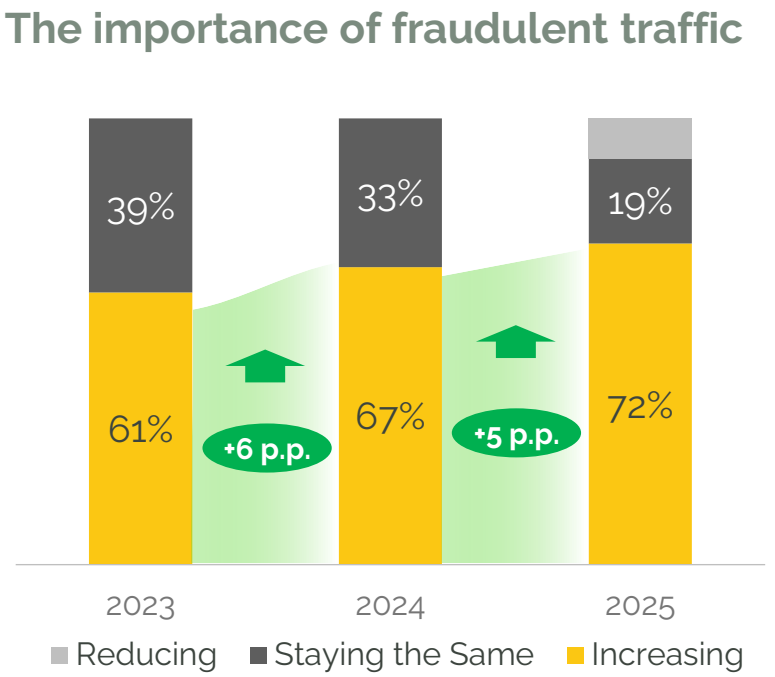
Making Fraud a Priority

FRAUDULENT TRAFFIC IS A HIGH PRIORITY FOR CARRIERS

01

69% of carriers state that fraudulent traffic is a 'top' priority — the highest since GLF started collecting this data





Note: BAU stands for Business as Usual

88%

of carriers say fraudulent traffic is 'top' or 'strategic' priority

48%

of carriers had a success rate for dispute resolution greater than 40%

77% Voice

77% SMS

of carriers foresee additional investments in anti-fraud systems in 2025

FTI DELTA

GLF

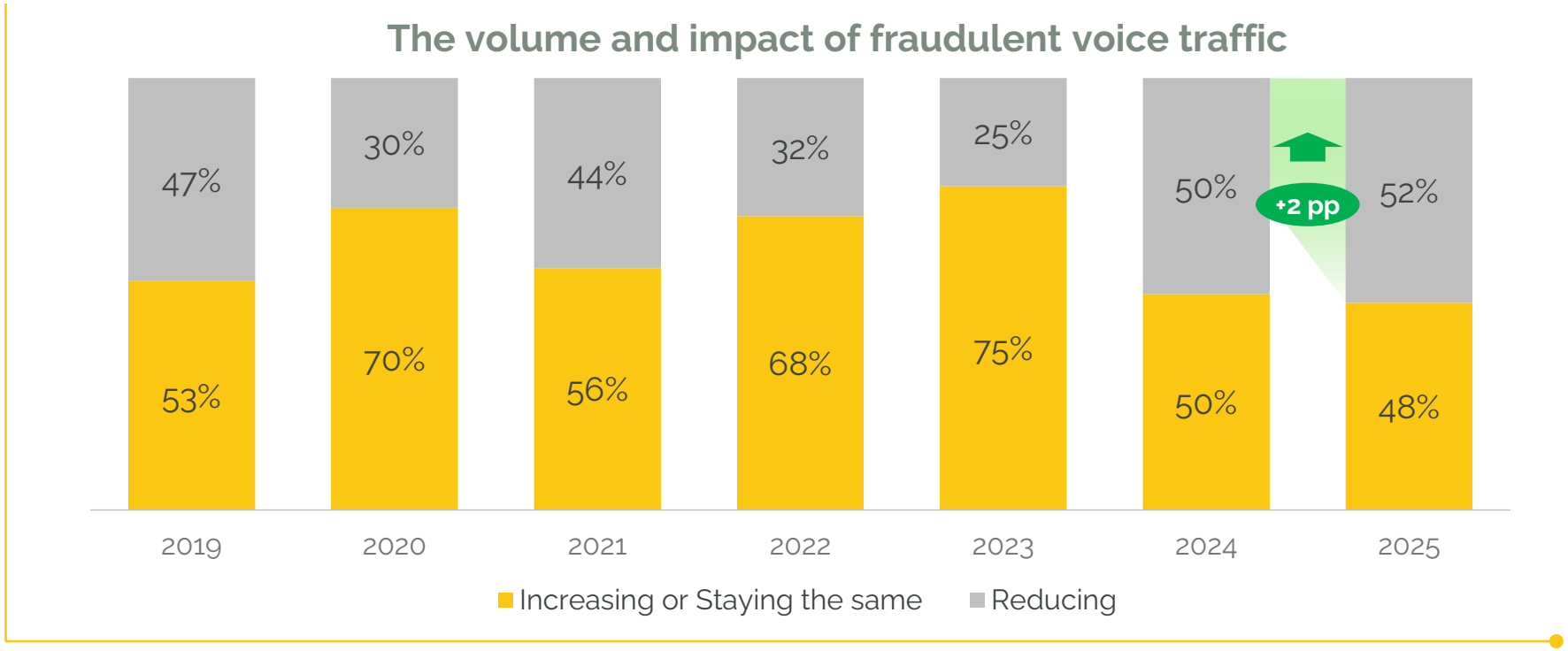
01 INTRODUCTION: KEY FINDINGS

International Voice Fraud

FRAUDULENT VOICE TRAFFIC SHOWS BALANCED TRENDS IN VOLUME AND IMPACT

02

52% of operators report that the volume and impact of fraudulent voice traffic has been reduced in the last 12 months, against 50% in the last year



Note: IRSF stands for 'international revenue share fraud'; OBR stands for 'origin-based rating'.

CLI Spoofing, IRSF and OBR Fraud are cited as the fraud types with the highest volume and financial impact

69%

of carriers say they have experienced a 'high' volume of **CLI Spoofing**

67%

of carriers say they have experienced a 'high' volume of **IRSF**

45%

of carriers say they have experienced a 'high' volume of **Wangiri Fraud**

01 INTRODUCTION: KEY FINDINGS

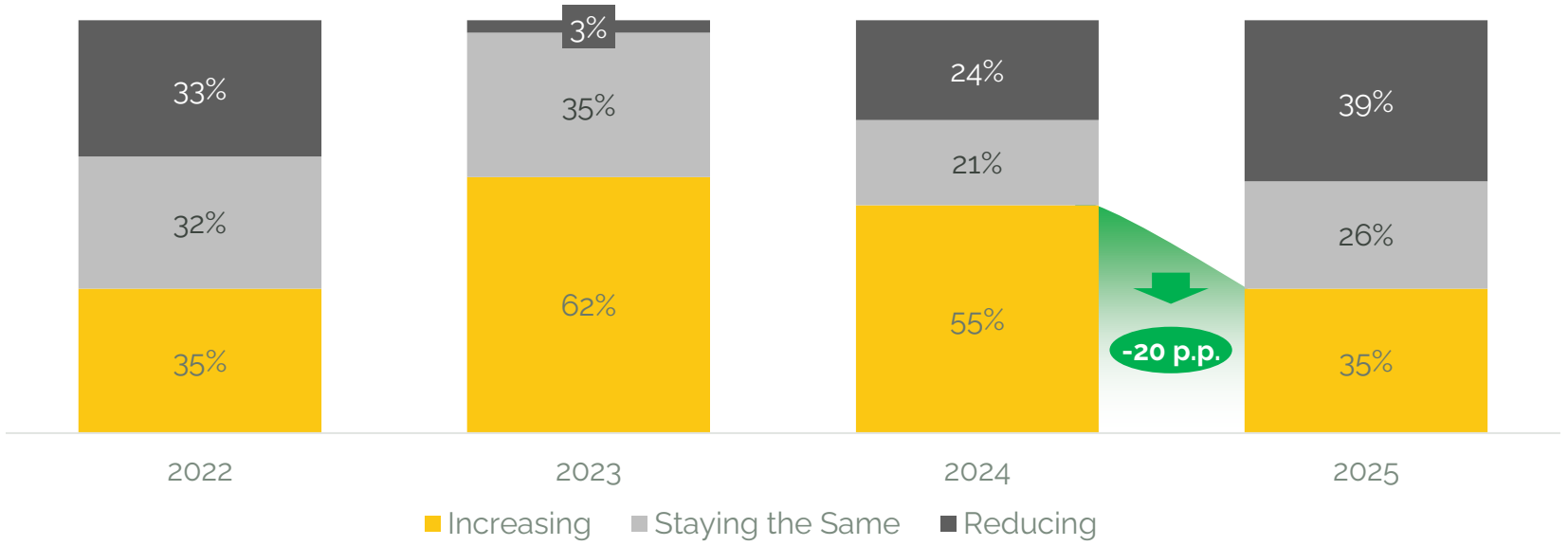
International Messaging Fraud

FRAUDULENT MESSAGING TRAFFIC STAYS HIGH WITH EARLY SIGNS OF REDUCTION

03

35% of operators reported an increase in fraud in the last 12 months, reflecting a 20 p.p. decrease compared to 2024

The volume and impact of fraudulent messaging traffic



Note: AIT stands for 'artificially inflated traffic'.

AIT, Smishing and SMS Originator Spoofing are the biggest threats in terms of volume and financial impact

61%

of carriers say they have experienced a 'high' volume of **SMS phishing (Smishing)**

54%

of carriers say they have experienced a 'high' volume of **Artificially Inflated Traffic (AIT)**

33%

of carriers say they have experienced a 'high' volume of **SMS Originator Spoofing**

FTIDELTA GLF

01 INTRODUCTION: KEY FINDINGS

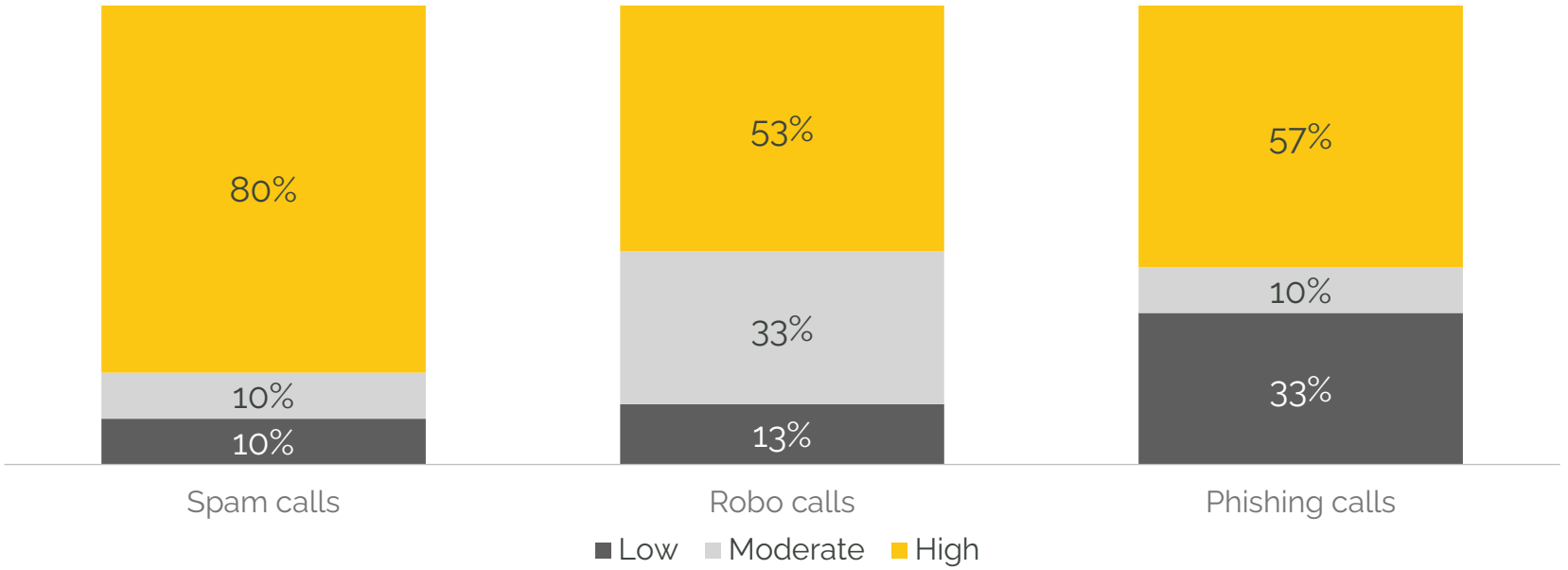
Unwanted Traffic

SPAM CALLS LEAD UNWANTED TRAFFIC, OUTPACING ROBO AND PHISHING CALLS

04

More than 53% of carriers report getting high volumes of nuisance calls, i.e., spam calls, robo calls and phishing calls

The volume of unwanted traffic experienced by carriers



83%

of carriers say unwanted traffic **reduces trust** in telecom carriers

63%

of carriers say unwanted traffic encourages **additional regulatory scrutiny**

67%

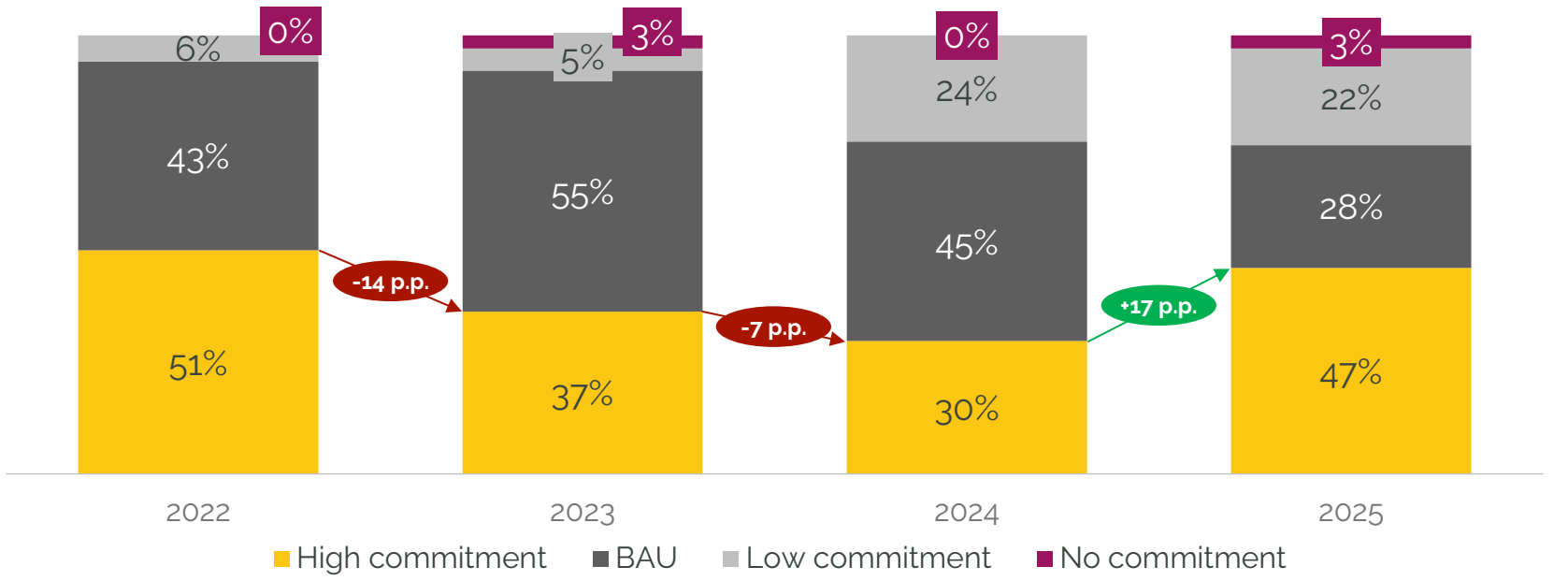
of carriers say unwanted traffic encourages **additional regulatory action**

COMMITMENT TO COLLABORATION IS NEEDED TO REDUCE FRAUD

05

47% of respondents believe their peers have a high commitment to collaboration, in comparison to 30% in 2024

Perceived level of peer commitment to fighting fraud



48%

of carriers say that compliance with the GLF CoC will impact the likelihood of trading with that carrier

74%

of carriers say the industry should provide a rating of compliance based on peer review

Note: CoC stands for 'code of conduct'.

01 THE GLF CODE OF CONDUCT

Compliant Carriers

CODE OF CONDUCT ATTESTATION HAS BEEN CARRIED OUT FOR THE FIFTH YEAR

07

21 carriers were attested as compliant with the GLF Code of Conduct in 2025

‘Excellent’

A1 Telekom Austria Group

airtel

bayobab

bics

BTS

CIMA GROUP

colt

T

e&

iBASIS

IDT global

LANCK TELECOM

orange

PCCW Global

SPARKLE

TATA COMMUNICATIONS

Telefónica Global Solutions

Telin

vodafone

‘Advanced’

stc

21

Carriers passed the attestation process in 2025

48%

of carriers say that a peer’s compliance with the GLF Code of Conduct impacts their likelihood of trading with them, demonstrating the relevance of the Code of Conduct as an emerging trust mark for the carrier industry

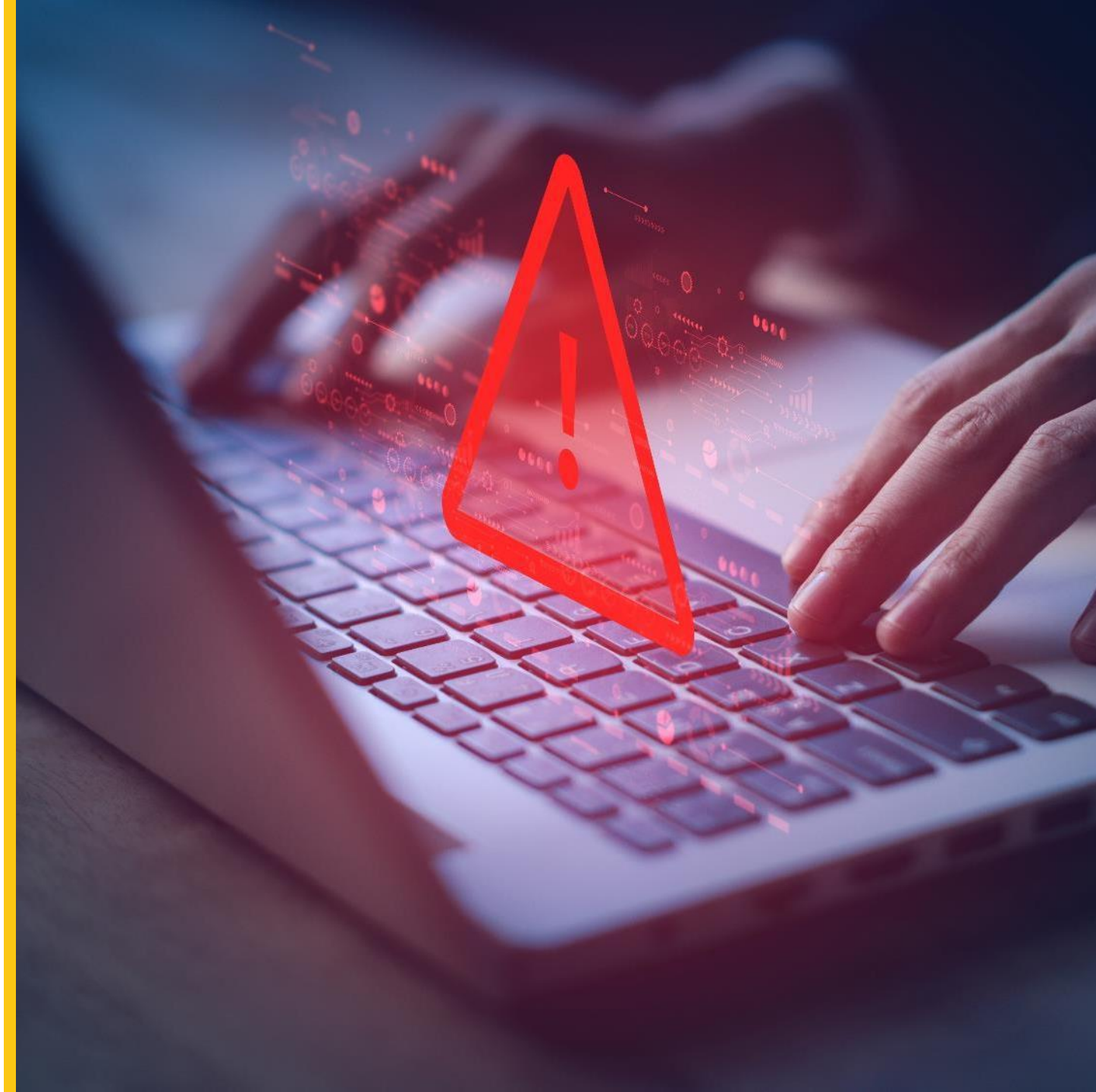
FTIDELTA

GLF

02

MAKING FRAUD A PRIORITY

GLOBAL LEADERS' FORUM GLF™ a techoraco brand



02 MAKING FRAUD A PRIORITY

Introduction

This section explores how carriers are prioritising fraud prevention and examines the strategic decisions, investments and resources being allocated to combat the ever-evolving threats. By focusing on proactive measures and ensuring that blocking fraudulent traffic is treated as a priority by senior management, carriers can stay ahead of fraudsters and safeguard both their operations and customer trust.

01

Stopping fraudulent traffic is a priority: Fraud management has become a top priority for telecom operators, with 69% of carriers in 2025 ranking it as critical, the highest ever recorded, up from 64% in 2024. This shift is driven by shrinking margins in voice traffic, where even small incidents can cause significant financial losses. Over the past year, 70% of carriers have also reported increasing importance of fraudulent traffic, management as fraudsters increasingly use AI and machine learning to bypass traditional detection systems—pushing operators to accelerate investment in advanced AI-driven solutions.

02

On-going investments in anti-fraud systems: Carriers are maintaining a strong focus on fraud prevention, with 77% of them foreseeing increasing investment over the next year in both voice and SMS fraud detection. This is the joint highest level of investment outlook recorded in these categories and signifies the strong commitment of carriers towards fighting fraud recognising that systems are at the heart of the fight against fraud.

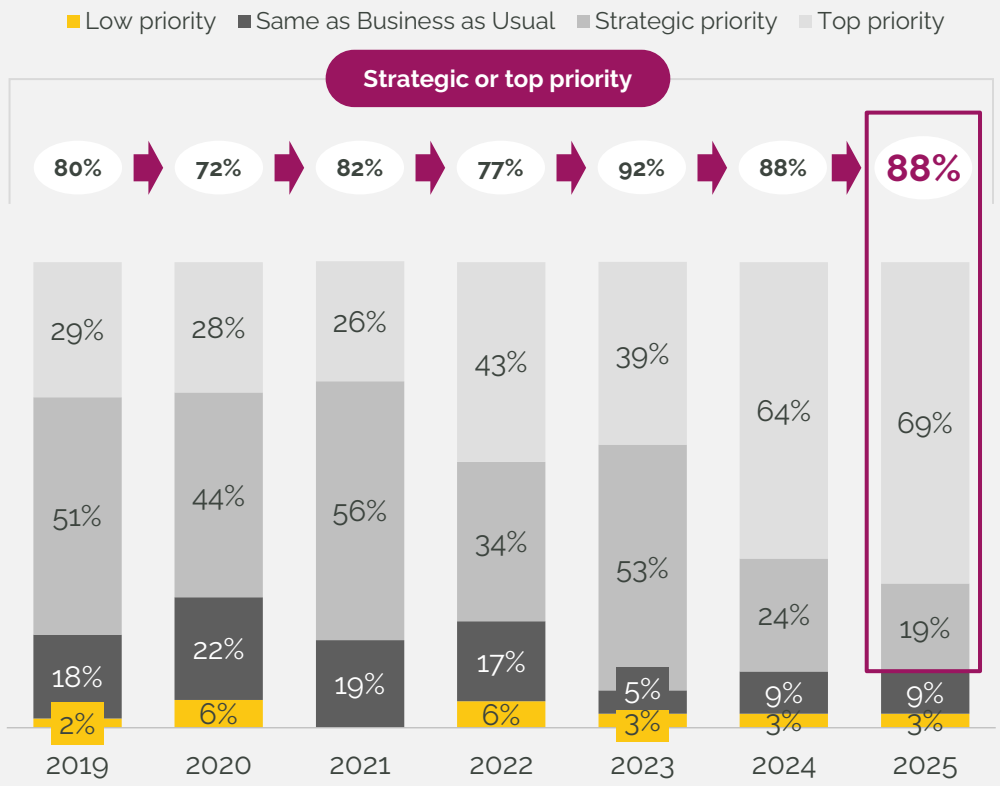
03

The need for collaboration, accountability & regulatory support: To counter emerging threats, carriers are prioritizing a more collaborative environment that promotes cross-border intelligence sharing, regulatory alignment across regions, and stronger accountability measures. A key focus is holding non-compliant telcos responsible for their practices while working with regulators to establish consistent, enforceable standards that protect the integrity of global networks

02 MAKING FRAUD A PRIORITY

The importance of fraudulent traffic in the organisation

Fig. 1. Ranking of fraud as a topic in the organisation
(% responses)



In 2025, **69% of carriers identified fraudulent traffic as a top priority, the highest level since GLF started its fraud report,** continuing the upward trend from 64% in 2024 and 39% in 2023, underscoring the industry's growing commitment to combating fraud but also the fact that despite historic focus, fraudulent traffic sustains across network.

Three key reasons cited by carriers for treating anti-fraud as a priority include:

1. **Financial sustainability**: With global fraud losses surpassing $1 trillion[1], unchecked fraud directly threatens revenue and operational resilience.
2. **Customer trust**: Fraud erodes user confidence and brand reputation, making fraud prevention a customer experience issue as much as a security one.
3. **Regulatory and market pressure**: Tighter rules, coupled with peer and partner expectations, raises awareness and compels carriers to act decisively.

> *Fraud has evolved into a strategic issue because it directly affects financial sustainability and erodes customer and peer trust. In a trust-based ecosystem, fraud undermines brand integrity and competitive positioning, demanding executive-level focus*

88% of carriers say managing fraudulent traffic is a '**top**' or '**strategic**' **priority**

Notes: n (2019) = 45, n (2020) = 32, n (2021) = 27, n (2022) = 35, n (2023) = 36, n (2024) = 33, n(2025)=32. To the carriers, 'top' priority means implementing urgent measures to combat fraud; meanwhile, a 'strategic' priority means embedding this topic into long-term planning.
Source: (1) Global Anti-Scam Alliance, GLF Survey 2025.

02 MAKING FRAUD A PRIORITY

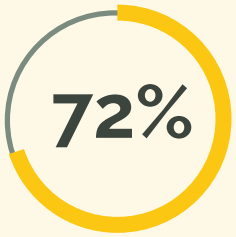
The importance of fraudulent traffic management in the organisation

The importance of managing fraudulent traffic within organisations continues to increase. **In 2025, 72% of carriers reported an increased focus on fraud management, continuing the upward trend from 67% in 2024 and 61% in 2023.**

Importantly, **44% of telcos now expect a significant increase in importance of fraud prevention**, reflecting the scale of the challenge and the need for stronger, more proactive measures.

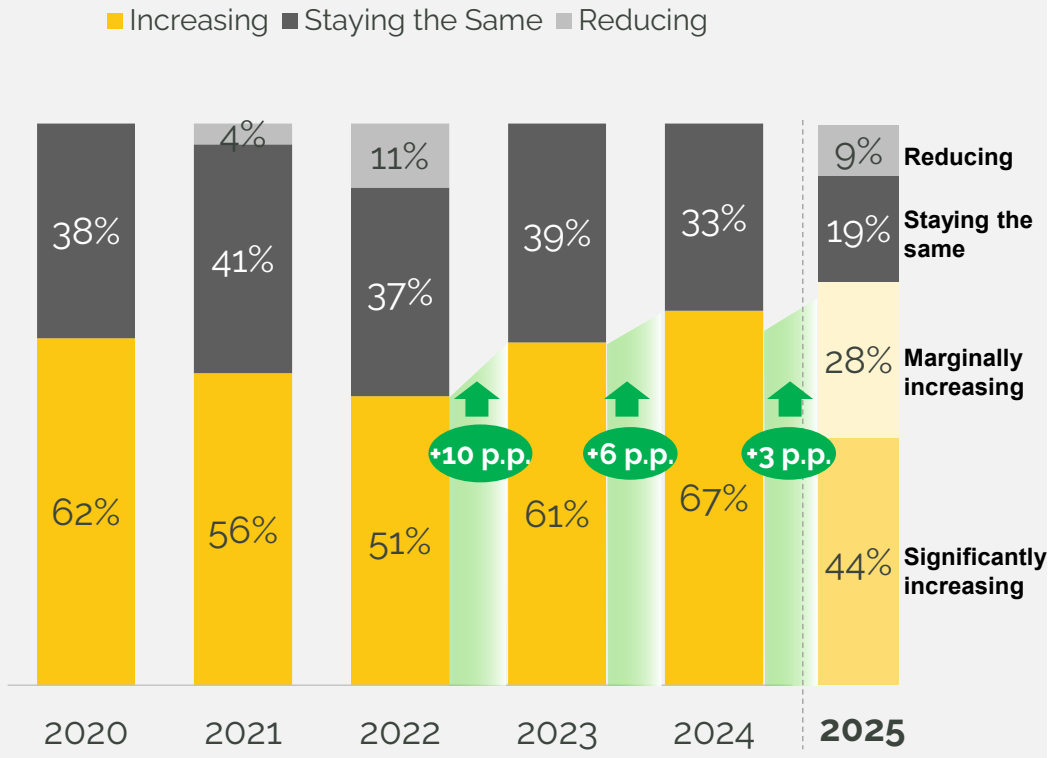
Certain types of fraud, such as International Revenue Share Fraud (IRSF), CLI Spoofing, and OBR Fraud in voice, as well as Smishing, Artificially Inflated Traffic (AIT), and SMS Originator Spoofing in messaging, persist because fraudsters continually evolve their tactics to exploit gaps in detection and blocking mechanisms at a speed that exceeds carriers' responses. As such, organizations must continue to treat fraud management as a priority to combat these persistent yet evolving threats.

> *We are improving the systems, but fraud adapts so quickly that even small issues are more significant every day. This is why carriers must treat fraud as a strategic priority, not just a technical one*



of carriers say the importance of fraudulent traffic management has **increased** in 2024

Fig.2. Change in the importance of fraudulent traffic management in the organisation
(% responses)



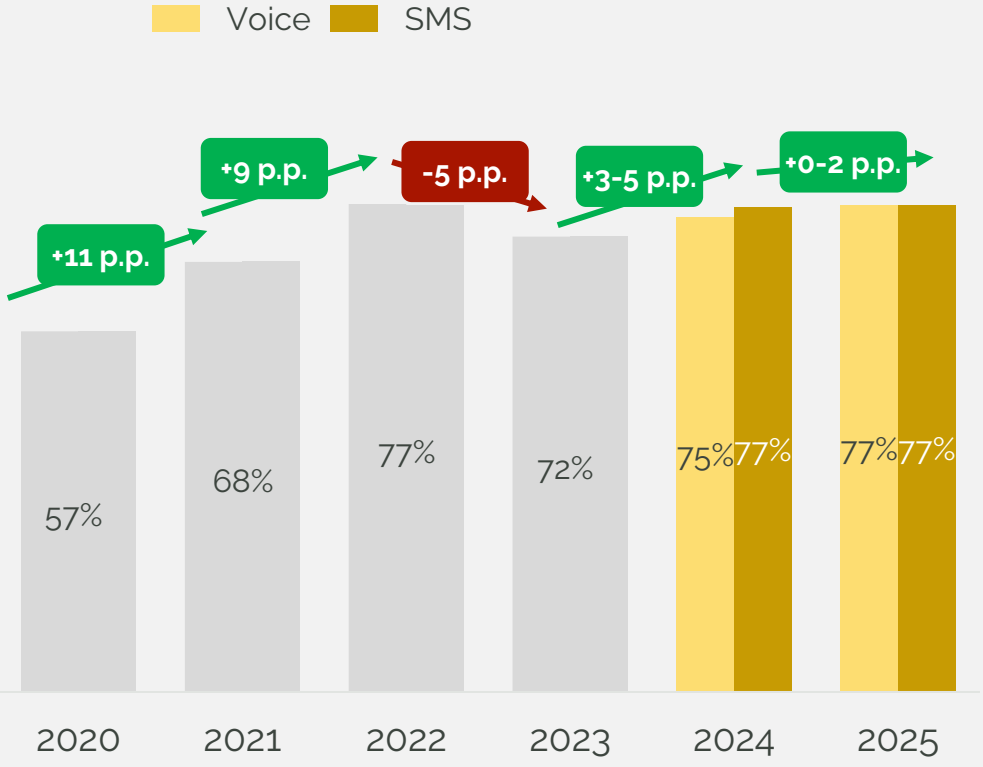
Notes: n (2020) = 20, n (2021) = 27, n (2022) = 35, n (2023) = 36, n (2024) = 33, n(2025) = 32.
Source: GLF Survey 2025.

02 MAKING FRAUD A PRIORITY

Anticipated investments in fraud prevention tools and monitoring infrastructure

Fig. 3. Share of carriers who foresee investing more in fraud monitoring / prevention infrastructure

(% responses)



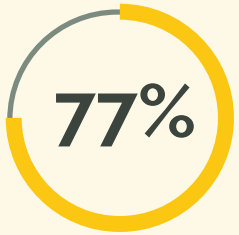
Notes: n (2020) = 20, n (2021) = 27, n (2022) = 35, n (2023) = 36, n (2024) = 33, n(2025) = 30.
Source: GLF Survey 2025.

Carriers are doubling down on fraud prevention, with 77% expecting increased investment in both voice and SMS fraud prevention respectively in 2025.

Additionally, among organisations that have made fraud management a top or strategic priority, 80% expect increased investment in voice, demonstrating a clear correlation between prioritisation and willingness to invest.

Organisations are expected to target investments towards AI-driven detection systems, with a significant number of carriers already adopting them for enhanced fraud prevention. Other key areas include joining Fraud Prevention Registries (FPR) for real-time data sharing, bolstering identity verification, and increasing multi-factor authentication (MFA) adoption. Compliance with frameworks like the GLF Code of Conduct, which emphasises monitoring, reporting, and contractual blocks on fraudulent traffic, will also see focus with investments being made to support adherence..

> *There is limited impact through investment in human resources, so we must invest in systems with AI and self-learning. Our goal is to block fraud before it starts—people can't act as fast as the systems.*



of carriers on average foresee **additional investments in antifraud systems for voice/SMS** for 2025

02 MAKING FRAUD A PRIORITY

Initiatives in line with fraud being a top priority

CARRIERS THAT PRIORITISE FRAUD PREVENTION ARE DEMONSTRATING THEIR COMMITMENT THROUGH A VARIETY OF INITIATIVES, SUCH AS:

AI and ML deployment to detect and block fraudulent activity in real time, reducing human intervention and improving efficiency

We use AI and machine learning for real-time fraud detection, leveraging big data, anomaly detection, and near real-time blocking through signalling protocols

Our fraud management system is powered by advanced AI, including machine learning models, anomaly detection, and time-series analysis

Expansion of partnerships across the industry and with regulatory bodies to share fraud intelligence and improve global fraud detection efforts

We maintain transparent and direct communication with our partners, encourage sender ID registration and scrubbing, and share feedback when suspicious traffic is detected. Our close collaboration ensures proactive handling even before issues arise

We coordinate with others primarily through active participation in industry forums & working groups, including the i3Forum, the GSC Fraud Working Group and the One Consortium. We attend conferences, share expertise & present best practices to be adopted collectively

Shifts from reactive fraud responses to proactive via AI, predictive analytics and integrating real-time detection directly into the Traffic Management Systems

We proactively block number ranges and destinations, monitor traffic at very low and granular thresholds for fraud detection, and adopt best practices from industry collaboration

We have launched anti-spam measures, and proactive monitoring by MNOs across the industry has helped drive down fraud levels

Source: GLF Survey 2025.

02 MAKING FRAUD A PRIORITY

Conclusion

01

Each year, telecommunications carriers are increasingly prioritizing fraud prevention. This trend is fuelled by shrinking voice revenue margins, the adoption of AI by fraudsters, and escalating international regulations, all of which are compelling carriers to invest in more flexible fraud detection systems to safeguard their earnings and preserve compliance credibility.

02

International carriers are progressively adopting AI-powered detection tools and live monitoring platforms to counter advancing fraud strategies recognising that systems will be much more effective than human intervention. Using AI, the sector is transitioning from a reactive to proactive approach, allowing for improved detection of anomalous traffic behaviours and averting financial damages at the earliest opportunity.

03

Combating fraud necessitates greater industry-wide collaboration and data-sharing programs. Carriers, regulators, and other stakeholders must collaborate to establish uniform prevention measures. Absent cohesive initiatives, the sector continues to be susceptible to progressively complex fraudulent operations, emphasizing the critical need for joint endeavours.

Source: GLF Survey 2024.

03

INTERNATIONAL VOICE FRAUD

GLOBAL LEADERS' FORUM GLF™ a techoraco brand

03 INTERNATIONAL VOICE FRAUD

Definitions

01 International Revenue Share Fraud (IRSF)
A motivation for committing fraud that has the end goal of generating traffic to high-rate destinations or premium-rate end numbers. This encompasses many techniques to generate fraudulent traffic and is the most prevalent in the industry.

02 Missed Call Campaigns / Wangiri Fraud
Missed call fraud campaigns and/or Wangiri fraud (Japanese term, as the fraud first occurred in Japan) is a telecom fraud scheme based on CLI spoofing, spamming, deception and IRSF, and in most instances targets unsuspecting mobile end-users in a country and/or subscribers ('Target Subscribers') of a specific mobile operator ('Target Mobile Operator').

03 Call hijacking
Rerouting of legitimate traffic to a non-legitimate, usually high-rate destination to obtain additional monetary benefit from the original traffic.

04 Hacking of a customer telephone system
Control of a customer phone system is obtained by a bad actor, and the system is utilised to generate traffic to high-rate destinations. Usually the traffic origination is software-generated, and a lot of fraudulent volume can be generated in a very short time.

05 False Answer Supervision
When a bad actor returns a fraudulent answer signal to routing carriers, thereby triggering the billing process of an otherwise uncompleted call.

06 OBR Fraud / CLI Spoofing
Altering the Caller ID information to deceive the recipient into answering the call, typically by making it appear as a different subscriber's number, facilitating impersonation fraud, inter-carrier wholesale fraud, and spamming.

07 Bypass
Routing traffic through unauthorised or illegal channels, often using SIM boxes, to avoid paying legitimate termination fees. This leads to revenue loss and degraded service quality for telecom operators.

08 Calls to manipulated B-numbers
A type of fraud where the terminating number is altered so that the call is routed to destinations with artificially high or misrepresented termination rates. By changing or generating false B-numbers, fraudsters exploit the way operators handle routing and billing, causing calls to be directed to premium-rate or otherwise inflated destinations, allowing the fraudsters to capture illicit revenue

Source: i3 Forum, Fraud classification and recommendations on dispute handling: Release 4.0, March 2023; GLF; FTI Delta analysis.

03 INTERNATIONAL VOICE FRAUD

Introduction

While international voice fraud continues to evolve with new threats, operators are steadily gaining ground. In 2025, only 48% of carriers reported stable or rising fraud levels, a decline of 27 p.p. over the past two years, providing clear evidence that coordinated anti-fraud measures are delivering real results. In the following section, we look at how operators are shifting the balance in their favour, while adapting to the latest threats.

01

Decline volume and impact of international voice fraud: 52% of operators are reporting a reduction in volume and impact, up from 50% last year and hitting the lowest levels recorded by GLF. This reduction is fuelled by the deployment of advanced AI-driven fraud management tools, stronger industry-wide collaboration, and the adoption of best practices such as proactively blocking risky number ranges, applying granular traffic thresholds, and tightly managing high-risk destinations.

02

Among the rising fraud types, three have demonstrated a significant increase in volume: International Revenue Share Fraud, CLI spoofing, and Missed Call Campaigns/ Wangiri fraud

a. **International Revenue Share Fraud (IRSF)** has risen to be the top fraud concern, as fraudsters continue to exploit roaming-originated traffic leading to 67% respondents reporting high volume. This year, the data shows a broader geographic spread, with high incidences now reported across both emerging and developed markets.

b. **CLI spoofing** also remains a major concern, with 59% of operators reporting high volumes of fraud in the last 12 months vs. 55% in 2025. Additionally, the percentage of carriers reporting a high financial impact (52%) has gone up drastically by 16 p.p. from 2024. Fraudsters leverage this technique to carry out more sophisticated attacks, including vishing and scam calls, making CLI spoofing a serious and persistent issue.

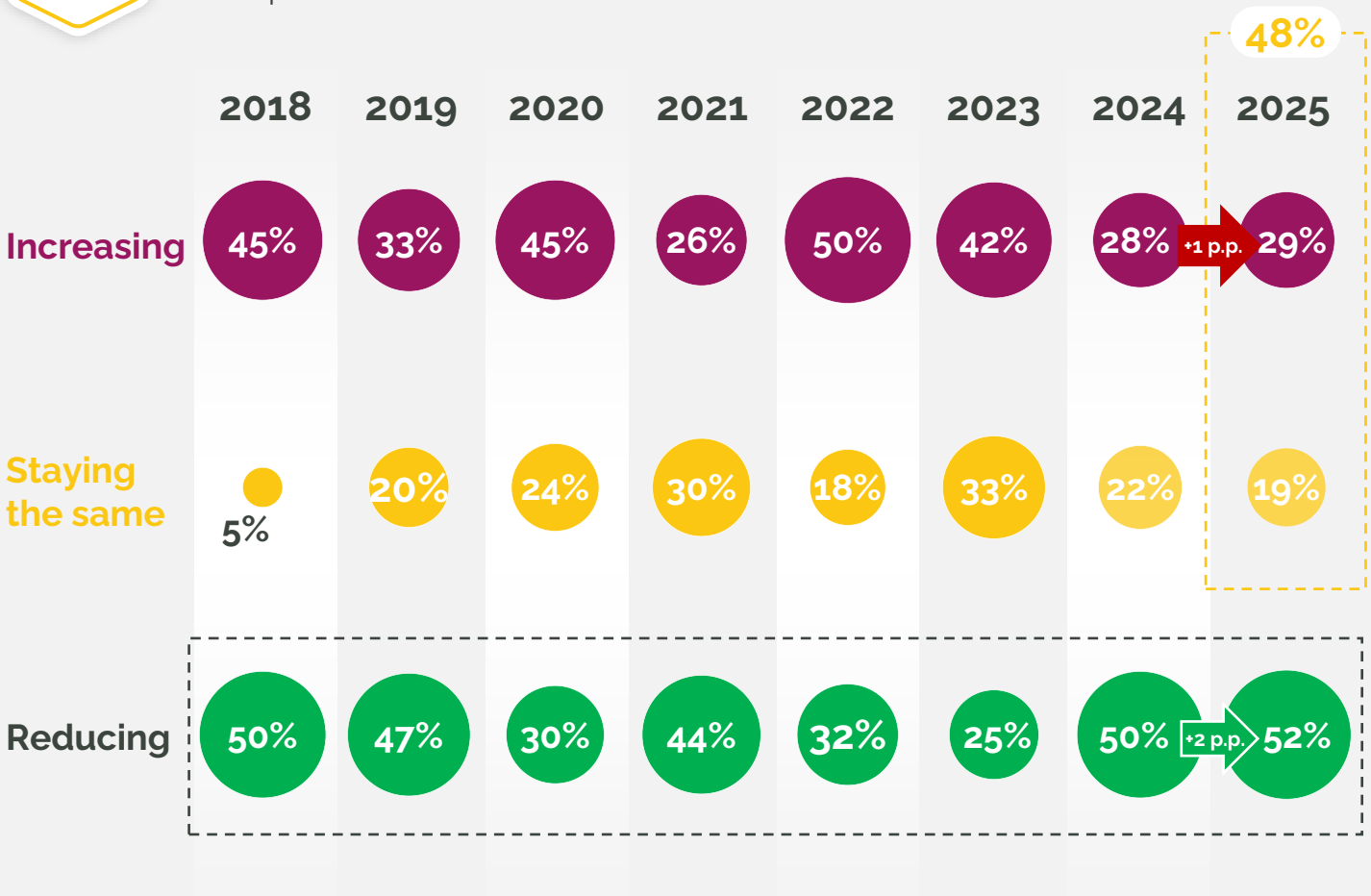
c. **Missed Call Campaigns/Wangiri Fraud** has also seen a considerable uptick as 45% of respondents now face a high volume of this type of fraud. This is particularly damaging, as they remain harder to detect in real time and can generate revenue through high termination charges or call-backs from unsuspecting users.

03 INTERNATIONAL VOICE FRAUD

The volume and impact of fraudulent voice traffic

Fig. 4. Year-on-year comparison of the volume and impact of fraudulent voice traffic

(% responses)



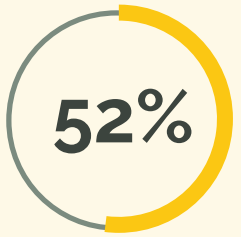
Notes: n (2019) = 34, n (2020) = 20, n (2021) = 27, n (2022) = 35, n (2023) = 36, n (2024) = 33, n(2025) = 32
Source: Global Anti-Scam Alliance, GLF Survey 2025.

52% of operators claim that the volume and impact of fraudulent traffic has reduced, the highest year-on-year level ever recorded. Within this 52%, **19% of operators have claimed "significant reduction" in volume and impact** suggesting that industry wide investments in fraud detection are starting to pay sustained dividends.

Though reducing in volume, fraud persists as it remains profitable and adaptable. Overall **losses from international scams and frauds exceeded $1 trillion** in 2024, fraudsters developing ever more complex fraud attacks.

Weak links in routing, uneven regulation, and non-universal adherence to stopping payment flows let schemes like IRSF and CLI Spoofing sustain, while carriers face trade-offs between strict blocking and service continuity. This imbalance ensures fraud remains persistent and strategically damaging.

> *We will never get to a zero-fraud environment. You can diminish the volume but there will always be something new coming.*



of operators report that the **volume and impact of fraudulent traffic is reducing**

03 INTERNATIONAL VOICE FRAUD

Extracts from the conversations with the carriers on fraudulent voice traffic

xx% % of responses

What is driving the change in the volume and impact of fraudulent voice traffic hitting your organisation in the past 12 months?

Reduction 52%

We proactively block number ranges and destinations, monitor traffic at very low and granular thresholds for fraud detection, and adopt best practices from industry collaboration

Our decision to stop supporting VAS breakouts in the Pacific region, along with improved systems, processes & alerting, has improved our fraud prevention efforts

No change 19%

Our use of excellent anti-fraud and prevention systems and adoption of industry best practices, have resulted in fewer cases of fraud.

We believe fraud is increasing, but better fraud management is reducing the fraudulent traffic reaching our network

Increase 29%

Most of the cases we see are IRSF and traffic inflation on hidden ranges (officially legitimate mobile range)

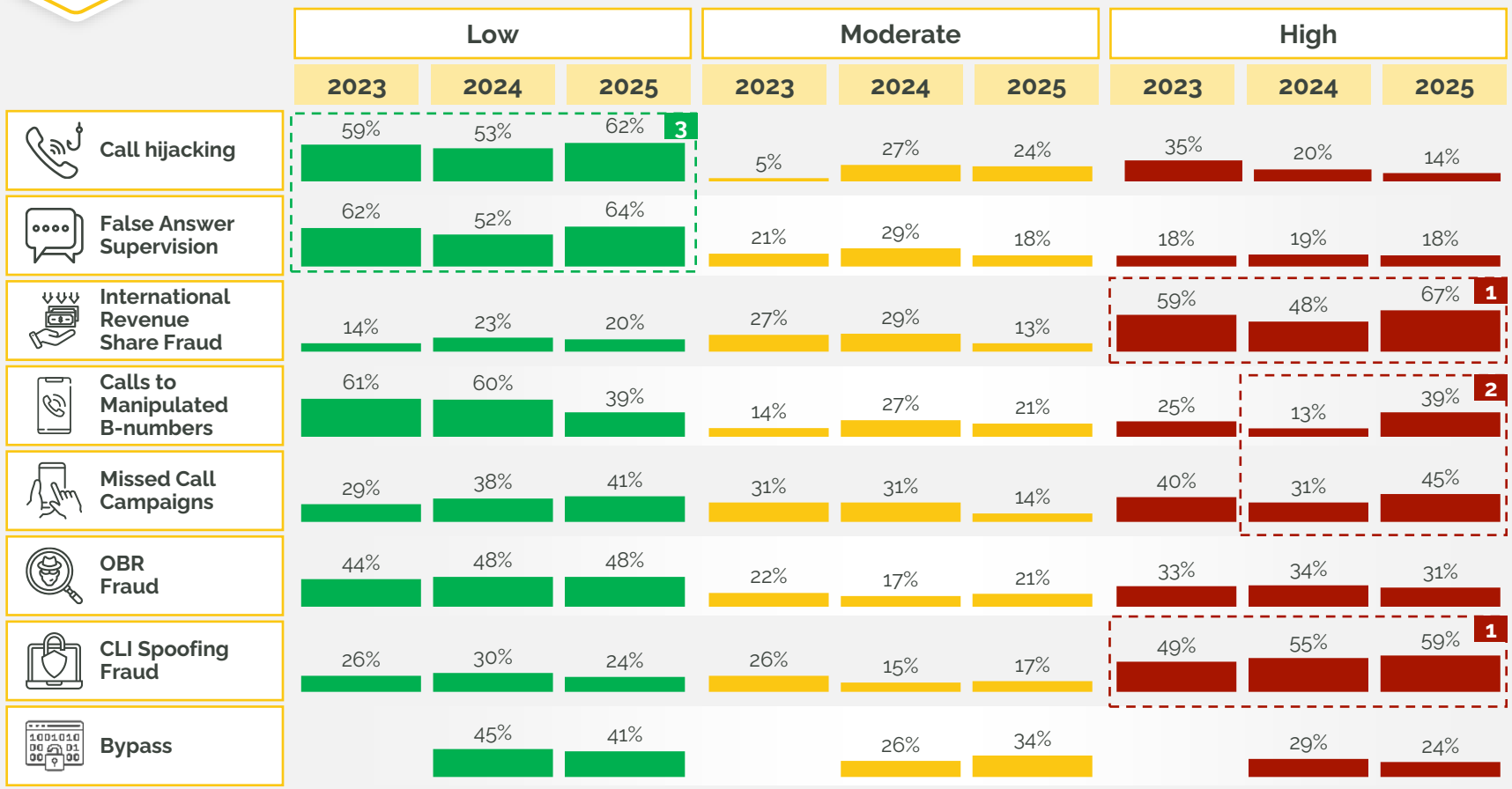
More PBX compromises are observed as the hosted PBX business grows.

Source: GLF Survey 2025.

03 INTERNATIONAL VOICE FRAUD

Volume of fraudulent voice traffic, by use case

Fig.5. Year-on-year comparison of the volume of fraudulent voice traffic
(% responses)



Notes: n (2023) = 36, n (2024) = 33, n (2025) = 28. 1. Vishing (short for "voice phishing") is a type of phishing attack where fraudsters use phone calls to deceive individuals into revealing personal, financial, or security-related information.
Source: GLF Survey 2025.

Consistently in the last three years, a large share of operators' report 'high' volumes of IRSF and CLI spoofing.

1 Despite prevention efforts, IRSF continues to exploit roaming-originated traffic leading to a 19-p.p. increase in respondents reporting high volume. CLI spoofing continues to be a top concern.

2 There has been a considerable increase in Calls to manipulated B-numbers and Missed Call campaigns as they remain harder to detect in real time and can generate revenue through high termination charges or call-backs from unsuspecting users.

3 Over 60% report low volumes of call hijacking and FAS. Main reasons include better detection systems and proactive blocking measures.

> *Fraudsters are getting more sophisticated with missed call campaigns, using AI to scale attacks that are harder to spot*

03 INTERNATIONAL VOICE FRAUD

Financial impact from fraudulent voice traffic, by use case

Fig. 6. Level of financial impact experienced by the carriers, by fraud use case
(% responses)

Notes: n (2023) = 36, n (2024) = 33, n (2025) = 28
Source: GLF Survey 2025.

IRSF, OBR Fraud and CLI Spoofing continue to have a high financial impact, as fraudsters are following the money by targeting 'high-cost destination' numbers.

1 Almost 60% of responders report high financial impact from IRSF, a y-o-y increase of 9-p.p. from 2024 suggesting that IRSF remains highly damaging due to detection and blocking challenges.

2 Despite having comparatively low financial impact, there has been a concerning increase in the number of responders reporting a high impact of Missed Call Campaigns / Wangiri.

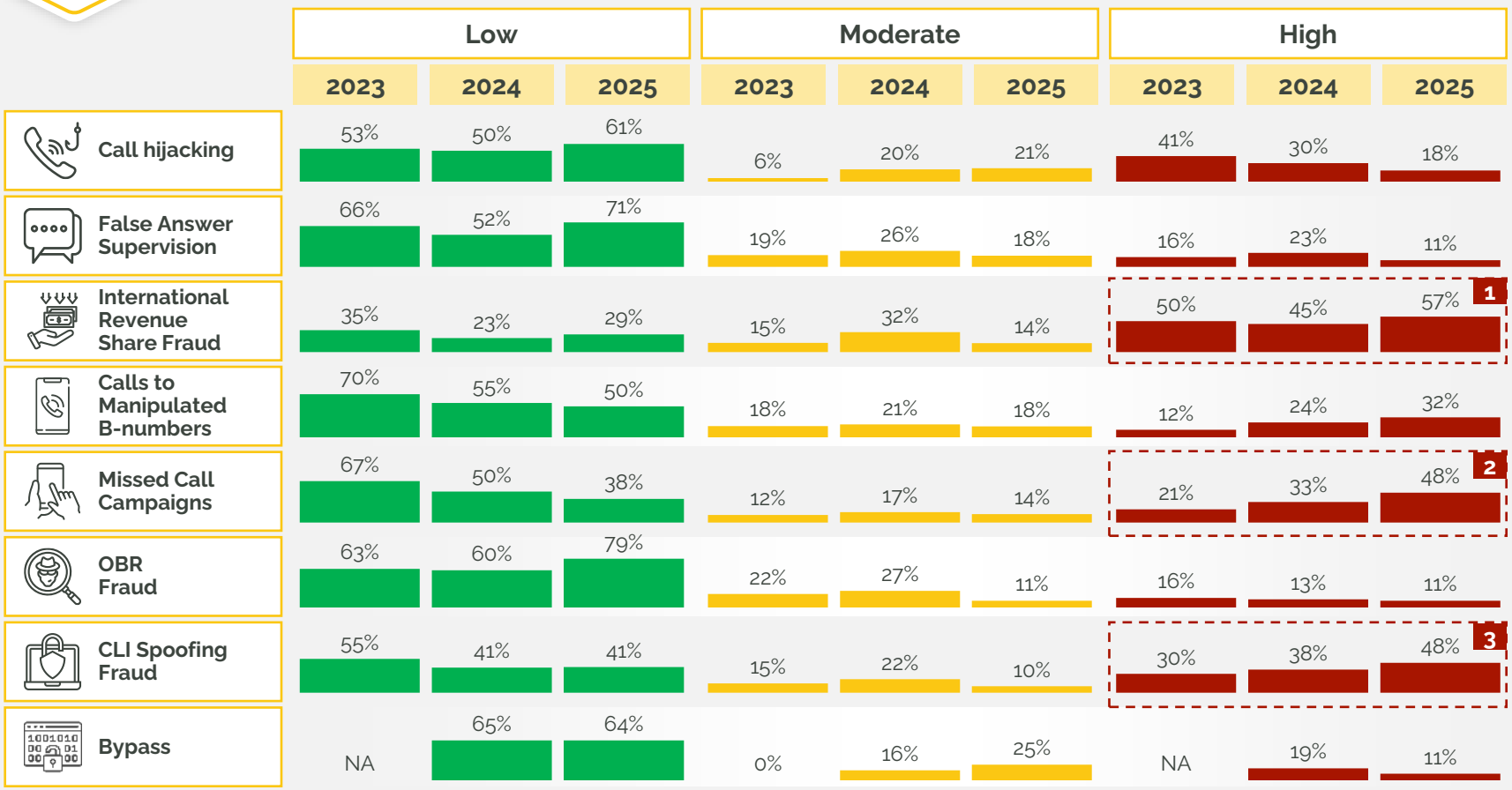
3 Responders reporting high financial impact of CLI spoofing has increased from 36% to 52% — a major issue as fraudsters leverage this technique to carry out more sophisticated attacks, including vishing and scam calls

> *Falling margins make every fraud incident hit harder, and adaptive tactics like CLI spoofing and deepfakes are driving up losses*

03 INTERNATIONAL VOICE FRAUD

Financial impact from fraudulent voice traffic, by use case

Fig. 7. Level of financial impact experienced by the end-user, by fraud use case
(% responses)



Notes: n (2023) = 36, n (2024) = 33, n (2025) = 28.
Source: GLF Survey 2025.

Frauds like IRSF, CLI spoofing, and Wangiri are causing mounting consumer harm. Carriers report there being stronger industry focus when end-users are impacted, and as such it is critical the industry works together to removed these fraud types

1 IRSF's financial impact is reported as high by 57% of carriers, making it the most damaging fraud type for end-users.

2 Missed Call Campaigns / Wangiri has continued on its trajectory, with 48% of telcos reporting high impact, showing a persistent challenge despite wider industry awareness.

3 The financial impact of CLI spoofing has surged, reflecting fraudsters' ability to impersonate trusted identities and exploit customer vulnerability.

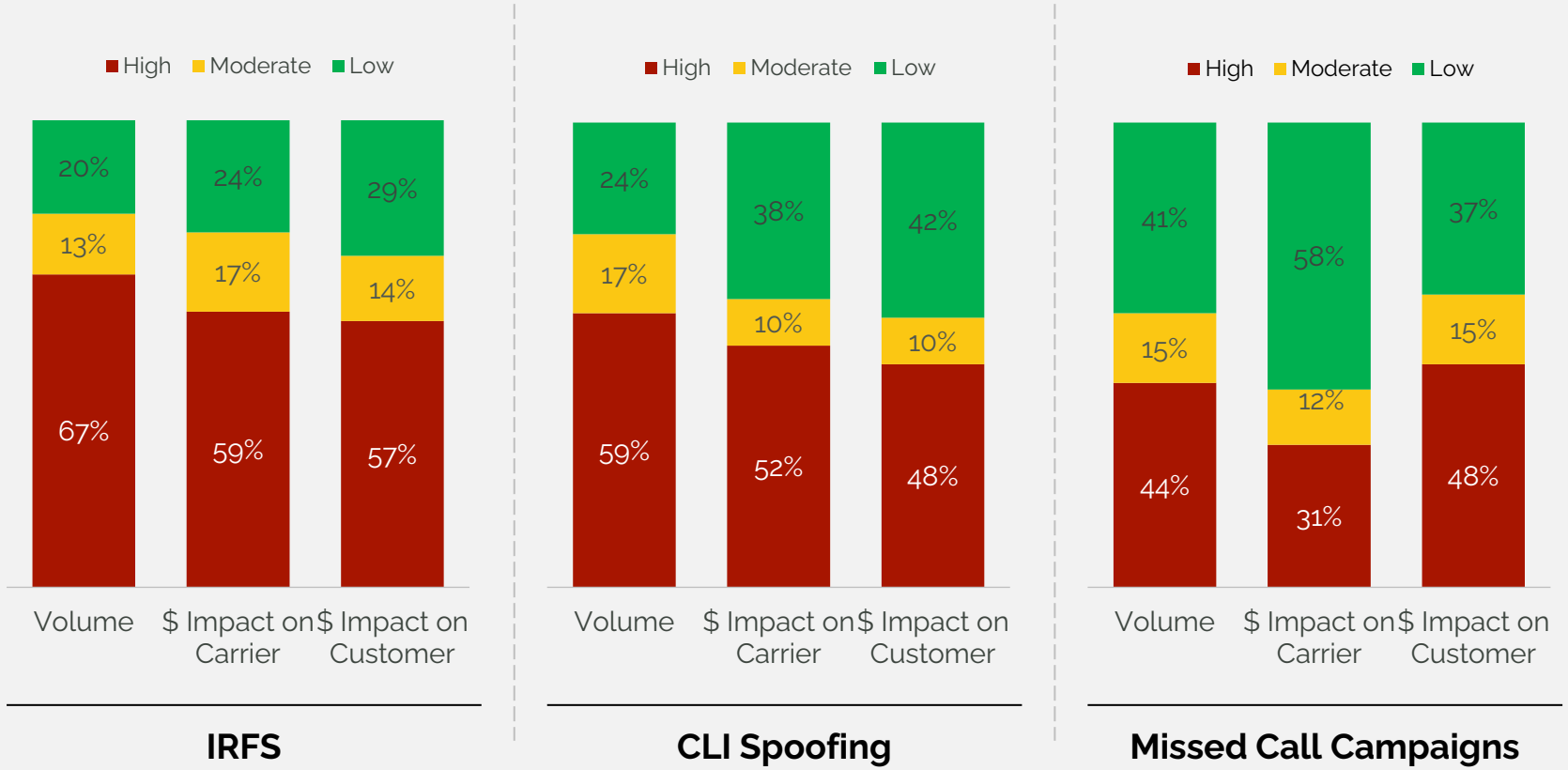
> *Ongoing threats like spoofing directly undermine brand reputation, leading to churn*

Deep-dives on next slides

03 INTERNATIONAL VOICE FRAUD

Most challenging types of fraudulent voice traffic

Fig. 8. Comparison of the top three voice fraud types by volume, financial impact on carrier and financial impact on final customer
(% responses)



Notes: n (2025) = 28
Source: GLF Survey 2025.

IRSF, CLI Spoofing and Missed call campaigns have risen as the top threats owing to evolving tactics and vulnerabilities in global telecom networks.

IRSF (International Revenue Share Fraud) exploits roaming and international traffic, where detection delays allow fraudsters to profit. Stronger real-time monitoring and AI tools are needed to stop attacks earlier.

CLI Spoofing is growing with VoIP, making caller ID manipulation easier. Enhanced caller authentication and industry collaboration are key to reducing its impact.

Missed Call Campaigns tricks users into calling back premium-rate numbers. Despite awareness, the impact remains high, highlighting the need for faster cross-border intelligence sharing and proactive blocking

> *IRSF persists because incentives remain, attackers simply shift numbers to keep revenue flowing*

DEEP-DIVE ON IRSF

Geographical Impact of International Revenue Share Fraud

Top countries where operators are seeing the highest incidence of IRSF fraud

IRSF remains one of the most persistent fraud challenges, but its geographic footprint is shifting. This year, the data shows a broader spread, with high incidences now reported across both emerging and developed regions. This evolution highlights how fraudsters are globalizing their operations, exploiting vulnerabilities wherever they exist. Carriers stress that tackling IRSF requires real-time detection, stronger international collaboration, and consistent enforcement beyond regional boundaries.

01 Tunisia

02 Burundi

03 Madagascar

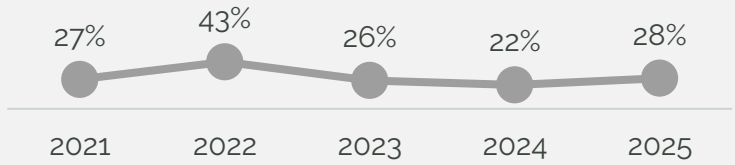
04 USA

05 Spain

IRSF has evolved from being an Africa-centric issue to a truly global threat. Fraudsters are moving fast, and unless detection and intelligence sharing keep pace, the problem will only expand

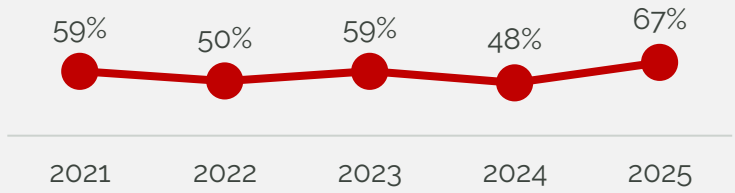
Note: Carriers were asked to name the top two countries with the most fraud by use-case in the survey. The most frequently mentioned countries were then compiled into the final list.
Source: GLF Surveys 2021, 2022, 2023, 2024, 2025.

Fig. 9. Respondents who said that the volume and impact of IRSF increased over the past 12 months
(% responses)



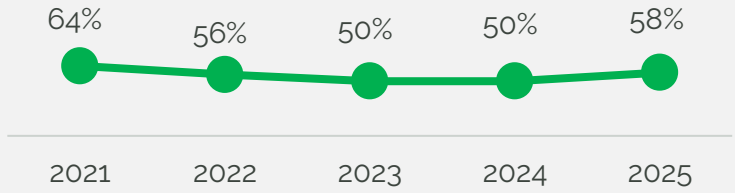
+ 1 p.p.
'21 - '25

Fig. 10. Respondents who said that they are experiencing a high volume of IRSF
(% responses)



+ 8 p.p.
'21 - '25

Fig. 11. Respondents who said that they are experiencing a high level of financial impact from IRSF
(% responses)



- 6 p.p.
'21 - '25

DEEP-DIVE ON CLI SPOOFING

Geographical Impact of CLI Spoofing

Top countries where operators are seeing the highest incidence of CLI Spoofing fraud

CLI Spoofing remains a persistent threat, with activity spreading beyond traditional hotspots to include a broader set of markets. Compared to last year, when issues were concentrated in the USA, Western Europe, and the Middle East, operators now report cases across a wider European footprint. Fraudsters continue to exploit VoIP-based caller ID manipulation, making detection complex and undermining customer confidence. While progress has been made in authentication and monitoring, gaps remain.

01 USA

02 UK

03 Belgium

04 Romania

05 France

CLI spoofing required advanced knowledge of telephony equipment. However, with open-source software, one can spoof calls with minimal effort

Note: Carriers were asked to name the top two countries with the most fraud by use-case in the survey. The most frequently mentioned countries were then compiled into the final list.
Source: GLF Surveys 2023-2025.

Fig. 12. Respondents who said that they experience a high volume of CLI spoofing
(% responses)

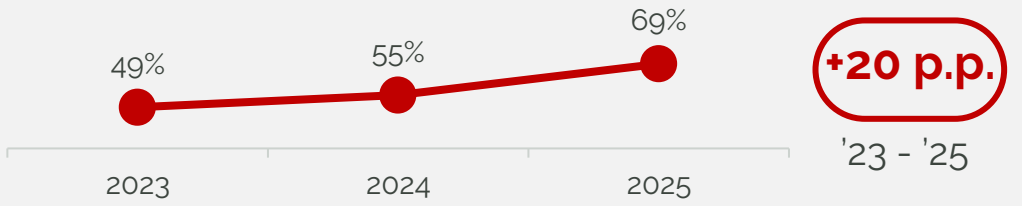
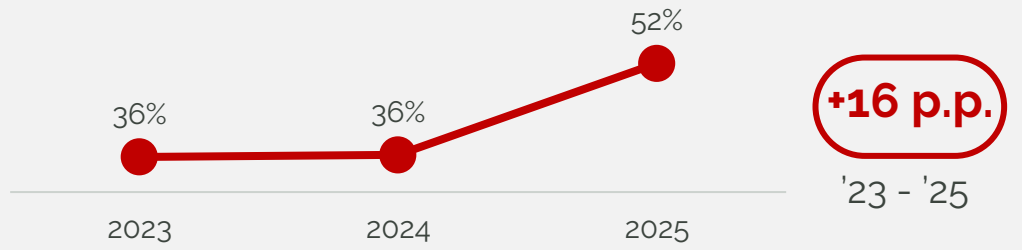


Fig. 13. Respondents who said that they experience a high level of financial impact from CLI spoofing (% responses)



DEEP-DIVE ON WANGIRI FRAUD

Geographical Impact of Wangiri / Missed Call Campaigns

Top countries where operators are seeing the highest incidence of Wangiri fraud

Wangiri fraud has expanded globally, with hotspots now spanning North America, North Africa, and Latin America. In this scheme, fraudsters generate missed calls from premium-rate or international numbers, luring victims to call back and incur high charges. While operators are tightening traffic validation and deploying advanced analytics to spot suspicious call patterns, cross-border collaboration remains essential to shut down these schemes at scale.

01 USA

02 UK

03 Tunisia

04 Morocco

05 Colombia

AI-driven traffic analysis is becoming essential for spotting the subtle patterns that humans often miss. The faster we automate detection, the fewer opportunities fraudsters have to exploit global networks

Note: Carriers were asked to name the top two countries with the most fraud by use-case in the survey. The most frequently mentioned countries were then compiled into the final list.
Source: GLF Surveys 2023-2025.

Fig. 14. Respondents who said that they experience a high volume of Wangiri Fraud
(% responses)

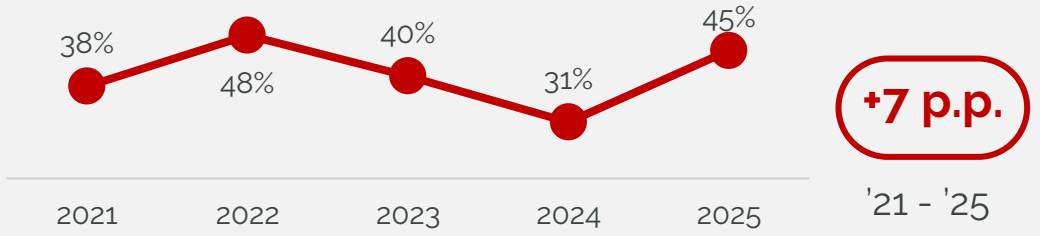
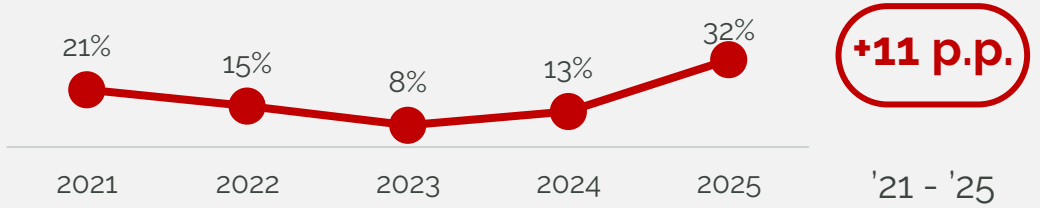


Fig. 15. Respondents who said that they experience a high level of financial impact from Wangiri Fraud (% responses)



03 GEOGRAPHIC SPREAD OF VOICE FRAUD

Top countries where operators are seeing the highest incidence of overall voice fraud

Voice fraud is no longer concentrated in a single region but has become a global issue. While parts of Africa remain consistent hotspots, major markets in North America and Europe are now also among the most impacted. This reflects the adaptability of fraudsters, who are targeting both high-value and high-traffic destinations. The shift underscores the need for stronger cross-border intelligence sharing and coordinated action.

01 USA

02 UK

03 Tunisia

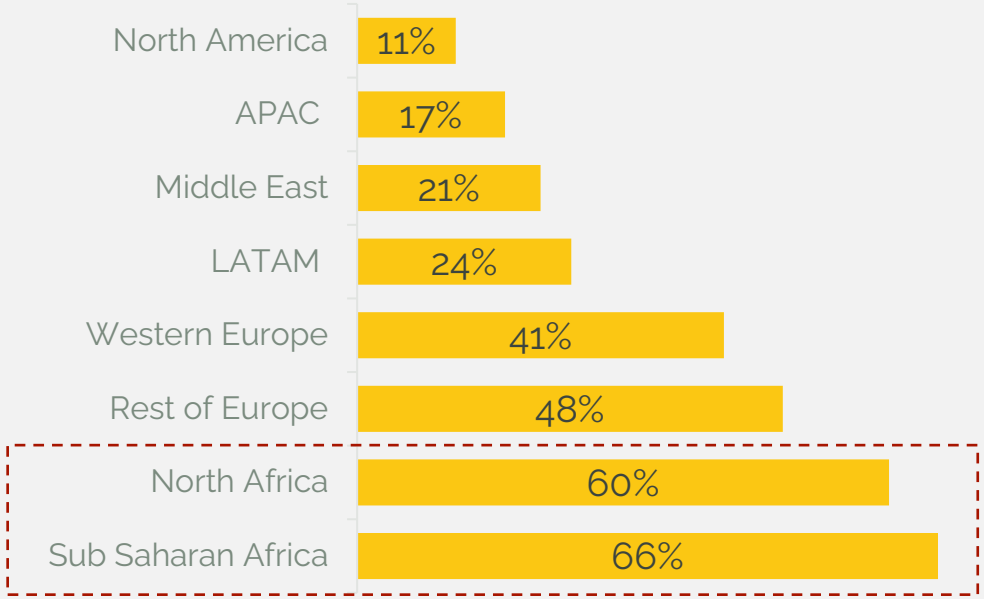
04 Morocco

05 Zimbabwe

> *Fraud is evolving into a borderless threat, and carriers everywhere are at risk. Only by sharing intelligence globally and acting in real time can we hope to stay ahead of fraudsters*

Note: Carriers were asked to name the top two countries with the most fraud by use-case in the survey. The most frequently mentioned countries were then compiled into the final list.
Source: GLF Survey 2025.

Fig. 16. Respondents who said that they experience a high volume of voice fraud per region
(% responses)



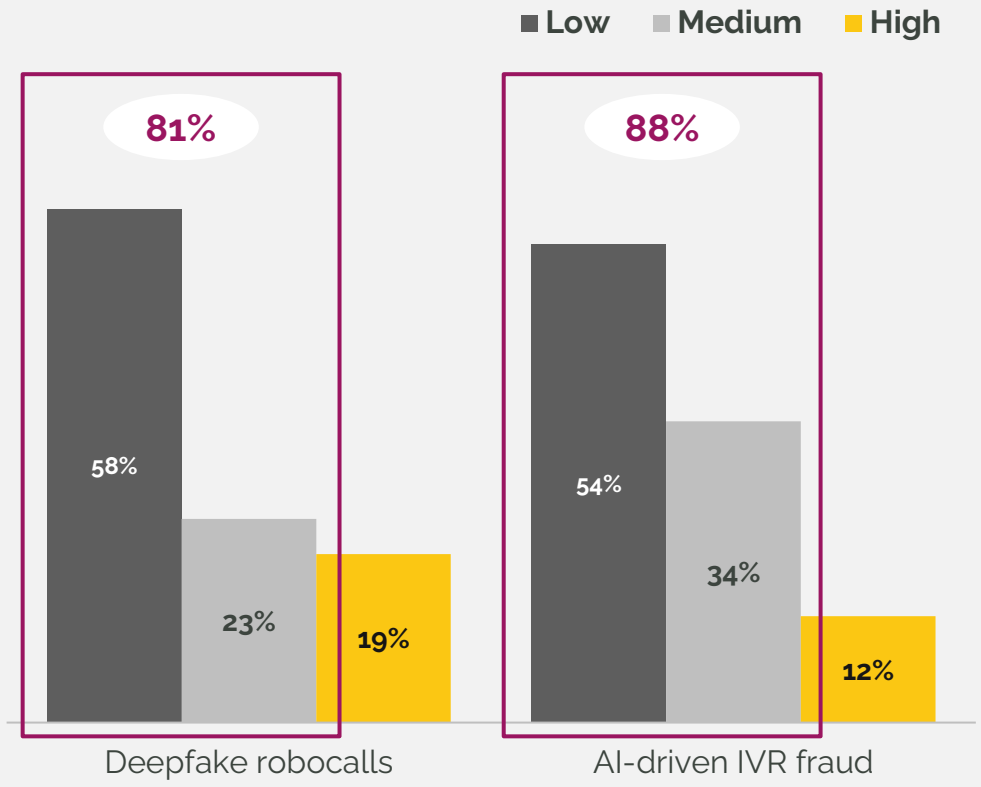
Voice fraud continues to show significant regional variation, with Africa standing out as the most impacted region. **Sub-Saharan Africa (66%) and North Africa (60%) report the high volumes of fraud**, reflecting challenges stated by survey respondents with revenue share fraud and weak enforcement environments.

Many carriers also report high fraud volumes in Rest of Europe (48%) and Western Europe (41%), where fraudsters exploit complex cross-border routing and regulatory gaps.

03 INTERNATIONAL VOICE FRAUD

AI-generated voice traffic

Fig. 17. Volume of AI-generated voice fraud by fraud type in the last year
(% responses)

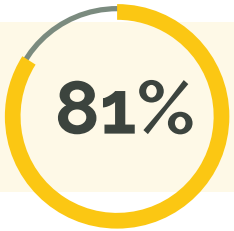


While AI has transformed fraud tactics, **most carriers continue to report low to medium volumes of AI-generated voice fraud.**

- **81% of respondents report low to medium volumes of deepfake robocalls**
- **88% report low to medium volumes of AI-driven IVR fraud**

Although AI-driven fraud in telecom remains low in volume, its potential for severe impact is significant, with fraudsters rapidly advancing deepfakes, spoofing, and adaptive tools beyond current detection speeds. Widely available voice cloning enables real-time impersonation of executives or family in vishing attacks, boosting social engineering like fake kidnappings (e.g., 2024 Arizona cases). **In wholesale, AI facilitates IRSF, Wangiri, and bypass fraud via impersonated officials or evasion tactics**. Robocalls, such as the 2024 Biden spoof, pose disinformation risks. North America reported a 1,740% deepfake surge (2022–2023), with Q1 2025 losses over $200 million[1]. Regulations like the EU AI Act (2024) and U.S. proposals demand transparency and penalties. The industry views this as an emerging threat requiring urgent investment in proactive detection.

> *Fraud adapts quickly due to fraudsters' agility in leveraging emerging technologies like AI for deepfakes, adaptive phishing, and call interception, outpacing the slower rollout of industry-wide standards and tools*



of carriers report low to medium volume of AI-generated voice fraud

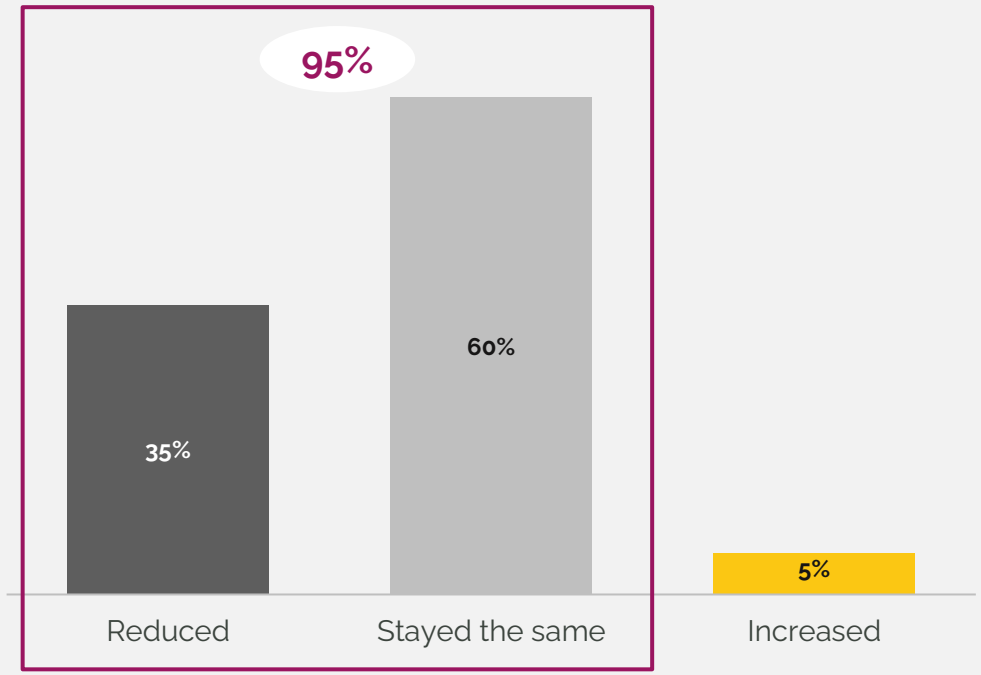
Notes: n(2025) = 26.
Source: GLF Survey 2025, (1) World Economic Forum.

03 INTERNATIONAL VOICE FRAUD

Fraudulent voice traffic on 5G networks

Fig. 18. Change in volume of 5G related fraudulent traffic in the last year

(% responses)



The rollout of 5G has not led to a notable rise in fraudulent voice traffic, **with 95% of carriers reporting volumes that have decreased or remained stable over the past year, and only 5% noting an increase**. This indicates that initial security investments are effective. 5G's features—ultra-low latency, massive connectivity, and enhanced encryption—bolster defences through advanced authentication, real-time AI detection, voice biometrics, and SDN, while phasing out legacy vulnerabilities, potentially capping voice and SMS fraud below $20 billion by 2028.

However, **5G introduces new risks**: scalable IoT botnets for IRSF/Wangiri, subscription/roaming fraud creating potential to $8 billion data roaming losses by 2028[1], encrypted bypass scams, network slicing hijacks, and AI-amplified deepfake vishing/robocalls. Encryption may obscure detection, increasing complexity. Overall, **5G reduces traditional threats but enables sophisticated ones**, demanding ongoing investments in AI tools and secure APIs for mitigation.

> *5G cuts down legacy fraud but opens the door to new risks like IoT exploits, encrypted bypass, and AI-driven scams.*

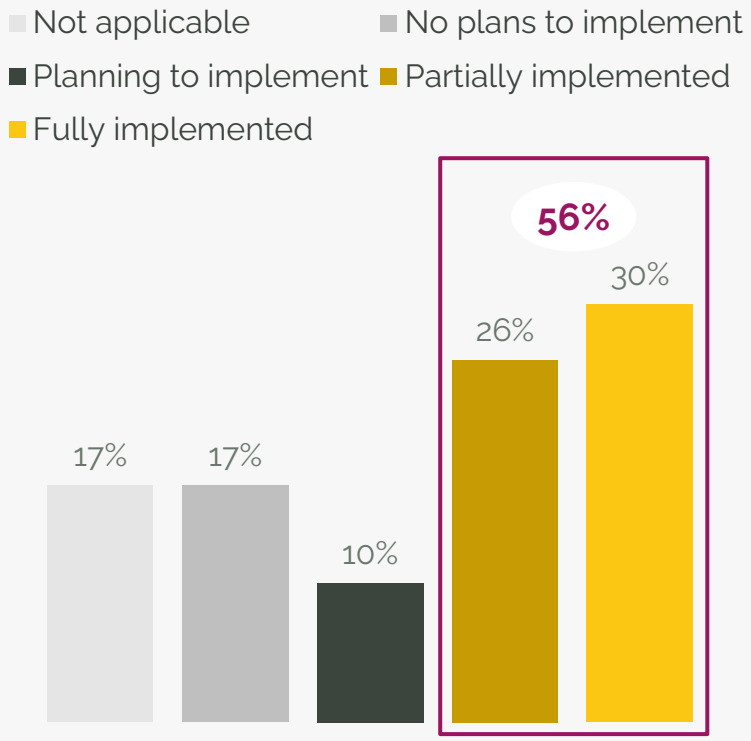
of carriers say that the volume of 5G related fraudulent traffic has reduced or stayed the same

Notes: n(2025) = 20.
Source: GLF Survey 2025, (1) Juniper Research, Kaleido Intelligence, GSMA.

03 INTERNATIONAL VOICE FRAUD

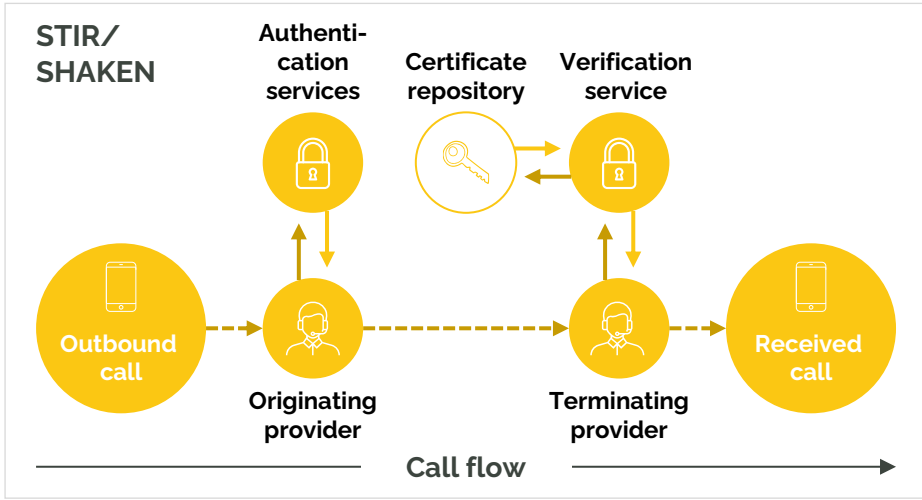
Compliance with voice authentication protocols such as STIR/SHAKEN

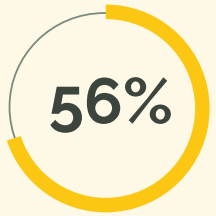
Fig. 19. Level of implementation of voice authentication protocols such as STIR/SHAKEN in 2025
(% responses)



In 2025, 30% of carriers reported that they have fully implemented voice authentication protocols and an additional 26% have partially implemented it.

STIR/SHAKEN is a standards framework designed to combat caller ID spoofing, ensuring that displayed numbers can be verified as legitimate and untampered. Wholesale telcos are increasingly adopting it as well as other voice authentication protocols as fraudulent traffic grows in scale and sophistication. With regulators tightening requirements in key markets, and customers demanding stronger safeguards, carriers face rising pressure to act. For operators, deploying STIR/SHAKEN not only reduces exposure to fraud-related losses and reputational damage, but also creates a differentiator in terms of trustworthiness.





of carriers have partially or fully **implemented voice authentication protocols such as STIR/SHAKEN**

Notes: n(2025) = 23
Source: GLF Survey 2025.

03 INTERNATIONAL VOICE FRAUD

Conclusion

01

More than half of operators (52%) are now reporting a reduction in fraudulent voice traffic, representing the highest rate observed since 2018. This improvement is fuelled by the implementation of cutting-edge AI-based fraud management systems, stronger sector-wide partnerships, and effective practices like pre-emptively restricting high-risk number ranges, implementing precise traffic limits, and strengthening oversight of vulnerable routes.

02

Telecommunications carriers continue to encounter substantial levels of IRSF, CLI spoofing, Wangiri, and OBR fraud, all of which carry major financial threats. IRSF capitalises on international call flows, CLI spoofing supports vishing and bypass schemes, Wangiri leads to revenue shortfalls via missed-call tactics that deceive individuals into dialling back premium-rate international lines, and OBR fraud alters routing mechanisms to drive up expenses and siphon profits from authorised providers.

03

Although AI is transforming fraud methodologies, most carriers continue to experience only low to moderate levels of AI-generated voice fraud, with more than 80% reporting sparse occurrences of deepfake robocalls and AI-orchestrated IVR deceptions. Likewise, the advent of 5G has not sparked a rise in fraudulent traffic, as 95% of carriers indicate that volumes have remained consistent or diminished. These patterns indicate that while fraudsters are testing novel technologies, their broad-scale influence is still nascent. Given the opportunities these technologies present for fraudulent activity focus is required.

Source: GLF Survey 2025.

04

INTERNATIONAL MESSAGING FRAUD

GLOBAL LEADERS' FORUM

GLF™

a techoraco brand

04 INTERNATIONAL MESSAGING FRAUD

Definitions

SMS Phishing (Smishing) 01
SMS phishing creates a legitimate-looking message impersonating a legitimate entity to obtain, through deception and social engineering, the end-user's personal information or other sensitive data. In some cases, smishing can be compounded by voice fraud, when a number is originally listed in a smishing message and the user calls a high-cost destination.

SMS Roaming intercept 02
The interception of legitimate messaging traffic when a user is roaming on another network, SMS roaming intercept is mostly used to intercept two-factor authentication messages or one-time passwords (OTPs) to access the final user's banking or mailing accounts.

SMS originator Spoofing 03
The use of aggregation routes and unchecked parts of the system to hide the originator's identity and trick the receiving party into believing it is a legitimate originator. SMS originator spoofing is used in combination with phishing to make the message appear more legitimate to the victim.

SMS Malware 04
Malware is installed by clicking on a link sent in a legitimate-looking message from a malicious party. The software gains control of the mobile phone's data and might steal sensitive information such as banking details or account passwords.

SMS Swap – OTP intercept 05
The fraudster gains control of the victim's SIM card to intercept incoming legitimate text traffic, which may include sensitive data such as OTPs or sensitive banking information that might be used to commit further fraud.

Artificially Inflated Traffic (AIT) 06
AIT is the fraudulent generation of fake A2P network activity, often for financial gain or disruption, and includes practices like pumping computer-generated traffic and creating fake web traffic through legitimate services, resulting in financial losses and network disturbances.

SMS trashing 07
SMS trashing involves deliberately discarding or deleting SMS messages before they reach their intended destination, often to prevent legitimate communications or to manipulate message delivery statistics.

Source: i3 Forum, Fraud classification and recommendations on dispute handling: Release 4.0, March 2023; GLF; FTI Delta analysis.

04 INTERNATIONAL MESSAGING FRAUD

Introduction

Messaging has overtaken voice as the primary channel for fraud, but carriers have responded proactively with targeted safeguards and advanced features, achieving measurable success in reducing these threats. In this section, we explore key trends in messaging fraud, including AIT and Smishing, and examine their impact on both carriers and end-users.

01

Thirty-five percent (35%) of carriers reported an increase in the volume and impact of SMS fraud, a substantial reduction of 20 p.p. from what it was in 2024. This suggests that the proactive measures taken by carriers such as better blocking systems, real-time monitoring, and stronger industry-wide collaboration have paid dividends. Still, carriers emphasise the need for continuous AI upgrades and closer regulatory collaboration to sustain these gains and stay ahead of more sophisticated AI-driven threats.

02

Three messaging fraud types have emerged as the most prevalent: smishing, artificially inflated traffic, and SMS originator spoofing.

a. **Artificially Inflated Traffic (AIT)** remains a major issue, with 54% of operators reporting high volumes in 2025, however proactive action from telcos in identifying responsible parties has led to a reduction of 12 p.p. in the last year. It however continues to be the most financially damaging with 50% of operators reporting high financial losses.

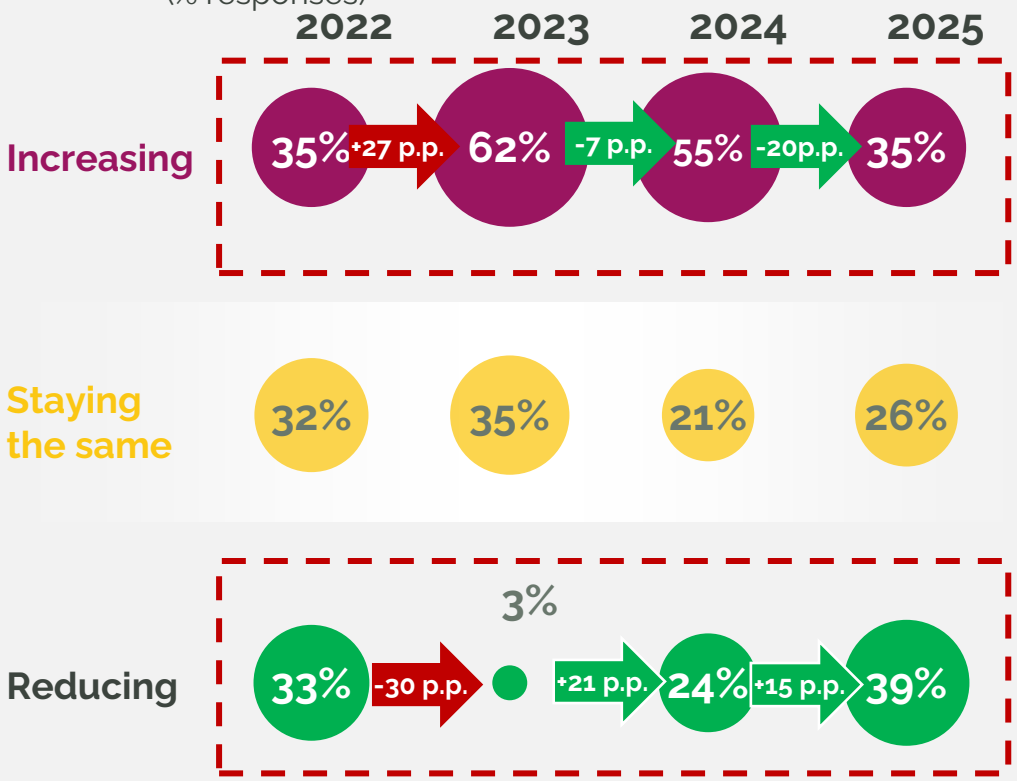
b. **Smishing** is the most widespread type of fraud and has seen a substantial rise in the last 2 years, with almost twice the number of carriers (61%) reporting high volume in 2025 as compared to 2023. These attacks can be highly damaging for end users, and the lack of advanced prevention tools, allows these to bypass security measures.

c. **SMS originator spoofing** has seen a 9-percentage point increase in carriers reporting high volumes, going from 24% in 2024 to 33% in 2025, and remains a threat especially in regions with weaker security. It can also have serious consequences for end-users with 37% of carriers reporting high end-user financial losses sustained due to this fraud.

04 INTERNATIONAL MESSAGING FRAUD

The volume and impact of fraudulent messaging traffic

Fig. 20. Year-on-year comparison of the volume and impact of fraudulent messaging traffic
(% responses)



In 2025, only 35% of respondents report an increase in fraudulent messaging traffic—a sharp drop from 62% in 2023 and 55% in 2024, marking a clear downward trend. This drop reflects stronger anti-fraud controls, the wider adoption of AI-driven detection, and more mature A2P monitoring frameworks. Some carriers also believe this decrease may be in part due to reduction of SMS traffic as partners use alternative messaging channels. However, vulnerabilities remain due to high termination rates, regulatory gaps in certain markets, and fraudsters' continued shift toward exploiting the more profitable SMS channel.

At the same time, 39% of carriers reported a reduction in SMS fraud, up significantly from just 24% in 2024. This progress is largely attributed to improved blocking systems, greater cross-operator intelligence sharing, and deeper partnerships with regulators and aggregators. Operators emphasise that sustaining these gains will require ongoing technology investment, broader industry cooperation, and constant adaptation as fraud tactics evolve.

> *Frauds that were on voice have moved almost completely to messaging. Messaging fraud is much harder to detect – you can see anomalies in voice traffic quickly, but SMS campaigns are harder to spot and manage in real time*

of carriers report a reducing volume and impact of fraudulent messaging traffic

Note: (1) 2022 was the first year GLF started collecting responses on messaging; (2) n (2022) = 31, n (2023) = 34, n (2024) = 33, n(2025) = 32.
Source: GLF Survey 2025.

04 INTERNATIONAL MESSAGING FRAUD

Extracts from the conversations with the carriers on fraudulent messaging traffic

xx% % of responses

What is driving the change in the volume and impact of fraudulent messaging traffic hitting your organisation in the past 12 months?

Reduce 39%

The reduction has been driven by improved controls, stronger collaboration with traffic sources, and a migration from SMS to RCS

Fraud levels have reduced after implementing real-time monitoring solutions. Without them, we would have seen a 200%+ increase

We have launched anti-spam measures, and proactive monitoring by MNOs across the industry has helped drive down fraud levels

No change 26%

Messaging fraud remains difficult to detect on SMS, and the industry is still in the early stages of building effective defences

The decreasing trend of A2P SMS traffic due to OTT services (WhatsApp)

Recently entered into this market so we are starting to see more fraud as we continue growing

Increase 35%

Key drivers include lack of message filtering at origination, use of grey routes, and rapid abuse of dynamic sender IDs and phishing links

AIT is the main driver. Trashing, smishing, bypass (including Spoofing) are also growing.

The rising use of A2P SMS for authentication and marketing, combined with grey routes and dynamic sender IDs

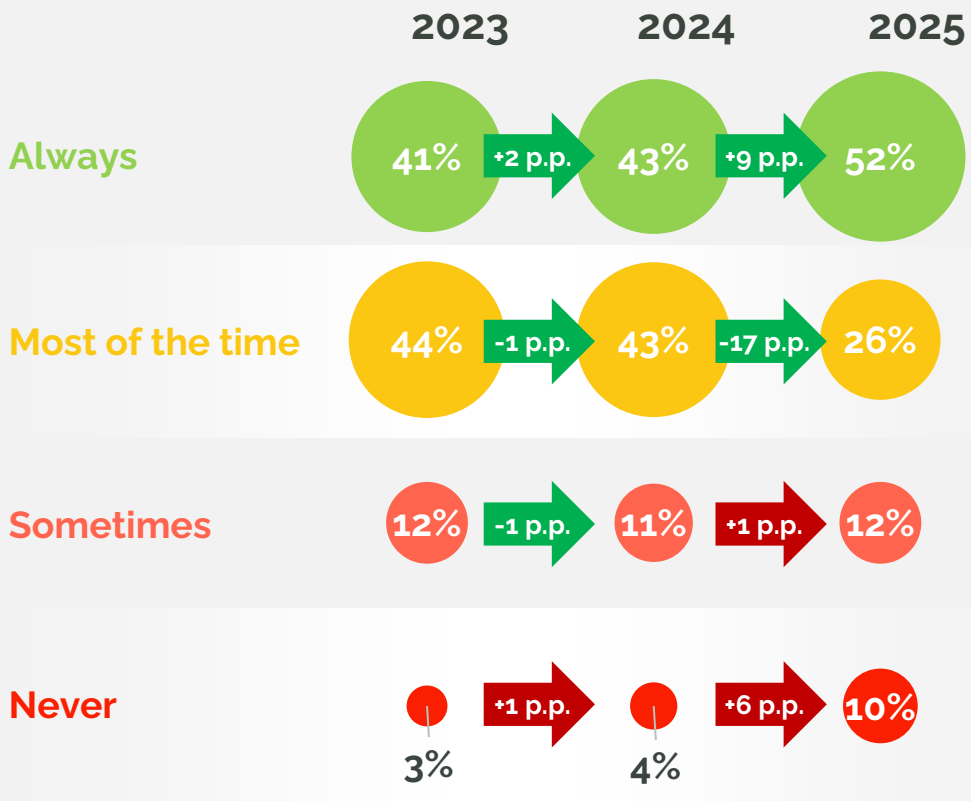
Source: GLF Survey 2025.

04 INTERNATIONAL MESSAGING FRAUD

Blocking and associated challenges

Fig. 21. Year-on-year comparison of the extent of blocking of fraudulent messages

(% responses)



The percentage of carriers that consistently block detected fraudulent messages has climbed substantially from 41% in 2023 to 52% in 2025, reflecting a deeper dedication to proactive fraud mitigation. Meanwhile, the share that blocks fraud most of the time has fallen dramatically from 44% in 2023 to 26% in 2025, indicating a transition to more rigorous and uniform enforcement practices.

Yet, hurdles persist. **A minor but expanding portion of carriers still block fraud only occasionally (12% in 2025) or never (10% in 2025)**. This points to enduring obstacles, including constraints in instantaneous detection, apprehension about disrupting valid traffic, and shortcomings in transnational cooperation. Though the broader trajectory is optimistic, the inconsistencies underscore that many telecom providers are still weighing fraud safeguards against operational reliability and user satisfaction. Carriers must keep allocating resources to AI-enhanced detection platforms to curb false positives, allowing for precise fraud spotting and interception while upholding service standards and consumer loyalty.

> *On messaging it is much more difficult – one campaign can hit millions of numbers. You cannot just block the receiver; you have to block the sender, often case by case. Automated systems help, but human analysis is still needed*

of carriers report that **they always block fraudulent messages upon detection**

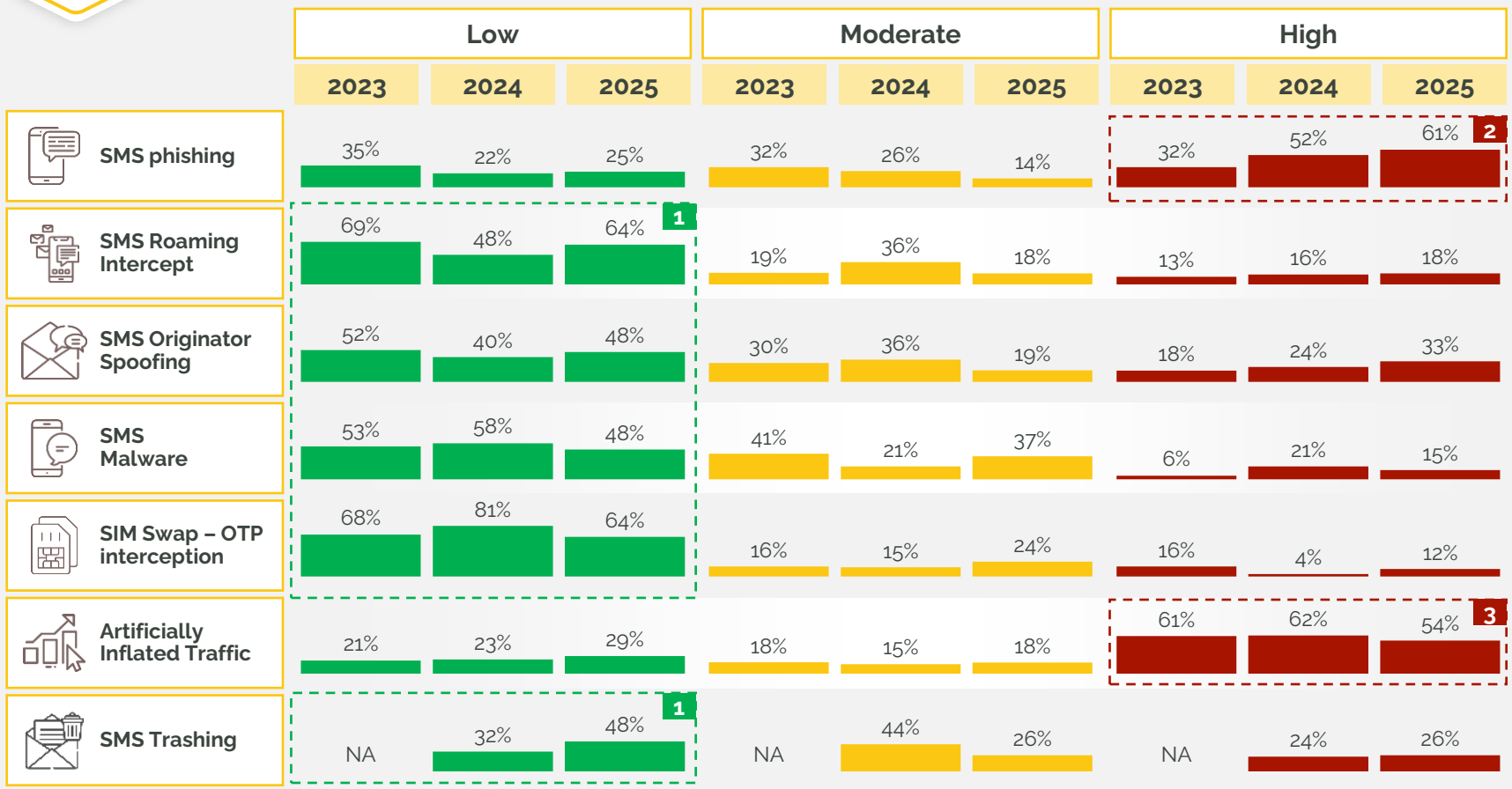
Notes: n(2025) = 23
Source: GLF Survey 2025.

04 INTERNATIONAL MESSAGING FRAUD

The volume of fraudulent messaging traffic, by use case

Fig. 22. Historical change in volume of fraudulent messaging traffic, by fraud use case

(% responses)



Notes: n (2023) = 36; n (2024) = 33; n (2025) = 28.
Source: GLF Survey 2025.

1 Most SMS fraud types are effectively contained by intelligent detection tools. However, vulnerabilities in certain areas remain, requiring continued vigilance and improvement in detection systems.

2 Smishing continues to grow with 61% of responders reporting high volume due to it being financially profitable. A few successful attacks can lead to significant losses for victims. The lack of advanced prevention tools, compared to voice, allows these attacks to bypass security measures.

3 AIT remains a major issue, with 54% of operators reporting high volumes in 2025, however proactive action from telcos in identifying responsible parties has led to a reduction of 12 p.p. in the last year.

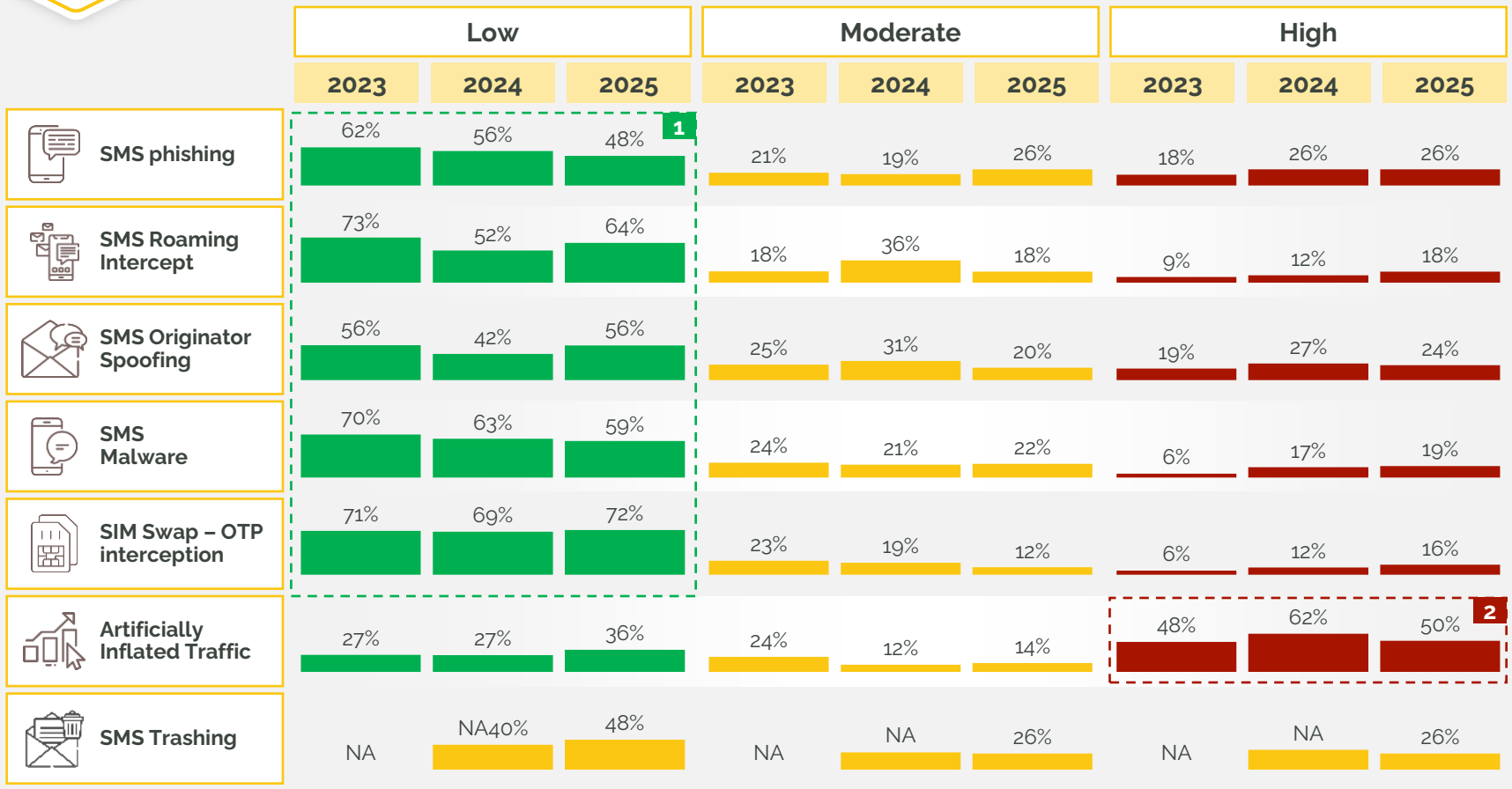
> *Fraudsters use grey routes, dynamic sender IDs, and phishing links to disguise attacks at scale.*

04 INTERNATIONAL MESSAGING FRAUD

The financial impact from fraudulent messaging traffic, by use case

Fig. 23. Historical change in financial impact experienced by carriers, by fraud use case

(% responses)



Notes: n (2023) = 36; n (2024) = 33; n (2025) = 28.
Source: GLF Survey 2025

1 Compared to AIT, other SMS fraud types — **phishing, roaming intercept, originator spoofing, malware and SIM swap — have a low financial impact, with at least 45%–50% of operators reporting a low impact in 2025**

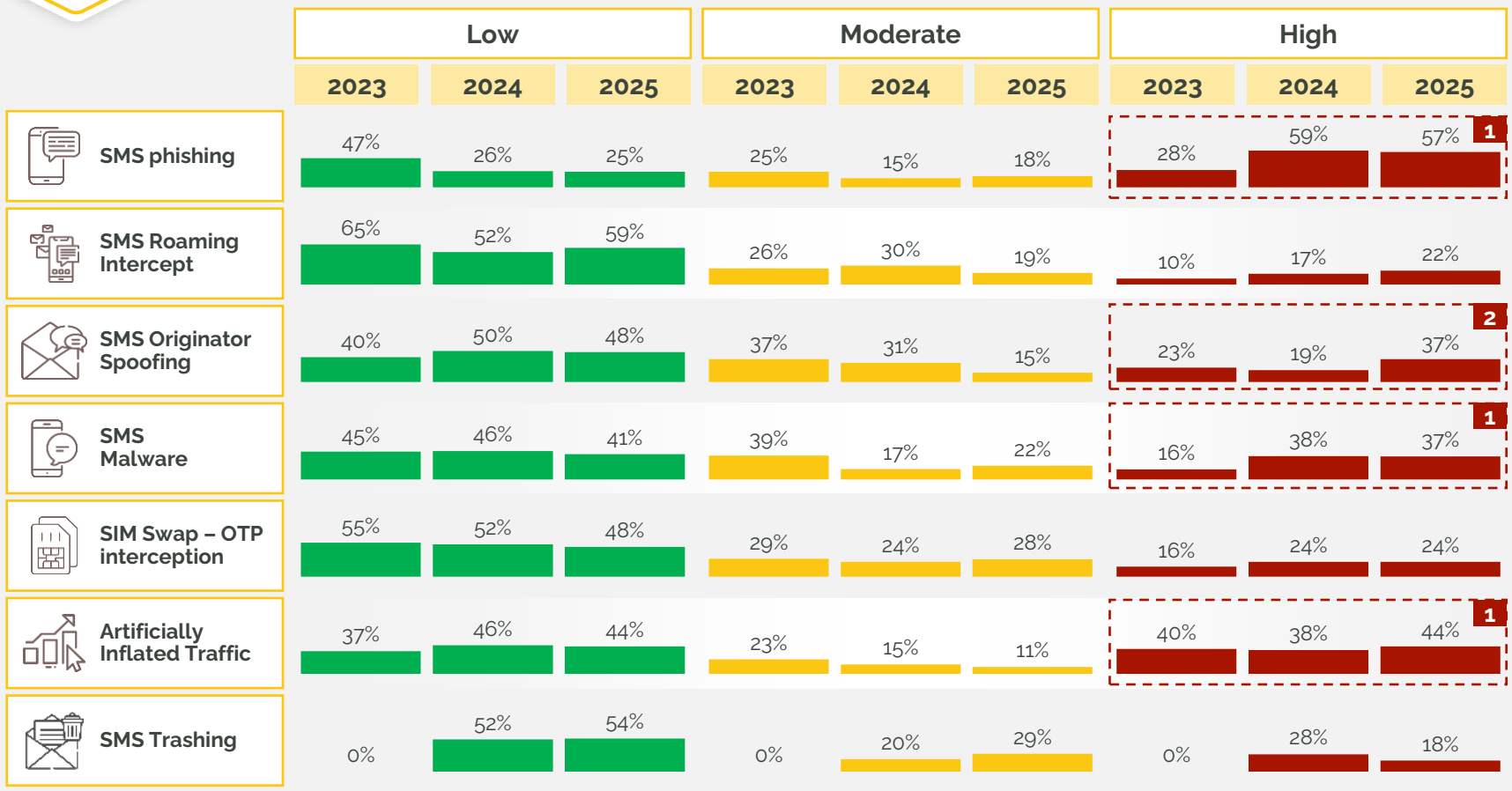
2 AIT impact remains high, making it the most financially significant type of fraud for carriers. This is driven by high termination rates and the growing use of OTPs, which fraudsters exploit to inflate traffic. Additionally, pressure from brands to meet volume commitments has contributed to the rise of illegitimate traffic.

However, carriers have fought back using real-time fraud detection and by following an Aggregator/Carrier Code of Conduct, including withholding payments when necessary. **This has resulted in a drop of 12p.p. of responders reporting high impact**. Brands must continue to fight AIT by prioritising traffic with compliant partners, sharing anonymised data with peers to detect fraud patterns, and leveraging industry databases.

04 INTERNATIONAL MESSAGING FRAUD

The financial impact from fraudulent messaging traffic, by use case

Fig. 24. Level of financial impact experienced by end-users, by fraud use case
(% responses)



Notes: n (2023) = 36; n (2024) = 33; n (2025) = 28.
Source: GLF Survey 2025.

1 Despite year-on-year fluctuations, reports of high impact from **SMS phishing, SMS malware, and artificially inflated traffic** has stayed at elevated levels. Fraudsters continue to exploit consumer trust, malware infiltration, and high termination rates, while carriers still face gaps in real-time detection. These threats remain steady because they are proven, scalable, and difficult to eradicate.

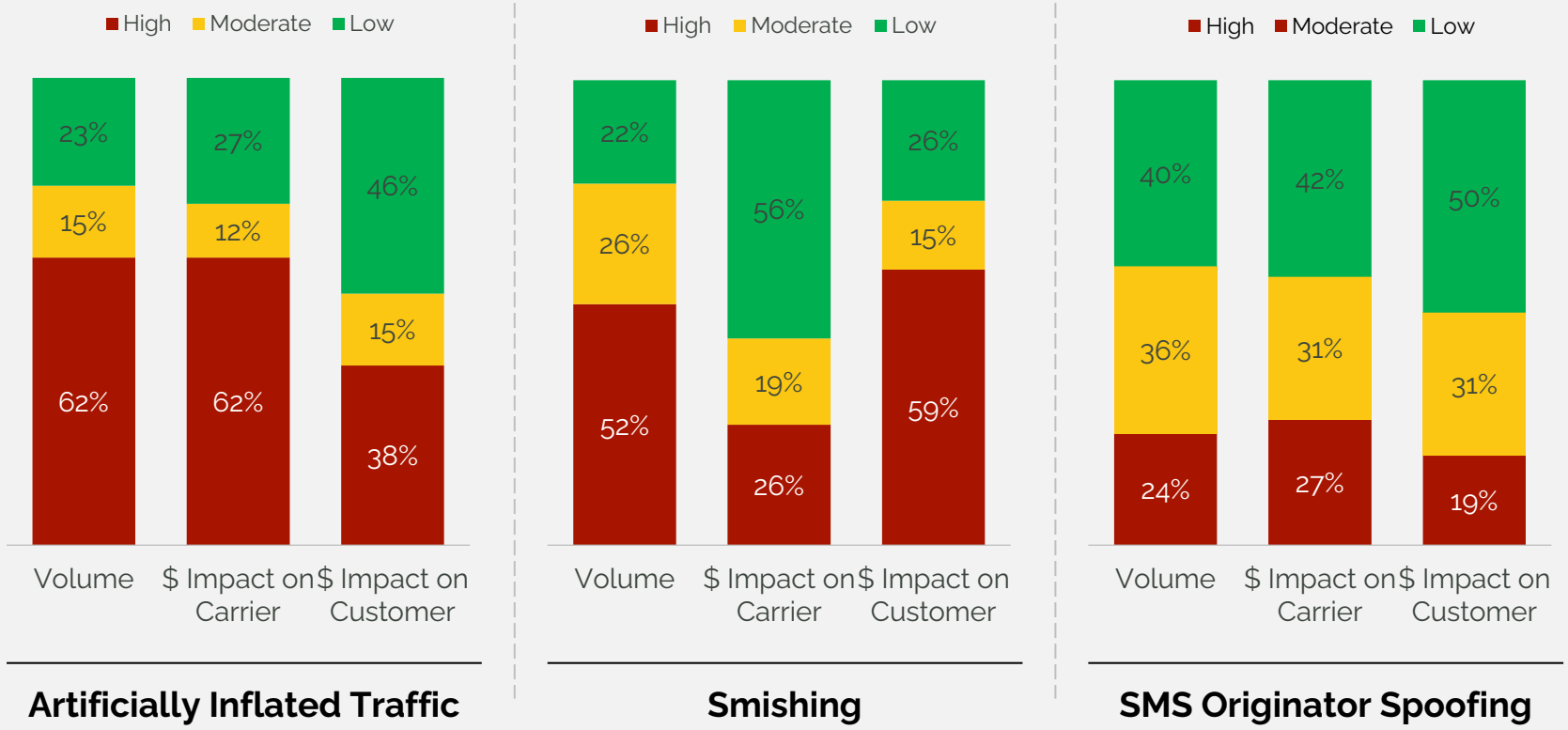
2 **There is a marked increase in the number of carriers (+18 p.p.) reporting high financial impact of SMS originator spoofing,** as fraudsters use fake sender IDs to impersonate trusted brands and deceive users. This tactic is growing in sophistication, making it harder for end-users to recognise fraudulent messages.

Strengthening fraud detection technologies and collaborating across the industry to set stricter standards are key steps. Furthermore, focusing on consumer education will empower users to better recognise and avoid fraud.

04 INTERNATIONAL MESSAGING FRAUD

Most challenging types of fraudulent messaging traffic

Fig. 25. Comparison of the top three messaging fraud types by volume, financial impact on carrier, and financial impact on end-user
(% responses)



Notes: n(2025) = 28.
Source: GLF Survey 2025.

Smishing, AIT, and SMS originator spoofing remain the dominant forms of messaging fraud.

AIT stands out as the fraud category most frequently cited by carriers for high volumes, positioning it as a major economic challenge for providers owing to escalated traffic expenses.

Although fewer carriers note high fraud volumes for smishing compared to AIT, it inflicts the greatest documented financial harm on end-users, as numerous individuals succumb to misleading tactics resulting in considerable monetary damages.

Lastly, **SMS originator spoofing, despite its relatively reduced volume and consequences, continues to present threats**. Carriers should primarily concentrate on bolstering security measures to address it.

> *For voice you see the spike in traffic and can act, but it is not as easy on messaging*

DEEP-DIVE ON AIT

Geographical Impact of AIT

Top countries where operators are seeing the highest incidence of AIT

AIT remains a persistent challenge, with hotspots shifting compared to last year. While South Asia featured prominently before, this year's reports highlight a broader spread across Europe, Asia, and Africa. The mix of developed and emerging markets underscores how both regulatory gaps and market practices continue to create vulnerabilities. Transparency in commercial agreements and cross-border alignment remain critical to curbing artificially inflated traffic.

01 UK

02 Bangladesh

03 Sudan

04 Indonesia

05 France

> *The drivers of AIT are often systemic, tied to commercial practices, which means the solution must come from stronger collaboration and accountability within the industry itself.*

Note: Carriers were asked to name the top two countries with the most fraud by use-case in the survey. The most frequently mentioned countries were then compiled into the final list.
Source: GLF Survey 2023-2025

Fig. 26. Share of respondents who said that the volume and impact of AIT increased over the past 12 months
(% responses)

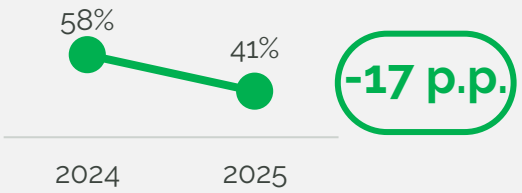


Fig. 27. Share of respondents who said that they are experiencing a high volume of AIT
(% responses)

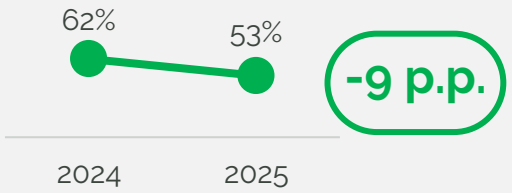
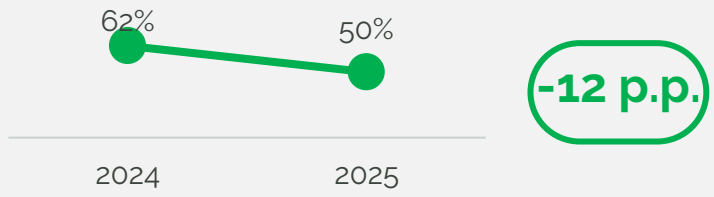


Fig. 28. Share of respondents who said that they are experiencing a high level of financial impact from AIT
(% responses)



DEEP-DIVE ON SMS PHISHING (SMISHING)

Geographical Impact of Smishing

Top countries where operators are seeing the highest incidence of smishing

Smishing continues to rise, but the geographic profile has shifted significantly from last year. While previously concentrated in Africa and parts of Europe, it is now more widely reported across Europe and Asia. Fraudsters are exploiting weak controls in cross-border SMS delivery and adapting their tactics to bypass traditional spam filters. Operators are responding with stronger content screening, enhanced authentication, and closer cooperation with regulators, but gaps remain in consistency across regions.

01 Spain

02 UK

03 France

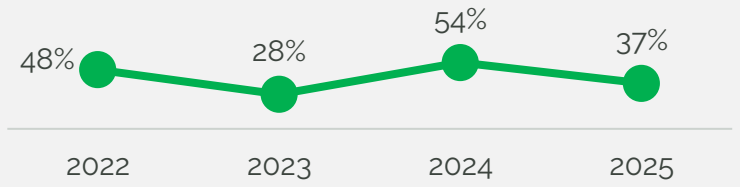
04 India

05 Nigeria

Smishing is evolving faster than defences, with fraudsters tailoring attacks to local markets. The industry needs more standardised protections across borders, otherwise these schemes will simply migrate to the weakest link

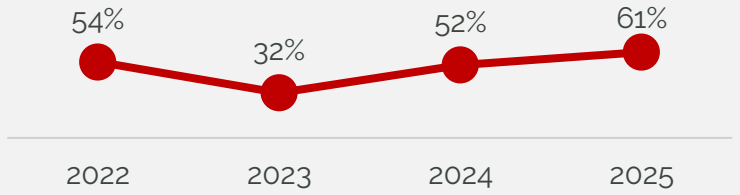
Note: Carriers were asked to name the top two countries with the most fraud by use-case in the survey. The most frequently mentioned countries were then compiled into the final list.
Source: GLF Surveys 2022-25.

Fig. 29. Share of respondents who said that the volume and impact of smishing increased over the past 12 months
(% responses)



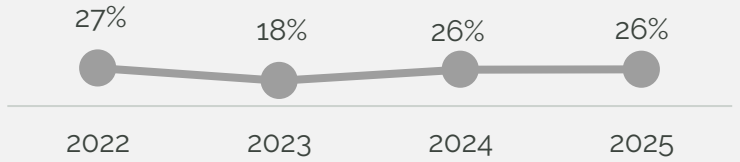
-11 p.p.
'22 - '25

Fig. 30. Share of respondents who said that they are experiencing a high volume of smishing
(% responses)



+7 p.p.
'22 - '25

Fig. 31. Share of respondents who said that they are experiencing a high level of financial impact from smishing
(% responses)



+0 p.p.
'22 - '25

DEEP-DIVE ON SMS ORIGINATOR SPOOFING

Geographical Impact of SMS Originator Spoofing

Top countries where operators are seeing the highest incidence of fraud

Though there has been a reduction in carriers who report a high volume of SMS Originator Spoofing, it is still a major threat and continues to shift geographically. While last year's hotspots were more concentrated in Africa and the Middle East, this year's data highlights a stronger presence across Europe and North America. The persistence of spoofing reflects both regional weaknesses in authentication and fraudsters' ability to adapt quickly to local defences.

01 USA

02 Germany

03 France

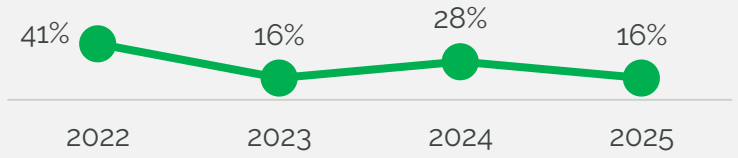
04 Spain

05 South Africa

Fraudsters are highly opportunistic — as soon as one region tightens controls, they move to softer targets elsewhere. Until authentication standards are harmonised globally, spoofing will remain a recurring threat

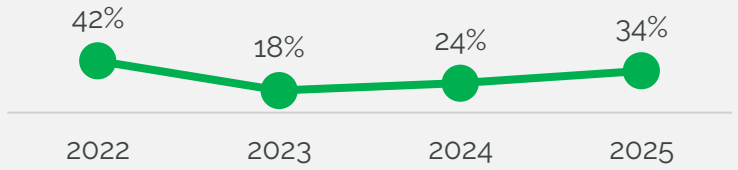
Note: Carriers were asked to name the top two countries with the most fraud by use-case in the survey. The most frequently mentioned countries were then compiled into the final list.
Source: GLF Surveys 2022-25.

Fig. 32. Share of respondents who said that the volume and impact of SMS Originator Spoofing increased over the past 12 months
(% responses)



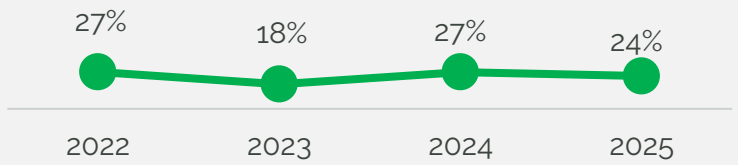
-25 p.p.
'22 - '25

Fig. 33. Share of respondents who said that they are experiencing a high volume of SMS Originator Spoofing
(% responses)



-8 p.p.
'22 - '25

Fig. 34. Share of respondents who said that they are experiencing a high level of financial impact from SMS Originator Spoofing
(% responses)



-3 p.p.
'22 - '24

04 GEOGRAPHIC SPREAD OF MESSAGING FRAUD

Top countries where operators are seeing the highest incidence of fraud

Messaging fraud is increasingly concentrated in markets with high traffic volumes and diverse international connections. Fraudsters are exploiting vulnerabilities in both established and emerging regions, with activity spanning Europe, South Asia, and beyond. The presence of both developed and developing markets in the top list highlights how fraud adapts to regulatory gaps and inconsistent enforcement across regions.

01 UK

02 India

03 Pakistan

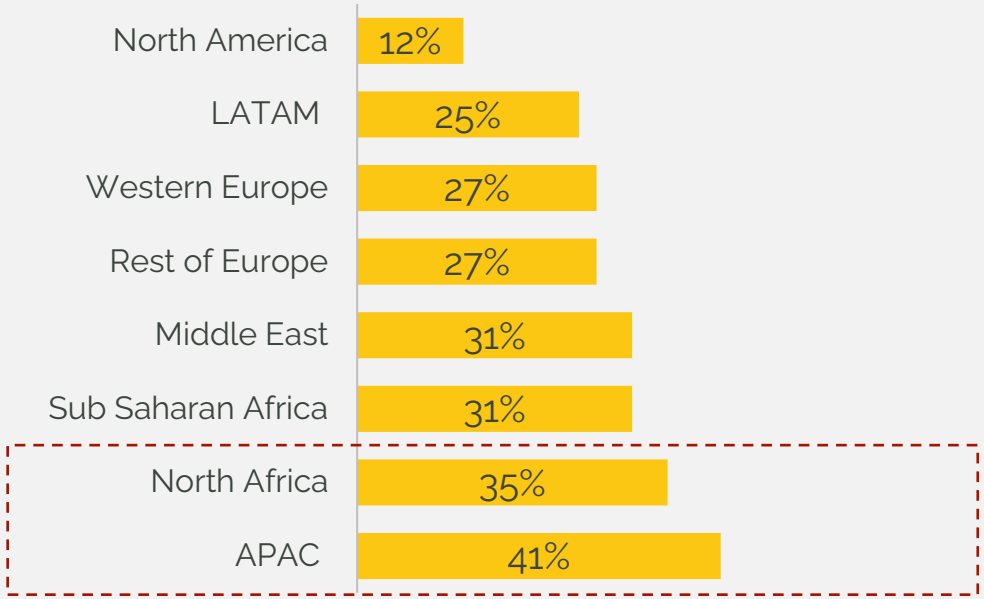
04 Russia

05 Spain

Messaging fraud is no longer confined to one geography, it follows opportunity. Carriers in every region need to raise defences, as fraudsters exploit both weak regulation and high traffic routes

Note: Carriers were asked to name the top two countries with the most fraud by use-case in the survey. The most frequently mentioned countries were then compiled into the final list.
Source: GLF Surveys 2025.

Fig. 35. Respondents who said that they experience a high volume of messaging fraud per region
(% responses)



Messaging fraud shows a more balanced global distribution compared to voice fraud, though certain regions remain more exposed. **APAC and North Africa are reported to have the highest levels of messaging fraud**, reflecting the rapid growth of mobile messaging and vulnerabilities in regional enforcement frameworks.

Sub-Saharan Africa and the Middle East also face elevated risks, with fraudsters exploiting cross-border SMS routing and weak controls on A2P traffic.

04 INTERNATIONAL MESSAGING FRAUD

What are the regulators doing?

How are you seeing regulatory focus change for the different fraud types?

Sender ID and Messaging Regulation

We see a major regulatory shift towards Sender ID vetting and registration (Ireland, India, Singapore)

Regulatory bodies in India, UAE, and EU are tightening enforcement around sender ID spoofing, mandating DLT registration, and penalizing non-compliant traffic

Artificially Inflated Traffic Regulation

Regulators are making every effort to reduce risks linked to traffic inflation and are pushing telecom operators to adopt advanced solutions and best practices

Serious actions were taken in the past year. AIT fraud has dropped dramatically thanks to regulations such as pre-registration for SIDs and content checks

Regional Variability and Gaps

In general, there is no strong regulatory focus on fraud prevention at the EU level; the emphasis remains on reducing costs for end-users

None whatsoever. We lobbied the South African regulator (ICASA) to hold hearings on telecom fraud and received negative feedback. Action has been slow or absent

Source: GLF Survey 2025.

04 INTERNATIONAL MESSAGING FRAUD

Conclusion

01 The actions taken by carriers have gone a long way to reduce SMS fraud however issues such as AIT, smishing and spoofing are persistent threats that need to be continuously monitored. As AI-driven fraud increases, carriers will need to be on their toes to sustain the progress made against messaging fraud

02 Messaging fraud is becoming increasingly concentrated in high-traffic markets with extensive international connectivity. Fraudsters exploit weaknesses across both mature and emerging regions, with activity spanning Europe, South Asia, and beyond. The mix of developed and developing markets in the top list underscores how fraud quickly adapts to regulatory gaps and uneven enforcement worldwide

03 **Carriers are actively working to combat messaging fraud by:**

a. **Targeted measures against AIT and Smishing:** AIT remains the dominant challenge, often disguised through trashing, spoofing, grey routes, and dynamic sender IDs. Carriers are addressing this with stricter monitoring, OTT restrictions, and proactive aggregator controls, which have already helped reduce smishing volumes.

b. **Strengthening monitoring and industry collaboration:** Operators are deploying real-time fraud monitoring tools, AI-enabled SMS firewalls, and anti-spam measures. Improved internal controls, closer collaboration with aggregators, and migration from SMS to RCS have also contributed to reducing fraudulent traffic.

c. **Responding to market and technology shifts:** Fraudsters are exploiting the growth of A2P SMS for authentication and marketing, as well as shifting activity from voice to messaging platforms such as WhatsApp. To counter this, carriers are investing in advanced detection systems, better filtering at origination, and ongoing industry-wide cooperation to adapt to evolving fraud tactics.

Source: GLF Survey 2025

05

UNWANTED TRAFFIC

GLOBAL LEADERS' FORUM GLF™ a techoraco brand

05 UNWANTED TRAFFIC

Introduction

Although unwanted traffic is not formally categorised as fraud, its reputational impact—both real and perceived—has made it a central issue in efforts to rebuild trust in telecom services. This section reviews the current landscape of unwanted traffic on networks, considers its potential long-term consequences for carriers, and explores practical steps the industry can take to address it.

01

The volume of spam, robo calls and phishing is still high, with over 80% of carriers reporting high volumes of spam calls, a 19 p.p. increase from 2024. This is caused by the growing use of automated dialling systems, and low barriers for fraudsters to launch large-scale campaigns across international networks. To address this, carriers are deploying AI-driven call analytics, strengthening caller authentication measures, tightening cross-border cooperation, and educating customers to better recognise and report suspicious calls.

02

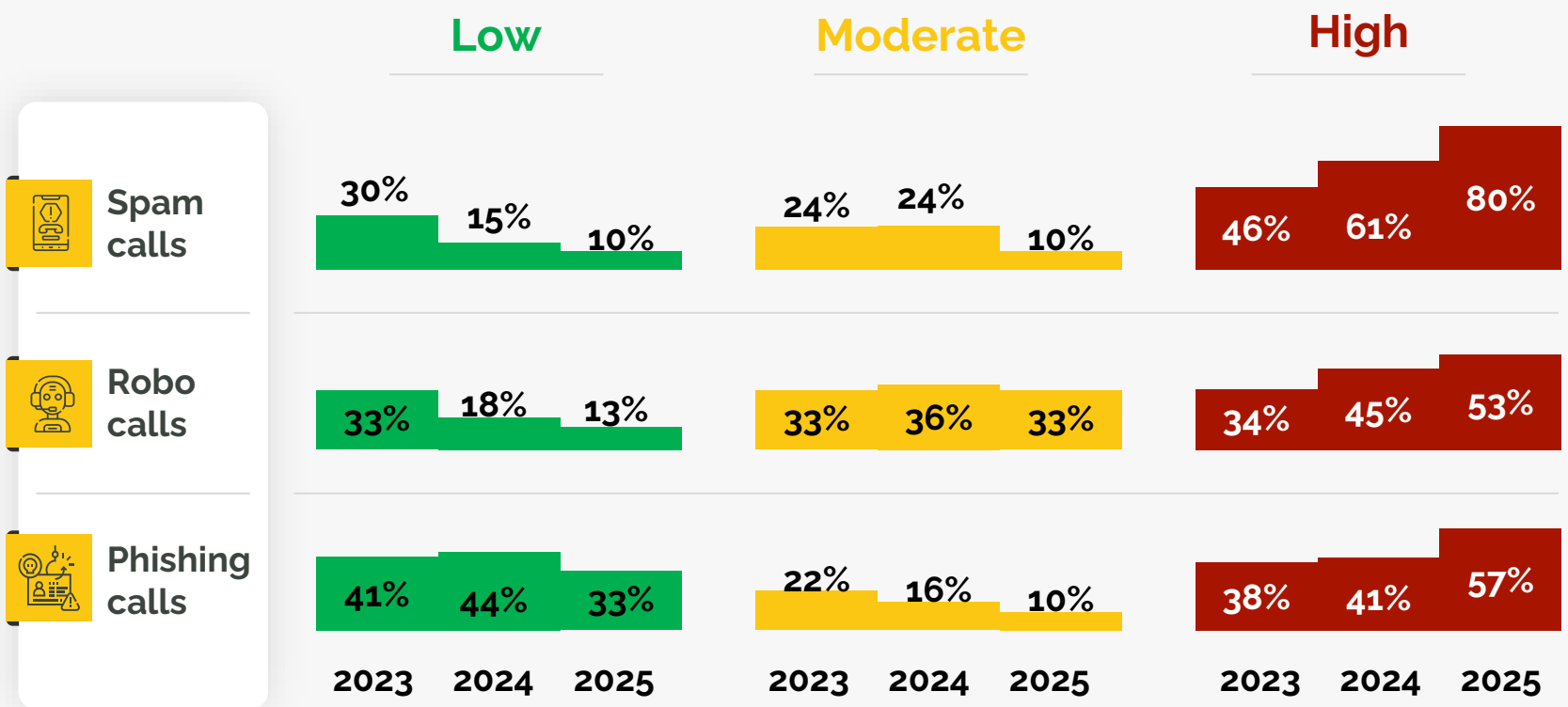
83% of carriers now say unwanted traffic erodes trust — up from 76% last year — driving users toward OTT services and threatening telecom revenues. At the same time, 67% expect tougher regulatory action in response to nuisance calls, though operators warn that excessive regulation could increase costs and compliance burdens, even as fraudsters continue to stay a step ahead of industry defences.

03

Carriers are stepping up efforts to combat unwanted traffic, with 48% taking significant action with growing prioritization and investment. At the same time, customer education is becoming a key focus, as over two-thirds of operators in 2025 report major initiatives to raise awareness of spam and fraud risks. This reflects a maturing industry approach that blends technology, organizational readiness, and consumer engagement to strengthen defences against unwanted traffic.

Nuisance calls volume

Fig. 36. Volume of nuisance calls experienced by the carriers (% responses)



Source: GLF Survey 2025

Nuisance calls remain a growing challenge for carriers, with spam, robocalls, and phishing all showing sharp upward trends.

- **Spam calls** have escalated most dramatically, with the share of carriers reporting high volumes climbing to 80% in 2025, compared to less than half two years earlier
- **Robocalls** also continue to rise, with more than half of carriers now facing high levels
- **Phishing calls**, while starting from a lower base, are also trending upward, with over half of operators reporting high exposure

These results highlight that nuisance calls are no longer a marginal irritation, they represent a core threat to customer trust and service integrity, demanding stronger industry-wide action in detection, blocking, and user education.

Organisational readiness

Fig. 37. Extent of action to reduce unwanted traffic
(% responses)

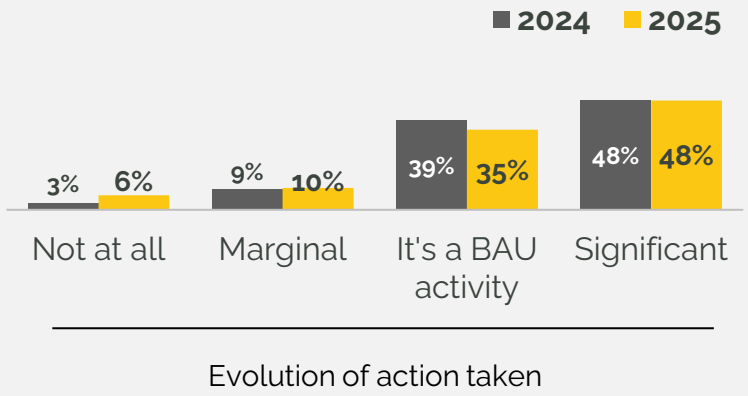
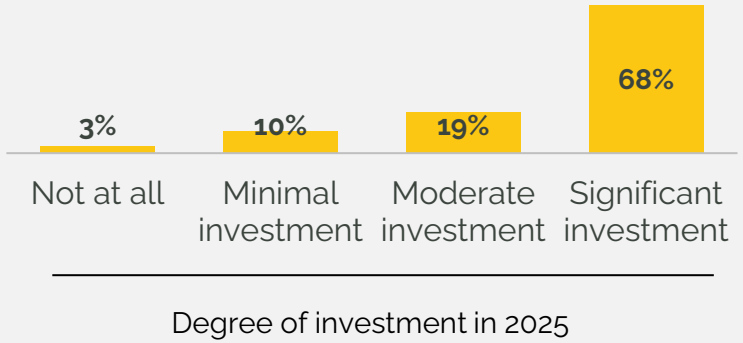


Fig. 38. Extent of investment in customer education
(% responses)

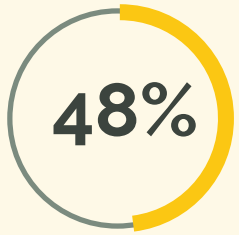


Note: n (2024) = 33; n (2025) = 31;
Source: GLF Survey 2025.

Telecom operators are intensifying their initiatives to tackle unwanted network traffic, as almost 50% indicate they are implementing substantial measures to curb it—consistent with patterns seen in 2024. Although the proportion of providers viewing this as routine operations hasn't changed, the broader sector is shifting toward heightened emphasis and funding.

Educating customers is gaining prominence as a key priority. For 2025, over two-thirds of operators state they are committing major resources to enhance user knowledge of spam and scam dangers. This underscores the understanding that technical solutions by themselves fall short; informed consumers represent a vital safeguard. Collectively, these advancements signal an evolving sector strategy that integrates technological tools, internal preparedness, and user involvement to counter the escalating challenge of undesired traffic.

> *Fraud is not just a technical problem, it requires investment in systems, but also in awareness and collaboration. Without a unified approach, carriers remain one step behind the fraudsters.*



of carriers' state that they are taking significant action to reduce unwanted traffic

Negative effects of unwanted traffic

Fig. 39. Share of carriers who believe that unwanted traffic has negative consequences on the telecom industry, by consequence

(% responses)

Notes: n (2024) = 31, n (2025) = 30; Source: GLF Survey 2025.

Unwanted traffic continues to erode trust in telecom services and increase regulatory risks.

1. In 2025, **83% of carriers report that unwanted traffic reduces trust in telecom operators**, up from 76% the year before. This loss of trust is particularly damaging as it accelerates user migration to OTT services, with 63% highlighting substitution away from traditional carrier messaging and voice.

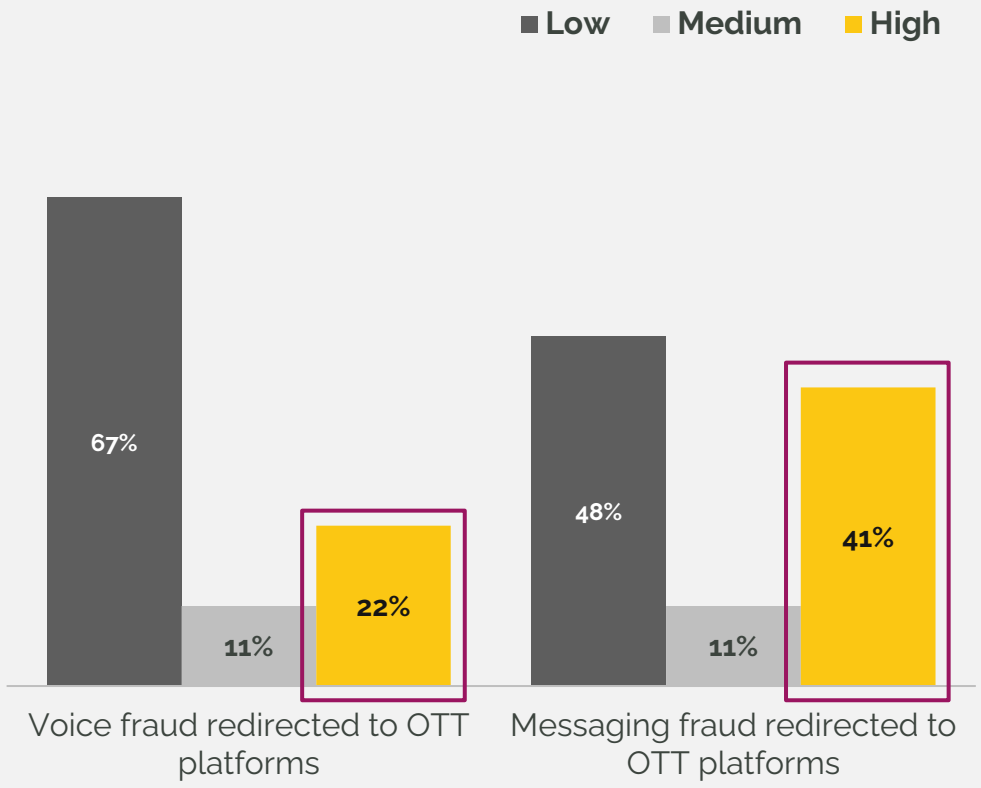
2. The regulatory burden is also intensifying, with **67% respondents anticipating additional regulatory action** as a consequence. Carriers warn that while stricter rules may help combat abuse, they risk raising compliance costs and slowing legitimate traffic.

> *Carriers can block some traffic, but without a unified industry strategy, unwanted traffic will keep undermining the ecosystem*

05 UNWANTED TRAFFIC

Fraudulent traffic originating from OTT platforms

Fig. 40. Volume of fraudulent traffic originating from or redirected to OTT platforms
(% responses)

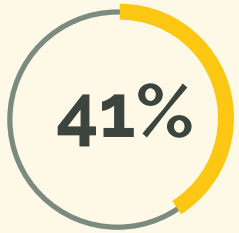


Notes: n(2025) = 27.
Source: GLF Survey 2025.

Over-the-top (OTT) services have become a major hub for fraudulent activity, with carriers noting substantial volumes of messaging scams being channelled through these platforms. For 2025, 41% of operators identified elevated rates of deceptive messaging traffic stemming from OTT sources, whereas OTT-associated voice fraud occurred at more modest levels. This evolution underscores scammers' prowess in taking advantage of OTT systems, which generally feature less stringent supervision and regulatory controls compared to established telecom networks.

Carriers caution that in the absence of enhanced collaboration among carriers, OTT companies, and oversight authorities, scam traffic will keep relocating to unregulated areas, eroding confidence throughout the digital landscape. The key obstacle for the sector lies in creating unified cross-platform guidelines and information-sharing frameworks to prevent OTT pathways from becoming vulnerabilities in international anti-fraud strategies.

> *There are controls built on managing SMS and voice fraud, but none on OTT—and that gap is increasingly being exploited*



of carriers report high volume of fraudulent messaging traffic originating from OTT platforms

05 WHY UNWANTED TRAFFIC IS SO RELEVANT?

What can we do?

What actions should the GLF take to address spam? Should best practices be defined?

Define and Standardise Best Practices

> *GLF should define and promote industry-wide best practices to combat spam—covering sender ID registration, traffic monitoring, and enforcement*

> *Start by developing a clear definition and publishing guidelines. Raise awareness and regularly review and update best practices*

Strengthen Collaboration and Information Sharing

> *Collaboration between partners in the GLF forum will contribute to reducing spam if each partner shares a weekly/monthly blacklist for other carriers to block*

> *GLF should encourage partners to share knowledge regularly, engage in proactive monitoring, and block special codes or ranges*

Invest in Technology and Regulatory Alignment

> *Arrange related campaigns to encourage using voice firewalls, AI-based detection, and regularly updated databases shared with GLF members*

> *Focus on legislative and regulatory changes. Unfortunately, self-regulation is simply not working, and carriers need to be held accountable for poor controls and lack of investment*

Source: GLF Survey 2025.

05 UNWANTED TRAFFIC

Conclusion

01

Spam, robo calls, and phishing remain widespread, with over 80% of carriers reporting high volumes of spam, driven by automated dialling systems and low entry barriers for fraudsters. To counter this, carriers are investing in AI-driven call analytics, stronger authentication, and customer education. Carriers warn that unwanted traffic is eroding trust and pushing users toward OTT services and they anticipate tougher regulations that could raise costs and compliance challenges

02

OTT platforms have become a major source of fraudulent traffic, with 41% of operators in 2025 reporting high levels of messaging fraud through these channels, though voice-related OTT fraud remains lower. Fraudsters exploit weaker monitoring and regulatory oversight in OTT ecosystems compared to traditional telecoms. Carriers warn that without stronger cooperation between telcos, OTT providers, and regulators, fraud will continue to migrate to less controlled environments.

03

Carriers encourage industry forums such as GLF to take a stronger role in combating spam by defining and standardizing best practices, including sender ID registration, traffic monitoring, and enforcement. They also call for greater collaboration and information sharing, such as maintaining shared blacklists, proactive monitoring, and blocking of high-risk codes or ranges. Finally, carriers stress the importance of stronger regulatory alignment and holding operators accountable for poor controls and insufficient investment.

Source GLF Survey 2025.

06

COLLABORATION

GLOBAL LEADERS' FORUM

GLF™

a techoraco brand

06 COLLABORATION

Introduction

Collaboration across the industry is strengthening commitment and driving progress in fraud prevention as carriers acknowledge that unified action, accountability, and shared standards are key to tackling global fraud challenges. Only by working together can carriers strive for a fraud-free environment. This chapter explores current effectiveness and carrier sentiment to collaboration.

01

In 2025, dispute resolution success rates reduced, with a 10 p.p. decrease in carriers reporting more than 40% of disputed amounts were resolved, going from 58% to 48%, and a 3 p.p. drop in cases settled in the 30-40% range, decreasing from 24% to 23%, compared with 2024. Streamlining the dispute resolution process, such as alternatives to the police report requirement, is viewed as key to reversing this trend.

02

This year, significantly more carriers are perceived by their peers as showing a "high commitment" to fraud prevention, with a 17 p.p. improvement from last year. Meanwhile, perceptions of 'same as usual' and 'low commitment' have dropped by 20 points, to 28% and 22% compared to last year. A stronger industry stance, through accountability measures for non-compliant carriers, tougher contractual anti-fraud clauses, and the collective efforts of forums such as GLF and i3forum, has been instrumental in driving this positive shift

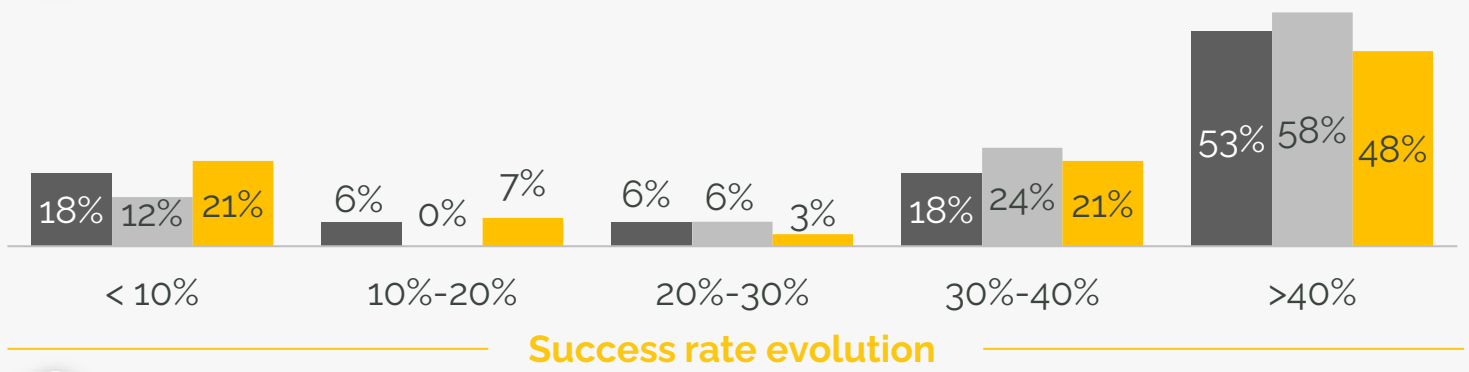
03

To curb fraudulent traffic, operators must go beyond individual efforts and focus on structured, collective action. Industry-wide sharing of anonymised fraud data, early-warning systems, and standardised reporting are critical to staying ahead of emerging threats. Establishing clear response SLAs, holding non-compliant carriers accountable and co-investment in shared fraud detection platforms, particularly to support smaller operators, will ensure a more unified and resilient approach to fraud prevention.

06 COLLABORATION

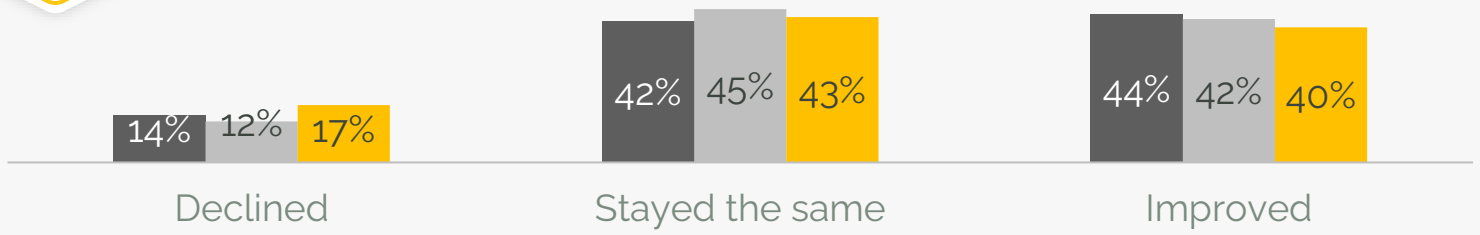
Dispute resolution

Fig. 41. Success rate of dispute resolution
(% responses)



Success rate evolution

Fig. 42. Change in success rate of dispute resolution versus the previous year (% responses)



Change vs. the previous year

Dispute resolution remains a critical element of industry collaboration, with mixed progress reported in 2025. **Nearly half of carriers (48%) report successfully resolving more than 40% of disputed amounts, consistent with previous years. However, there is a drop of 10 p.p.** in the amount of such carriers since 2024.

When comparing year-on-year performance, results are balanced: **around 40–44% of carriers report improvements, while a similar proportion say success rates have stayed the same**. A minority continue to see declines, pointing to uneven progress across the ecosystem.

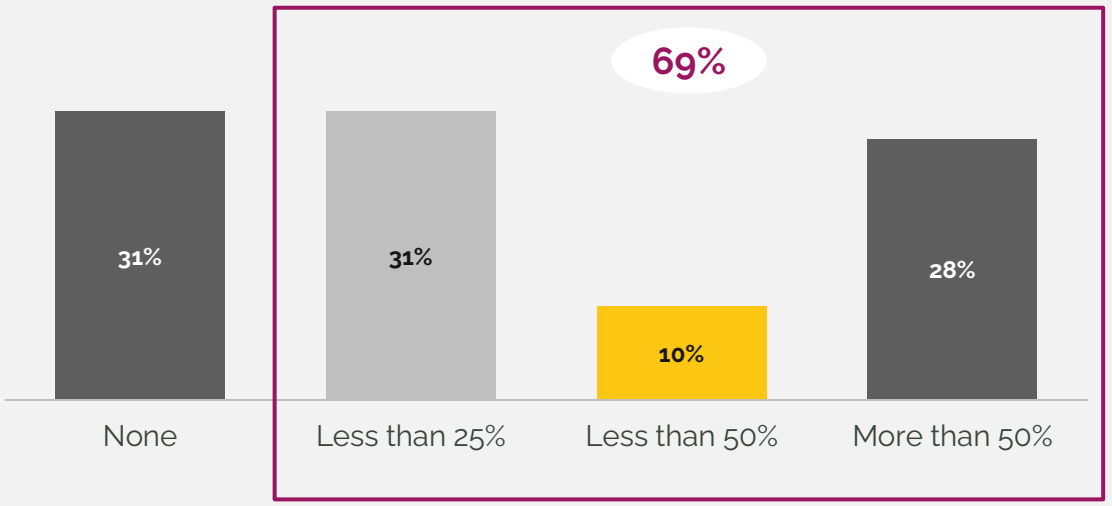
> *Timely response from partners is often missing. Alerts are shared, but the follow-up actions like blocking are delayed, making dispute resolution slow*

48% **of carriers' state that more than 40% of disputes amounts are resolved successfully**

Note: Considering the % success rate = amount of USD/EUR which received a credit note vs. total amount of value disputed.
Source: GLF Survey 2025.

Fig. 43. Percentage of successful recoveries involving GLF Code of Conduct adherents

(% responses)

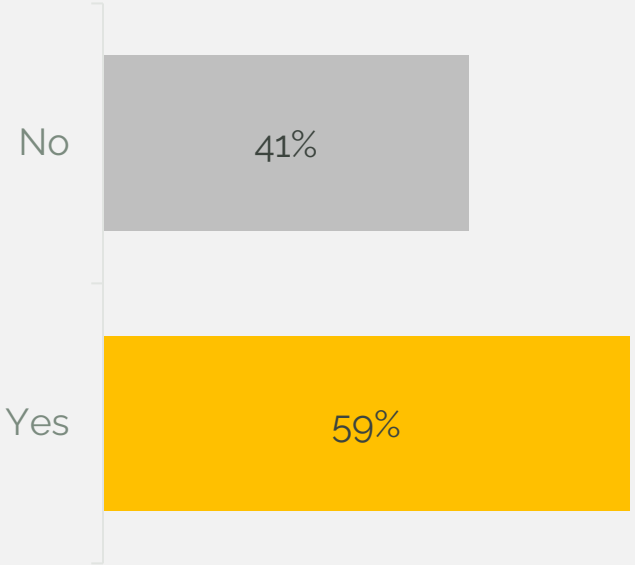


69% of respondents say that successful recoveries from fraud cases involve GLF Code of Conduct adherents, underscoring the value of common standards and accountability.

However, experiences vary: 31% report no recoveries linked to Code signatories, 31% see less than 25% of cases,—highlighting both progress and room for stronger enforcement.

Source: GLF Surveys 2025.

During the dispute process, should some alternative documents or evidences be enough to accept the dispute without having " a police report" in place?



59% of respondents believe that alternative documentation—such as proof from the destination network where the traffic was intended to terminate—should be accepted in place of a police report.

They argue that relying solely on police reports significantly delays the recovery process, hampers timely fraud prevention, and reduces the industry's ability to respond effectively to emerging threats. Accepting operational evidence from carriers could streamline procedures, improve recovery rates, and strengthen collective fraud-fighting efforts.

06 COLLABORATION

What can we do?

What steps should the GLF take next to support the industry in fighting fraud?

Education, Best Practices, and Industry Guidance

> *Continue to provide guidance on best practice, and share knowledge on new fraud types identified*

> *Enhance the Annual Fraud Report with high-quality insights, including analysis on AI-driven fraud, where there is a clear knowledge gap in the community*

Strengthen Collaboration and Information Sharing

> *Develop a central fraud intelligence hub for sharing anonymised incident data.*

> *Host monthly fraud sync calls, standardise global anti-fraud controls, enable real-time threat intelligence sharing, and revoke attestations for carriers who fail to meet standards*

Define and Enforce Standards & Accountability

> *Raise the bar and start taking serious action against carriers breaching the Code of Conduct. Industry should move to zero tolerance for organised crime*

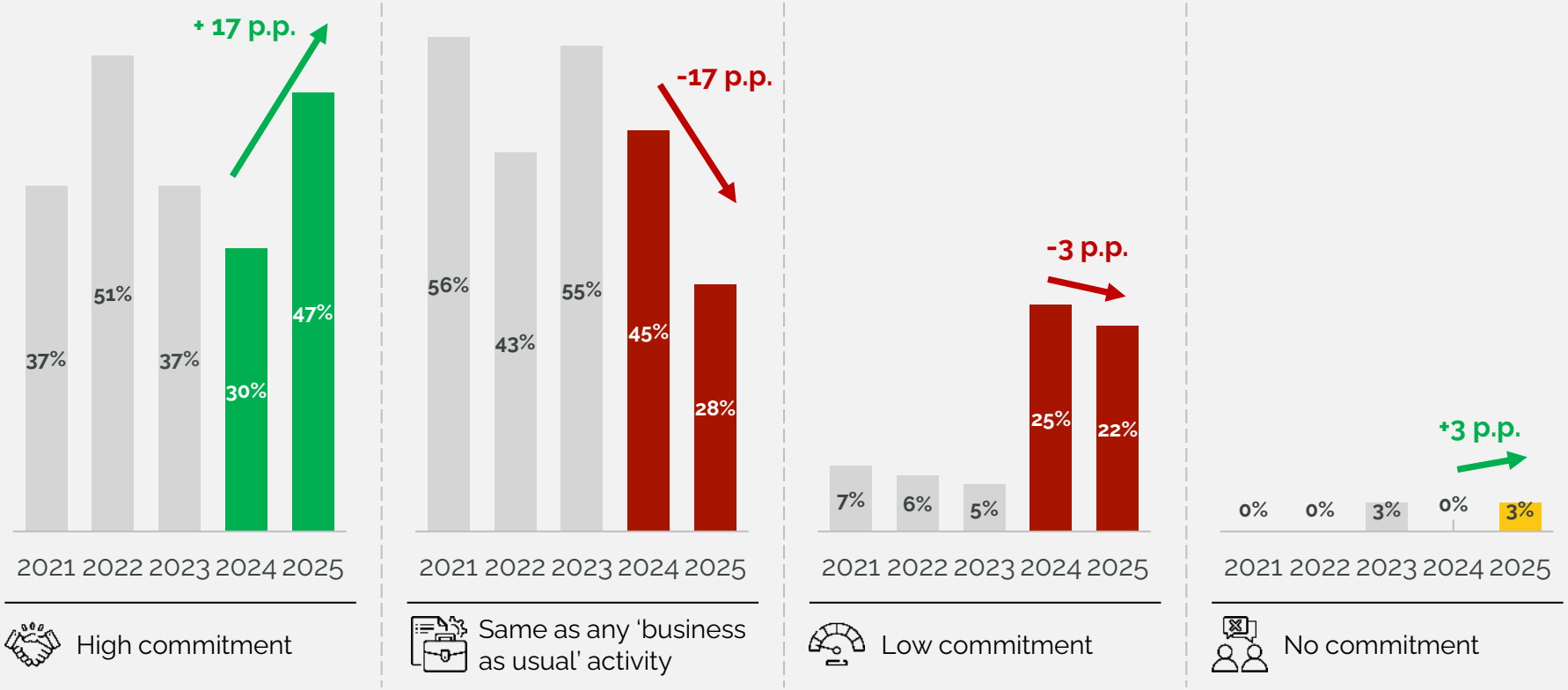
> *Publicly name and shame carriers perpetually involved in fraud, while encouraging partners to share knowledge, proactively monitor & block high-risk ranges & Wangiri traffic*

Source: GLF Survey 2025.

06 COLLABORATION

Level of commitment

Fig. 35. Perception of peer commitment to fighting fraud
(% responses)



Note: Question asked to Carriers: What level of commitment do you believe your peers have to addressing fraudulent traffic?
Source: GLF Surveys 2021, 2022, 2023, 2024, 2025.

Views on the dedication of industry peers to combating fraud are evolving, showing evidence of heightened involvement sector-wide. **For 2025, almost half of carriers (47%) indicate observing substantial levels of commitment from their counterparts**, representing a marked rise over the prior year.

Concurrently, the share of operators regarding fraud prevention as merely "business as usual" has declined notably, indicating that **a larger number are elevating it to a core strategic imperative rather than a standard procedure**. A persistent small segment of carriers continues to note minimal efforts from peers, which emphasises the irregular speed of advancements.

In general, **the findings reflect an increasing acknowledgment that effective fraud mitigation demands true resolve and joint efforts**, with a growing number of operators advancing to back their statements with concrete steps

06 COLLABORATION

Extracts from the conversations with the carriers on collaboration in the industry

How do you currently work with other carriers to combat fraudulent traffic?

We maintain transparent and direct communication with our partners, encourage sender ID registration and scrubbing, and share feedback when suspicious traffic is detected. Our close collaboration ensures proactive handling even before issues arise

We coordinate with others primarily through active participation in industry forums & working groups, including the i3Forum, the GSC Fraud Working Group and the One Consortium. We attend conferences, share expertise & present best practices to be adopted collectively

Following are some of the measures deployed to combat fraudulent traffic: knowledge sharing, proactive monitoring and alerts, blocking of special codes and Wangiri numbers, and anti-SPAM initiatives launched with regulators

What more could be done in terms of collaborative activity to reduce and prevent fraudulent traffic?

Industry-wide sharing of anonymised fraud patterns, joint early-warning systems, and standardised reporting mechanisms would greatly enhance collaboration. A GLF-hosted portal to alert members of emerging threats could also be valuable

Establish a fraud response SLA: define expected response times and actions for fraud alerts exchanged between carriers. Conduct regular audits, share blacklists, and hold non-compliant carriers accountable (including revoking attestations)

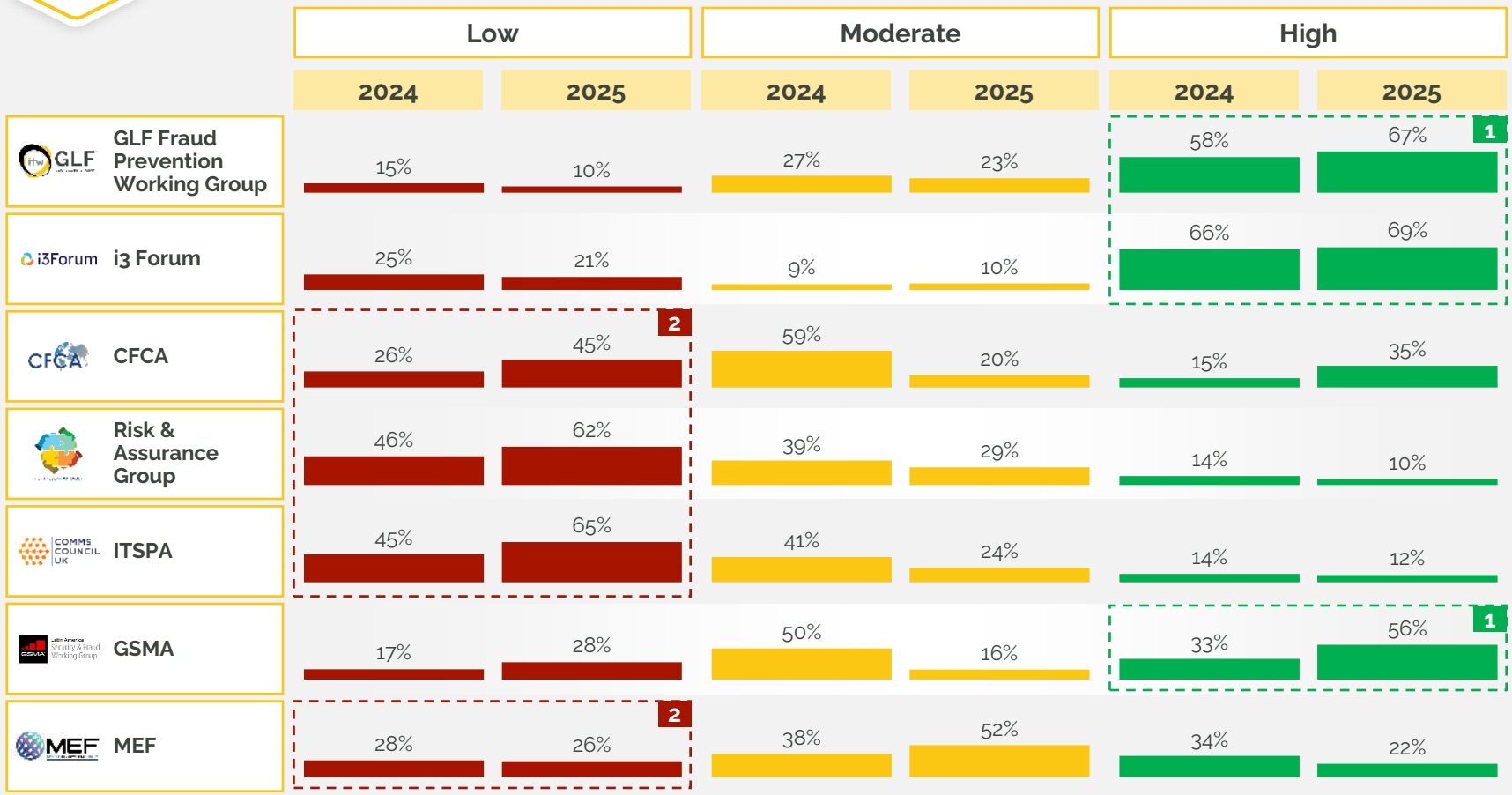
Cross-carrier threat intelligence sharing, joint industry task forces, standardised reporting protocols, regulatory alignment, and shared investment in technology would strengthen fraud prevention. Co-investing in shared fraud detection platforms especially help smaller operators

Source: GLF Survey 2025

04 COLLABORATION

The financial impact from fraudulent messaging traffic, by use case

Fig. 19. Effectiveness of organizations at reducing fraudulent traffic
(% responses)



Notes: n (2024) = 33; n (2025) = 30.
Source: GLF Survey 2025.

1 The GLF Fraud Prevention Working Group and the i3 Forum stand out, with around two-thirds of respondents rating them as highly effective in reducing fraudulent traffic. **GSMA also shows stronger recognition** this year with a growing share of carriers viewing its efforts as impactful.

2 By contrast, all other organizations have received a lower rating, with some showing a swing of around 20p.p. in the share of respondents rating them as having low effectiveness.

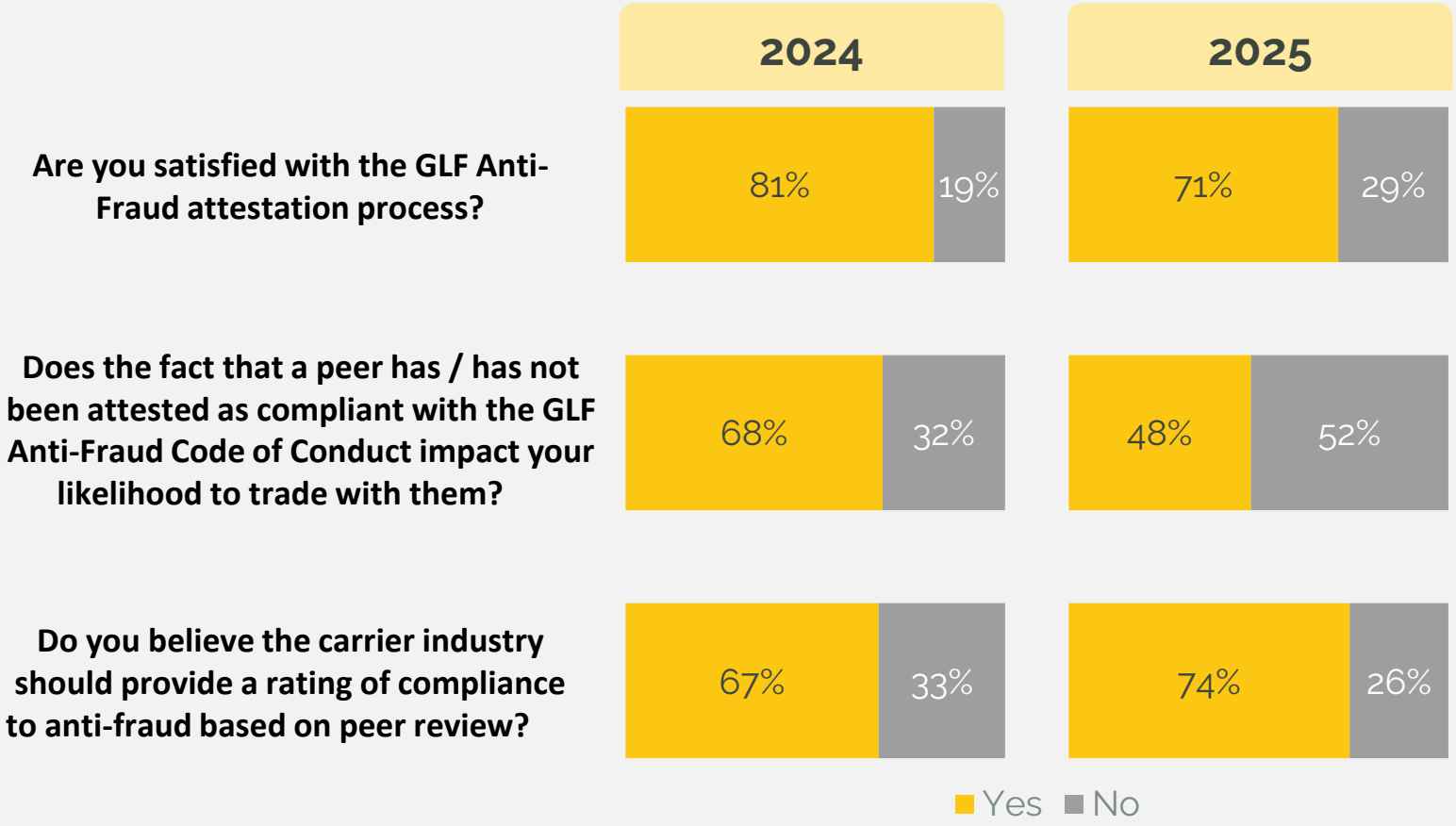
This split highlights that while collaboration is valued, carriers believe only certain forums are driving tangible results, while others need to step up with clearer mandates, stronger coordination, and more tools to address fraud at scale.

> *We need fewer initiatives with stronger mandates to make collaboration truly effective*

06 COLLABORATION

GLF Code of Conduct Attestation

Fig. 36. Questions regarding GLF Code of Conduct (CoC) Attestation
(% responses)



Source: GLF Survey 2025

Carrier sentiment toward the GLF Anti-Fraud Code of Conduct attestation process remains strong in 2025 with **71% of carriers reporting satisfaction with the attestation process**, though the perceived impact of attestation on trading decisions has weakened, only 48% of carriers say a peer's compliance status influences their likelihood to trade, down 20 p.p. This highlights the need to ensure that carriers are held to account for their CoC compliance.

However, **support for peer-driven compliance ratings has strengthened, with nearly three-quarters of carriers endorsing the idea of a peer review mechanism** to promote accountability.

> *Attestation is a good step, but without consequences for non-compliance, it risks becoming a box-ticking exercise*

06 COLLABORATION

Conclusion

01

The growing acknowledgment of carriers' commitment to fraud prevention highlights the substantial progress achieved in collective action over the past year. With fraudsters continually adapting their tactics, coordinated, industry-wide collaboration has never been more vital. Industry forums remain pivotal, with two-thirds of carriers rating GLF's initiatives as highly effective in fostering cooperation and strengthening fraud prevention across the ecosystem.

02

Compliance with the Code of Conduct continues to play a vital role, with nearly half of carriers reporting that it directly influences their trading decisions with peers. This underscores the increasing importance of shared standards as a foundation for building trust, ensuring accountability, and fostering stronger partnerships across the industry.

03

With almost three-quarters of carriers backing a peer-reviewed compliance rating, the industry is placing greater emphasis on trust and transparency. Partnerships are increasingly built around peers that demonstrate robust anti-fraud practices, strengthening the demand for clear, consistent, and accountable compliance standards.

Source GLF Survey 2024.

07

OUTLOOK

GLOBAL LEADERS' FORUM GLF™ a techoraco brand

07 OUTLOOK

Extracts from the conversations with the carriers

What do you see as the biggest challenge in combating fraud in the next 2 years?

Regulatory fragmentation and lack of collaboration

Fragmented global regulations… Evolving fraud typologies… Data sharing limitations… Resource and skills gap are all going to be challenges.

Lack of real-time, cross-carrier intelligence sharing and regulatory inconsistencies across regions will further complicate prevention.

AI-Driven Sophisticated Fraud Techniques

Increasingly sophisticated fraud techniques powered by AI and automation, especially OTP bots, brand spoofing, and global SIM farms.

The biggest challenge will be keeping pace with increasingly sophisticated fraud techniques, including those enabled by AI and deepfake tech.

Economic Incentives & Structural Vulnerabilities

Increasing MTR is an incentive for fraudster. Lack of clear policies and rules adopted by the industry. Arbitrage opportunities with unlimited packages

IRSF on VAS ranges and pulse changes at high-cost destinations leading to induced low-duration traffic and subsequent revenue loss

Source: GLF Survey 2025.

07 OUTLOOK

Extracts from the conversations with the carriers

How is your company preparing for emerging threats?

AI & Advanced Technology Investments

Leveraging AI/ML to enhance accuracy & speed, monitor traffic anomalies, identify smishing/IRSF patterns & support predictive risk assessments

Self-learning ML models for the identification of fraudulent traffic, with more granular blocking capability and the ability to apply varying RVAs

Collaboration, Regulation and Industry Engagement

We monitor regulatory shifts to adapt policies and routing logic proactively. Our team also participates in industry forums to stay informed & aligned

Collaborating with industry partners, including GLF, to share intelligence and best practices and establishing bilateral agreements for faster fraud mitigation

Governance, Processes & Workforce Readiness

Reinforce governance through new policies, regular security awareness training, and stronger workflows between Business, Operations, and Fraud teams

We have been constantly upskilling our internal teams to detect and combat new types of fraud as well as incorporating AI measures

Source: GLF Survey 2024.

07 OUTLOOK

Extracts from the conversations with the carriers

Has your company integrated AI into its fraud detection and prevention systems?

Full AI Implementation in Fraud Detection

> *We use AI and machine learning for real-time fraud detection, leveraging big data, anomaly detection, and near real-time blocking through signalling protocols*

> *Our fraud management system is powered by advanced AI, including machine learning models, anomaly detection, and time-series analysis*

R&D and Continuous Improvement

> *We are modernizing our platform, & AI is a key part of this process. Our SIP firewall is using advanced modelling rulesets with machine learning models of up to 100Bn data points*

> *We have begun incorporating AI tools towards detections and prevention of frauds. This is an in-house system which uses ML and predictive analytics*

Challenges and Mixed Results

> *Until today, results are moderate, but we believe that the coming years will bring better results*

> *No, we have not integrated AI-based systems yet. We are exploring AI-driven solutions such as anomaly detection and predictive analytics*

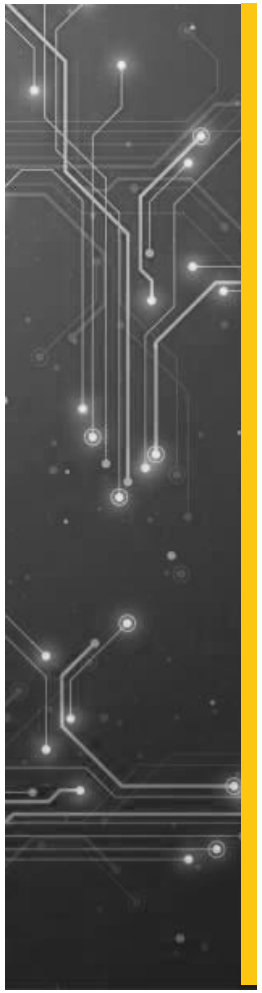
Source: GLF Survey 2024.

PART II

Adhering to the GLF Code of Conduct 2025

01 INTRODUCTION TO CODE OF CONDUCT

What is Code of Conduct and why does it matter?



In 2018, the Global Leaders Forum (GLF) partnered with the i3 Forum to develop a Code of Conduct designed to tackle fraudulent voice traffic. This initiative enabled international carriers to signal their commitment by becoming signatories. By September 2025, a total of 26 carriers have signed on.

By 2020, GLF members realised that mere public endorsement of the Code was not enough; they sought to evaluate actual compliance with its principles. To this end, the 2020 GLF Fraud Report introduced a survey assessing carriers' practices against the Code's six core principles. While carriers received personalised results benchmarked against anonymised, aggregated industry data, no public disclosure of compliant carriers occurred, as it was the inaugural assessment.

In 2021, GLF members opted to publicly list the names of carriers meeting all six principles. During that year's attestation, 19 carriers achieved full compliance, representing 83% of those surveyed. In 2022 and 2023, compliance rates among participants rose to 87% and 88%, respectively. For 2024, a seventh principle was added, addressing revenue share numbers and providing clients with opt-out choices for certain number ranges, with 86% of carriers attaining compliance.

This year, the attestation process incorporated an additional peer review phase. Initiated at the request of the GLF Board, this step aims to foster self-regulation within the industry, allowing carriers to mutually enforce anti-fraud efforts and ensure accountability.

Source GLF Code of Conduct Attestation

01 INTRODUCTION TO CODE OF CONDUCT FOR VOICE

GLF Code of Conduct Principles

PRINCIPLE 1

Targets and Monitoring

Targets for prevention of fraudulent traffic to be included within management reporting

PRINCIPLE 2

Processes

Carriers to adhere to i3 Forum recommended processes to detect and avoid fraud

PRINCIPLE 3

Destinations

Identified fraudulent number ranges and destinations to be blocked

PRINCIPLE 4

Payment flows

All reasonable action to be taken to avoid payment flows to the instigators of fraudulent traffic

PRINCIPLE 5

Reporting

Commitment to share information regarding fraudulent traffic flows with carrier peers

PRINCIPLE 6

Contracting

Adoption of standard contracting terms addressing fraudulent traffic management

PRINCIPLE 7

Revenue Share Numbers

Providing clients with the option to opt-out from specific number ranges

Source GLF Code of Conduct Attestation 2025

01 THREE TIERS OF ATTESTATION

Attestation process

	 "Basic"	 "Advanced"	 "Excellent"
Purpose	Engage carriers that currently lack the resources to invest in fraud control but are open to accepting fraud disputes	Provide an industry standard for the expected carrier actions against anti-fraud	Provide a communicated industry "gold standard" for carriers that are the benchmark for anti-fraud
Mechanism	Adherence to Principles 4 and Principles 6 of the Code of Conduct	Current attestation process with bar of 85% for compliance	Current attestation process with bar above 85% plus passing peer review process

01 INTRODUCTION TO THE CODE OF CONDUCT

Attestation process

THIS YEAR, THE GLF HAS REPEATED ITS ATTESTATION PROCESS, USING A CONSISTENT METHODOLOGY SINCE 2022. THE PROCESS FOR THE CODE OF CONDUCT ATTESTATION HAS FIVE STEPS

1. Carriers complete a 26-question, multiple-choice attestation survey asking about the level to which they are acting in accordance with each principle in the Code of Conduct
2. Carriers submit documents of evidence demonstrating adherence to each of the seven principles
3. GLF reviews the attestation survey responses and provides an initial score/result. Evidence is reviewed and judged either as 'passing' the attestation or requiring 'more information to be provided'
4. GLF has a call with the carrier to communicate the initial score and identify if there are any areas where questions were misunderstood or more data needs to be provided
5. Carriers have an opportunity to provide a written request supported by data to amend an attestation survey answer only if it was previously answered based on a misunderstanding, or to provide additional evidence

TO BE 'COMPLIANT', A CARRIER MUST:

1. Score over 85% in each of the seven principles within the attestation
2. Provide evidence which the GLF team views as satisfactory to demonstrate adherence

Source: Code of Conduct Attestations 2022, 2023, 2024, 2025.

01 INTRODUCTION TO THE PEER REVIEW

Peer Review Questionnaire

01	**Does this carrier systematically / consistently as standard business practice reject disputes with no intention to process or support the disputed issue?**
02	**Do you believe that the carrier, as a standard course of business, adheres to CoC Principle 4 - that all reasonable action is take to avoid payment flows to the instigators of traffic?**
03	**Do you believe that the carrier, as a standard course of business, adheres to CoC Principle 5 - commitment to share information regarding fraudulent traffic flows with carrier peers?**
04	**Do you believe that the carrier, as a standard course of business, adheres to CoC Principle 6 - adoption of standard contracting terms addressing fraudulent traffic management?**
05	**If you responded 'no' in the questions above, please provide information to assert why the carrier is not compliant with the Code of Conduct**

TO BE 'COMPLIANT', A CARRIER MUST:

1. Receive at reviews from at least six carriers
2. Have at least four responses or >60% of respondents (whichever is greater) scoring 80% or higher in their review

Source: Code of Conduct Attestations 2022, 2023, 2024, 2025.

List of compliant carriers for 2025

THE FOLLOWING 21 CARRIERS HAVE ATTESTED AS COMPLIANT FOR THE CODE OF CONDUCT FOR VOICE

‘Excellent’

A1 Telekom Austria Group
airtel
bayobab
bics
BTS
CIMA GROUP
colt
T
e&
iBASIS
IDT global
LANCK TELECOM
orange
PCCW Global
SPARKLE
TATA COMMUNICATIONS
Telefónica Global Solutions
Telin
vodafone

‘Advanced’

stc

02 ANALYSIS OF THE ATTESTATION DATA

Principle 1 – Targets and Monitoring

Fig. 1. Distribution of carrier compliance to Principle 1

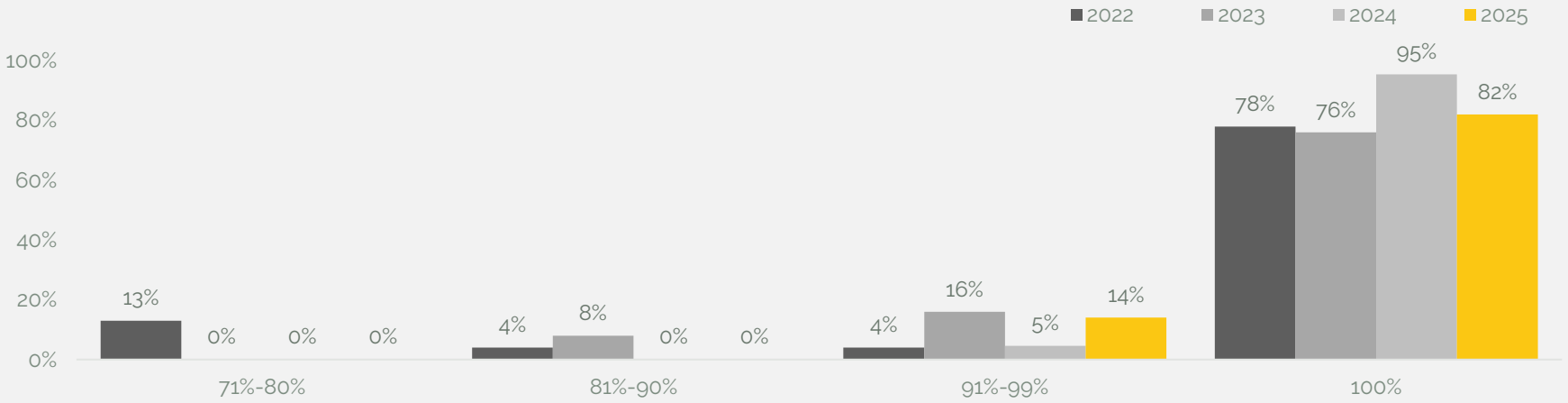
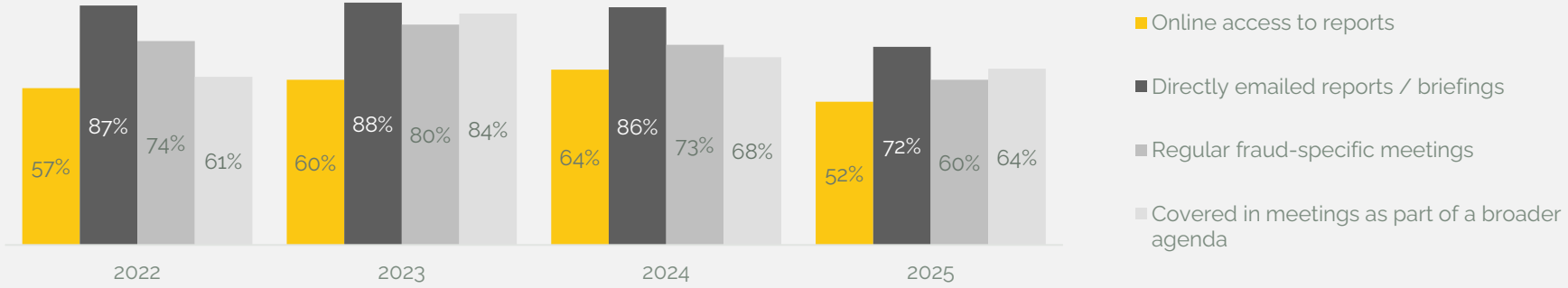


Fig. 2. Share of carriers who provide the most senior executives with updates on fraud, by means of information sharing



Notes: Omitted no responses; n (2022) = 23, n (2023) = 25, n (2024) = 22, n (2025) = 22.
Source: GLF Code of Conduct Attestations 2022, 2023, 2024 and 2025.

Targets for prevention of fraudulent traffic to be included within management reporting

In 2025, carrier compliance with Principle 1 remained strong, with 82% of carriers scoring 100%. While this marks a decline from the record 95% in 2024, it still underscores fraud prevention as a top management priority within most organisations.

In 2025, 72% of carriers continue to provide direct email briefings on fraud to senior executives, slightly down from 86% in 2024, but consistent with a multi-year trend of prioritising fraud at the leadership level. Online access to reports has stabilised at 52%.

Meanwhile, 60% of carriers now rely on regular fraud-specific meetings, a further decrease from 73% last year, suggesting a continued shift toward more streamlined, report-driven oversight rather than dedicated discussions.

02 ANALYSIS OF THE ATTESTATION DATA

Principle 2 – Processes

Fig. 3. Distribution of carrier compliance to Principle 2

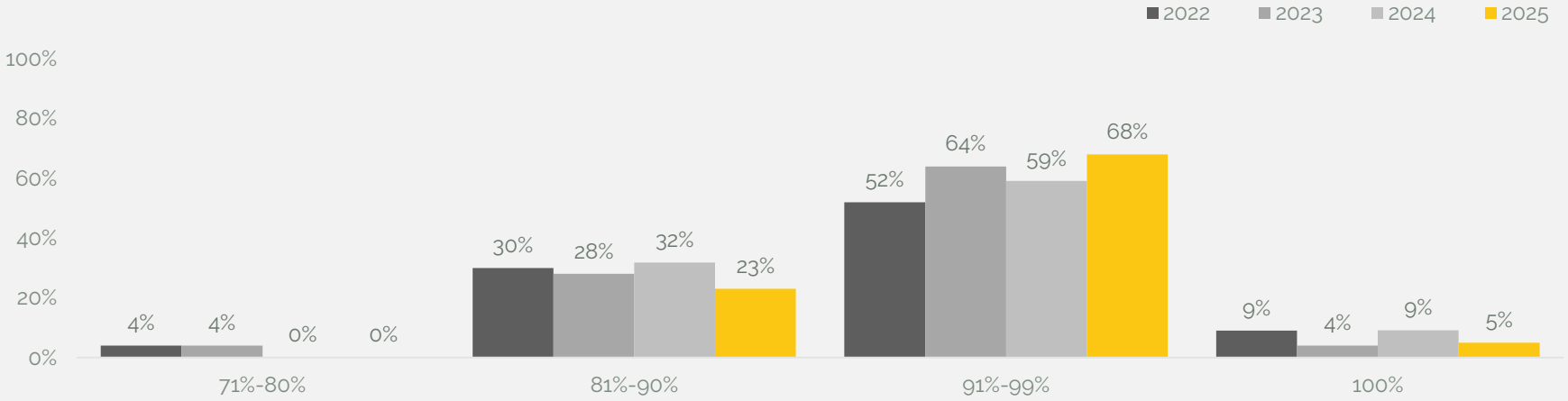
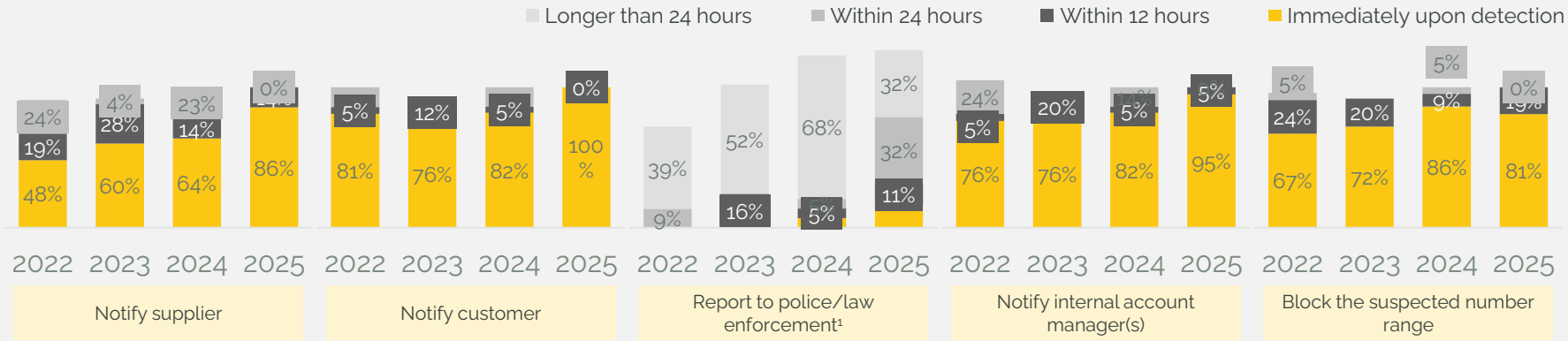


Fig. 4. Presence and speed of fraud processes (2022 – 2025)



Notes: Omitted no responses; n (2022) = 23, n (2023) = 25, n (2024) = 22, n (2025) = 22;. 1. Does not include the answer "Never"
Source: GLF Code of Conduct Attestations 2022, 2023, 2024 and 2025.

Carriers to adhere to i3 Forum recommended processes to detect and avoid fraud

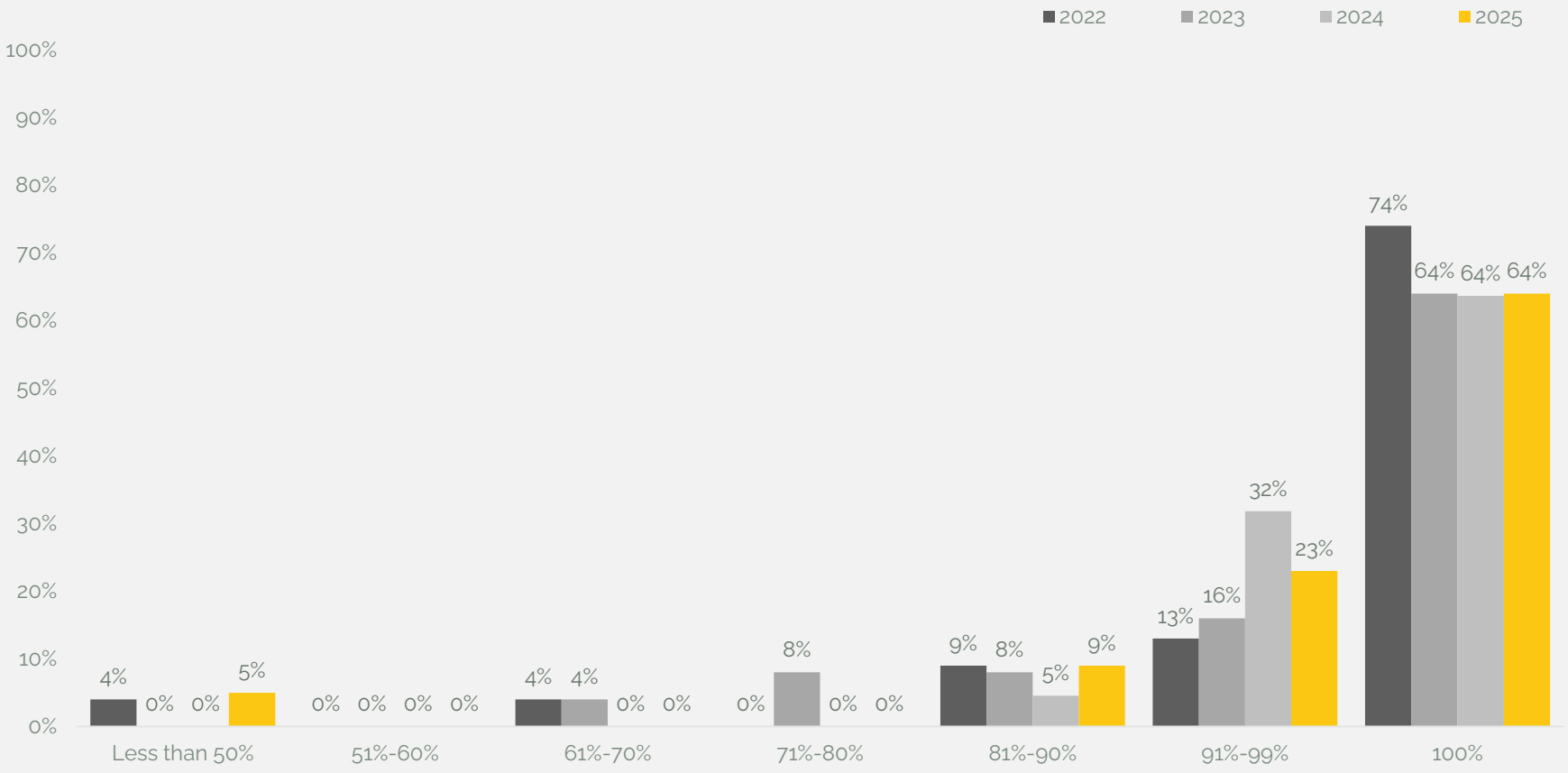
In 2025, all participating carriers remained compliant with this principle. Additionally, 5% of carriers achieved 100% compliance with Principle 2, down slightly from 9% in 2024. Meanwhile, 68% of carriers scored between 91% and 99%, an improvement from 59% last year, reflecting steady progress.

Carriers have further accelerated their response to suspected fraudulent traffic, with marked improvements in speed across key processes. Immediate notifications to suppliers and customers both reached 100%. These results show the growing impact of automation and real-time detection systems in enabling quicker, more coordinated fraud responses.

02 ANALYSIS OF THE ATTESTATION DATA

Principle 3 – Destinations

Fig. 5. Distribution of carrier compliance to Principle 3



Notes: Omitted no responses; n (2022) = 23, n (2023) = 25, n (2024) = 22, n (2025) = 22.
Source: GLF Code of Conduct Attestations 2022, 2023, 2024 and 2025.

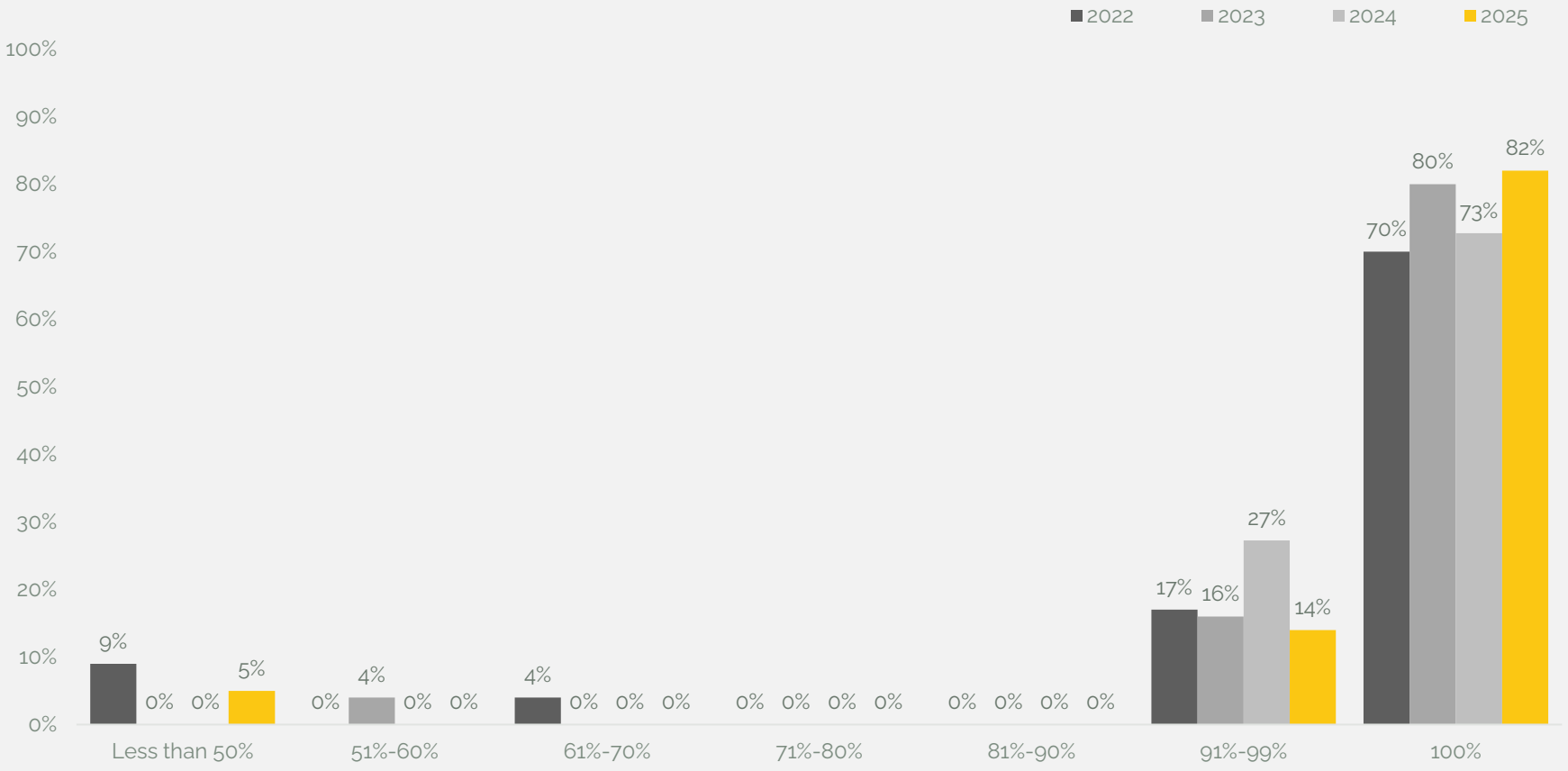
Identified fraudulent number ranges and destinations to be blocked

In 2025, all but one carriers complied with this principle, maintaining the strong performance achieved in 2024. However, 64% of carriers achieved full (100%) compliance, equalling 2024 results, as operators adopt more targeted approaches to blocking fraudulent traffic. Increasingly, compromised A-numbers are being restricted only for affected customers, ensuring that legitimate traffic is not unnecessarily disrupted.

On the positive side, compliance within the 91%–99% range declined to 23%, compared to 32% in 2024. This downward shift indicates that fewer carriers are reaching perfect compliance and demonstrating consistently high standards, reflecting a slight decline in progress in adopting best practices and strengthening fraud prevention measures across the industry.

Principle 4 – Payment flows

Fig. 6. Distribution of carrier compliance to Principle 4



Notes: Omitted no responses; n (2022) = 23, n (2023) = 25, n (2024) = 22, n (2025) = 22.
Source: GLF Code of Conduct Attestations 2022, 2023, 2024 and 2025.

All reasonable action to be taken to avoid payment flows to the instigators of fraudulent traffic

In 2025, 82% of carriers achieved full compliance with Principle 4, marking a strong improvement from 73% in 2024. This reflects growing industry commitment to applying i3 Forum payment flow processes consistently to block fraudulent actors and prevent revenue leakage.

At the same time, 14% of carriers scored within the 91%–99% range, a decline from 27% in 2024, as more operators moved into full compliance. This shift underscores increasing alignment with i3 Forum standards, though continued vigilance is needed to ensure uniform application across all cases.

02 ANALYSIS OF THE ATTESTATION DATA

Principle 5 – Reporting

Fig. 7. Distribution of carrier compliance to Principle 5

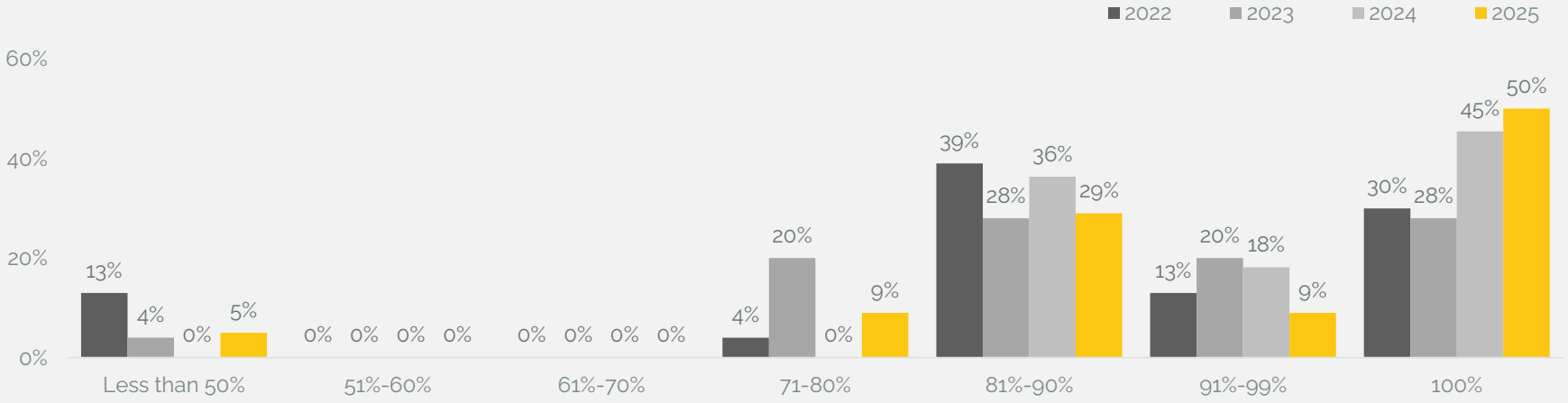
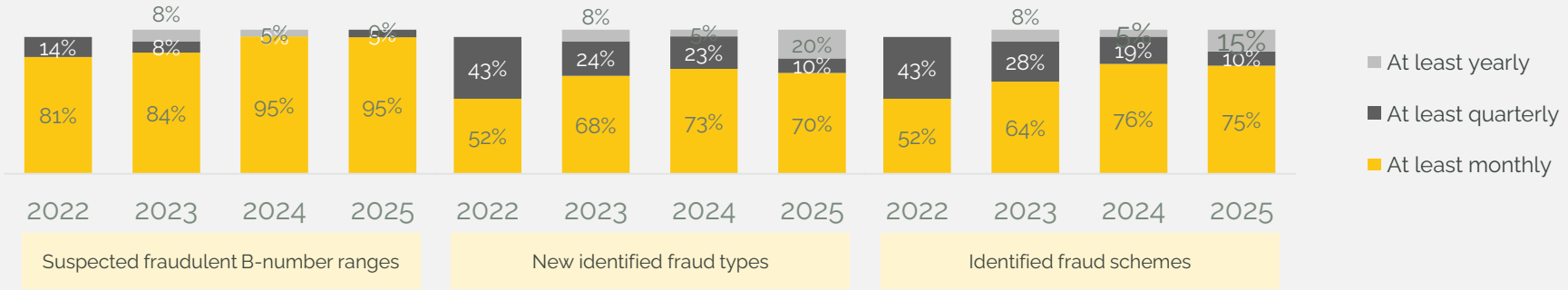


Fig. 8. Presence and speed of fraud processes (2022 – 2025)



Notes: Omitted no responses; n (2022) = 23, n (2023) = 25, n (2024) = 22, n (2025) = 22.
Source: GLF Code of Conduct Attestations 2022, 2023, 2024 and 2025.

Commitment to sharing information regarding fraudulent traffic flows with carrier peers

In 2025, carriers strengthened their commitment to sharing information on fraudulent traffic flows, with 50% achieving full compliance with Principle 5, up from 45% in 2024. This reflects continued investment in automated and standardised reporting systems that enhance consistency and coverage.

The frequency of reporting also improved, with 95% of carriers now updating suspected fraudulent B-number ranges monthly, while reporting on identified fraud types and schemes also became more consistent. These gains highlight the industry's move toward real-time, automated sharing practices that ensure faster detection and coordinated responses across the ecosystem.

02 ANALYSIS OF THE ATTESTATION DATA

Principle 6 – Contracting

Fig. 9. Distribution of carrier compliance to Principle 6

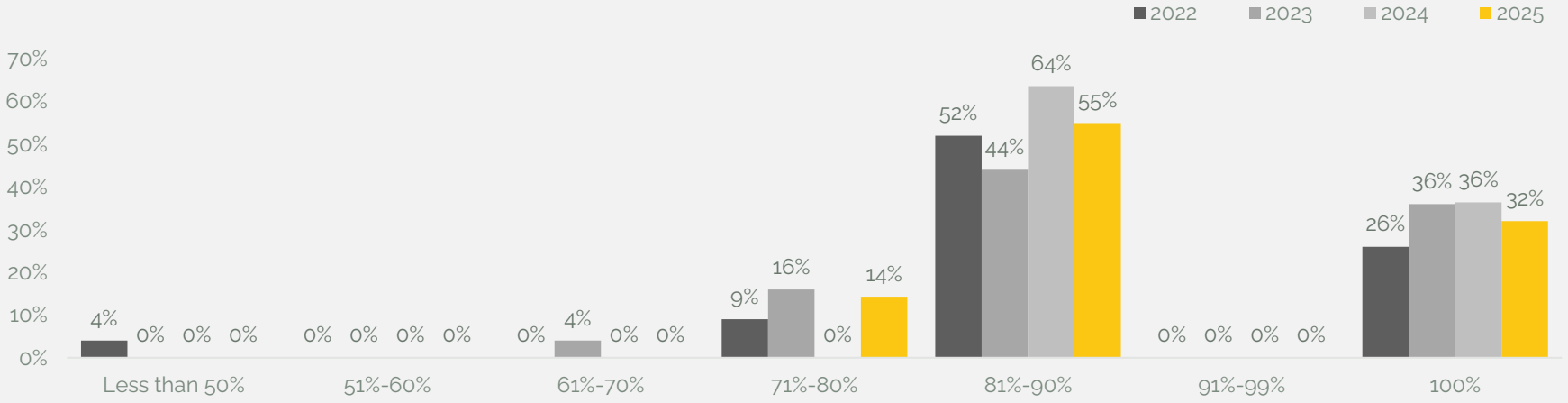
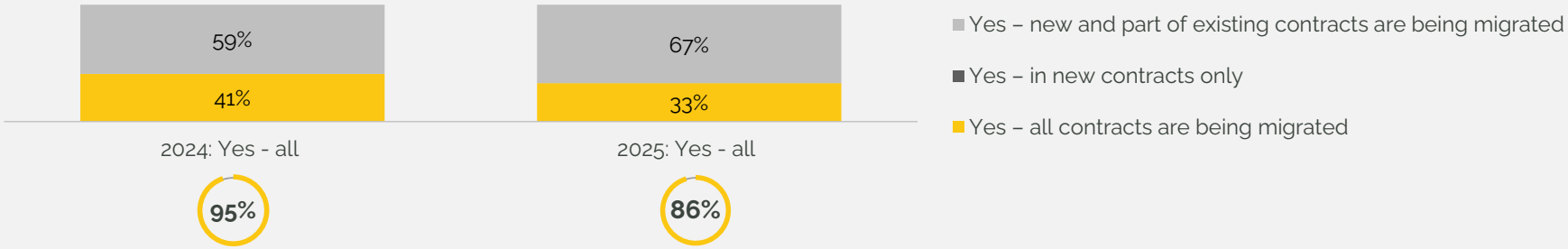


Fig. 10. Consistency of fraud clause contract adoption 2025 vs 2024



Notes: Omitted no responses; n (2022) = 23, n (2023) = 25, n (2024) = 22, n (2025) = 22.
Source: GLF Code of Conduct Attestations 2022, 2023, 2024 and 2025.

Adoption of standard contracting terms addressing fraudulent traffic management

The share of carriers at 100% compliance with Principle 6 is 32% (down from 36% in 2024). Most carriers now sit in the 81–90% band at 55% (vs. 64% in 2024), while 14% are in 71–80% (up from 0% last year). This points to solid adoption overall, with some slippage as operators work through legacy contracts and enforcement.

The proportion of carriers confirming anti-fraud clauses in all customer contracts fell to 86% in 2025 (from 95% in 2024). At the same time, 67% report clauses are present in new contracts and are still migrating across existing agreements (vs. 59% last year), indicating progress is ongoing but not yet complete.

02 ANALYSIS OF THE ATTESTATION DATA

Principle 7 – Revenue Share Numbers

Fig. 11. Distribution of carrier compliance to Principle 7

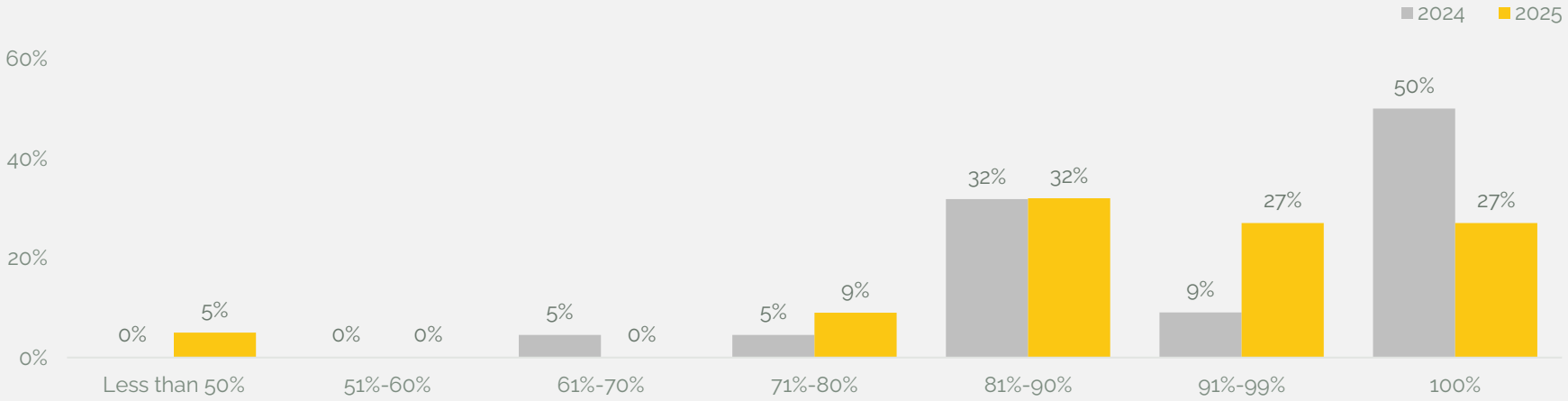
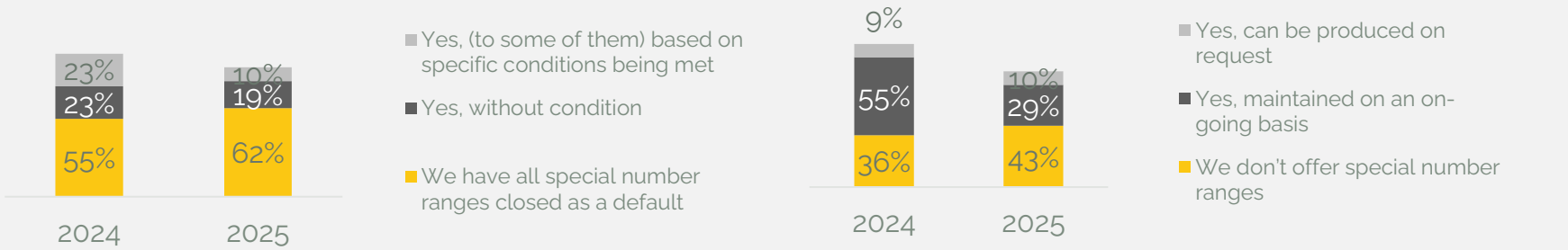


Fig. 12. Special number ranges opt-out and rate sheets



Do you provide customers the option to opt-out from special number ranges?

Do you provide a specific rate sheet that lists special number ranges for special services?

Notes: n (2024) = 22, n (2025) = 22
Source Code of Conduct Attestation 2025

Commitment to provide clients with the option to opt-out from specific revenue share number ranges

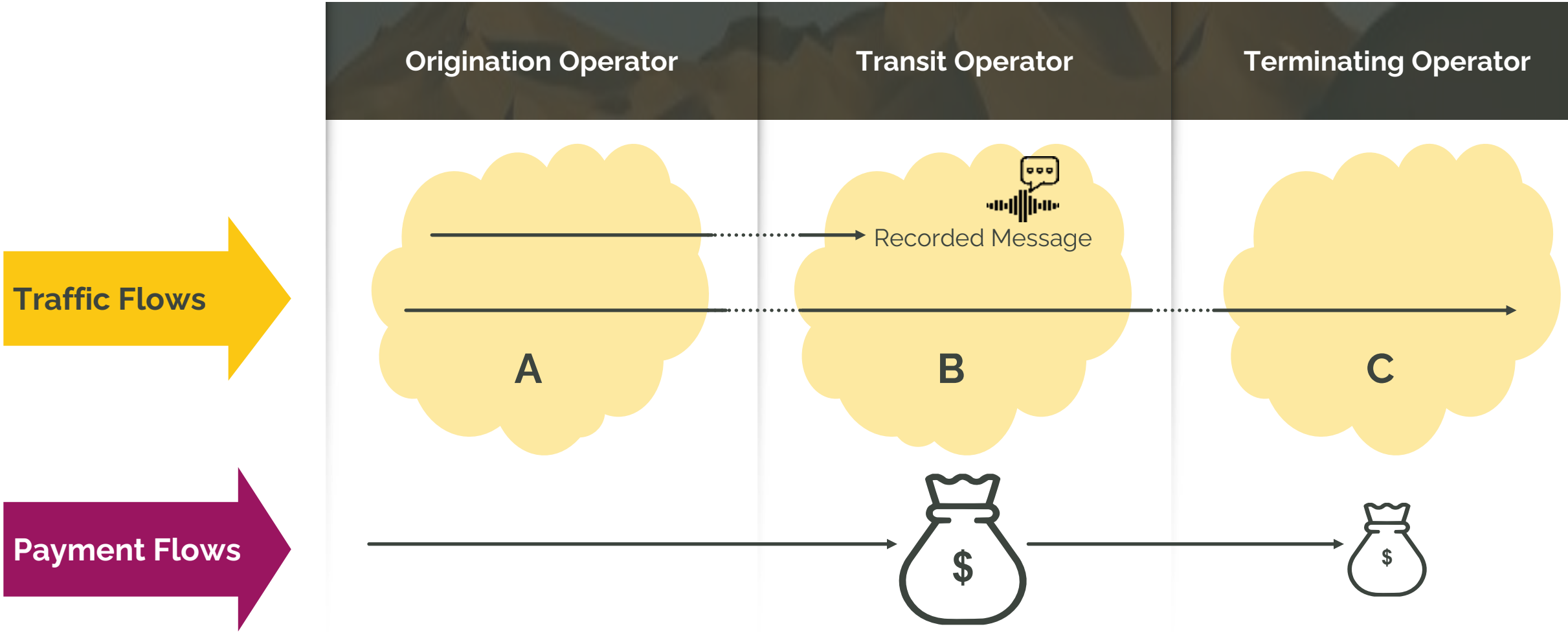
In 2025, compliance with Principle 7 remained strong, though the share of carriers at 100% compliance dropped to 27% (from 50% in 2024). Most carriers are now clustered in the 81–99% range (59%), showing that while adoption is broad, some gaps remain in execution.

On special number ranges, 62% of carriers now close all ranges by default (up from 55% in 2024), strengthening fraud prevention and customer protection. Regarding rate sheets, 43% maintain special number ranges on an ongoing basis, while 29% provide them only on request. Encouragingly, 10% no longer offer them at all, limiting exposure to revenue share fraud.

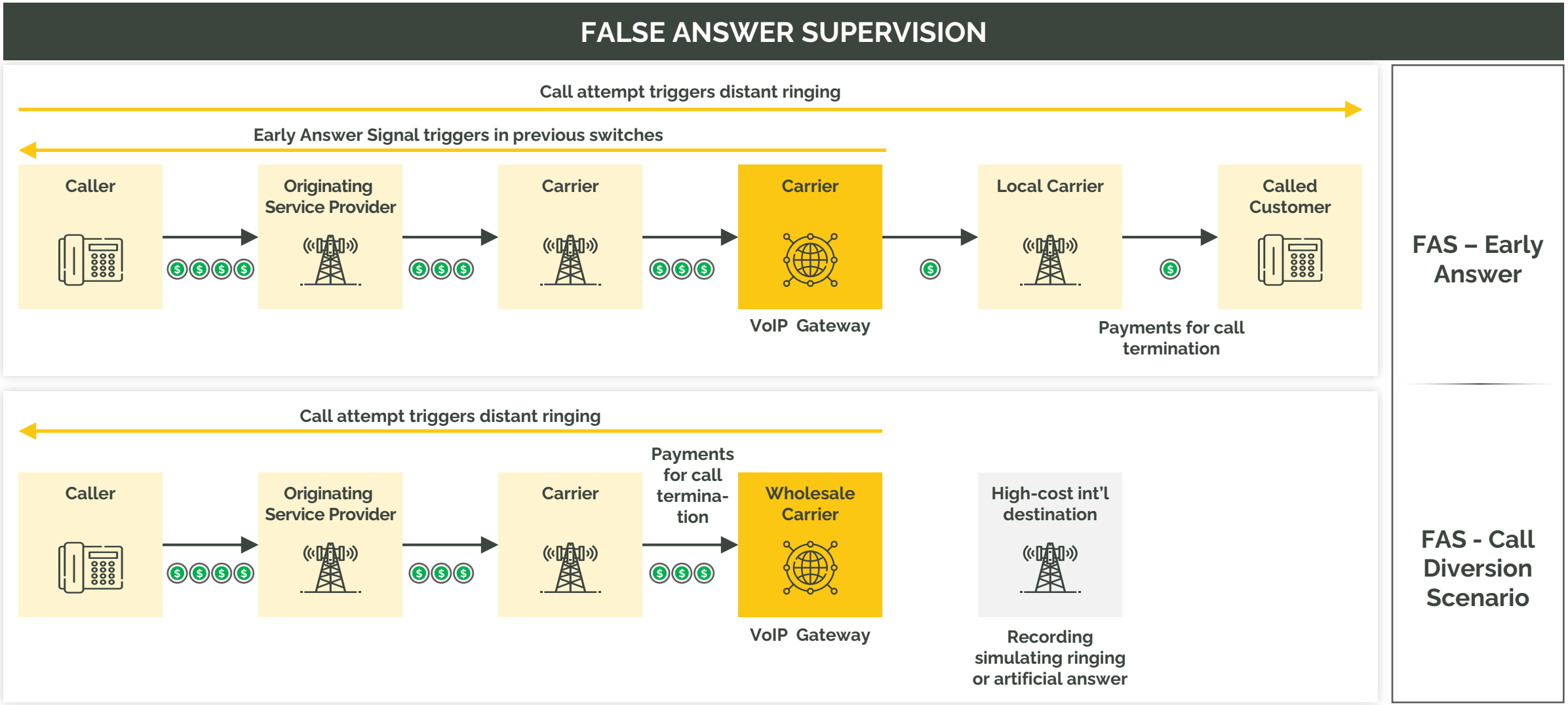
Appendix

Fraud Mechanisms - VOICE

A. Call Hijacking



B. False Answer Supervision



C. International Revenue Share Fraud

1 The criminals acquire numbers from international Premium Rate Number (PRN) providers

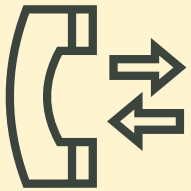
Acquire number

2 The criminals generate a high volume of international calls to those numbers, for instance, using botnets, servers running stolen M cards, or the Wangiri scam

Generate traffic

3 The fraudulent calls may pass through 7 operators to get to their termination point

Calls pass through



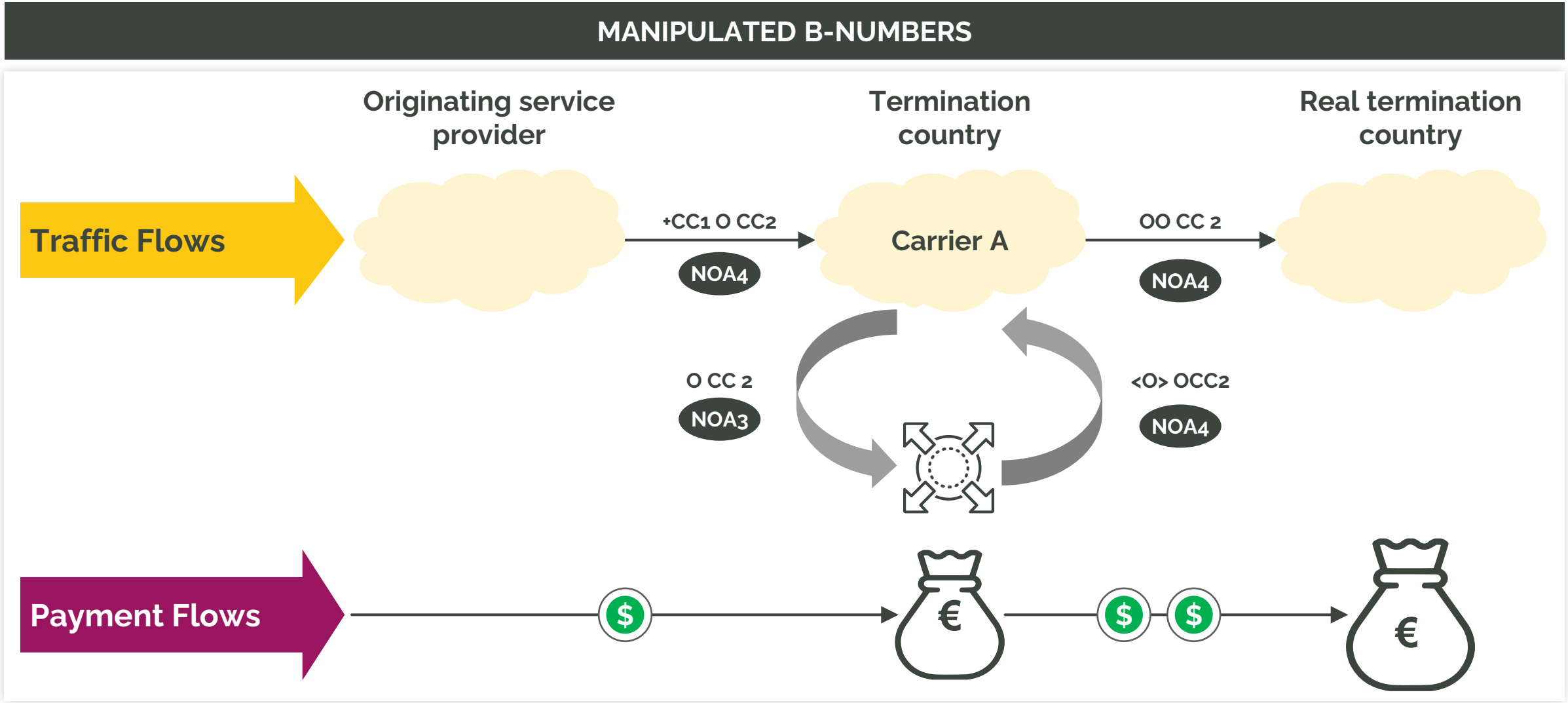
4 Eventually, the telecom operations will block the calls to the premium-rate number

Operators block calls

5 The IPRN providers share the revenue with the criminal

Revenue is shared

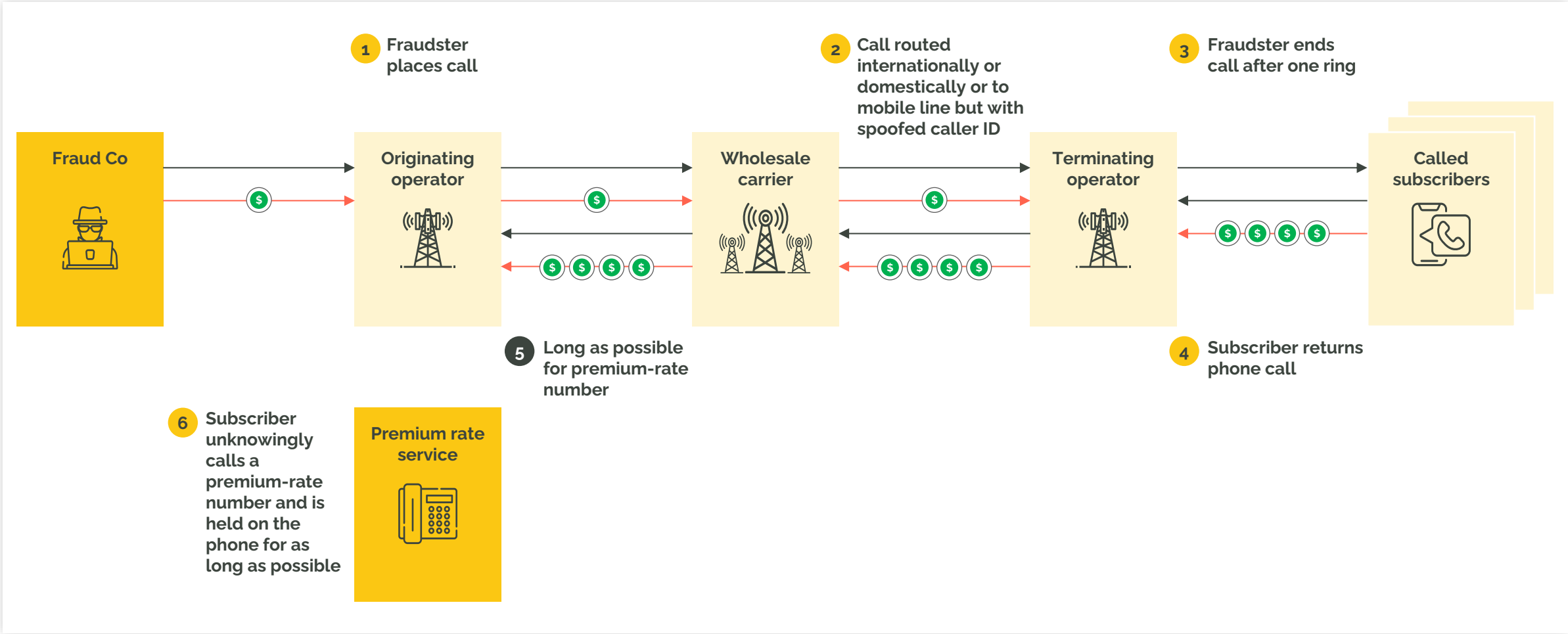
D. Calls to manipulated B-numbers



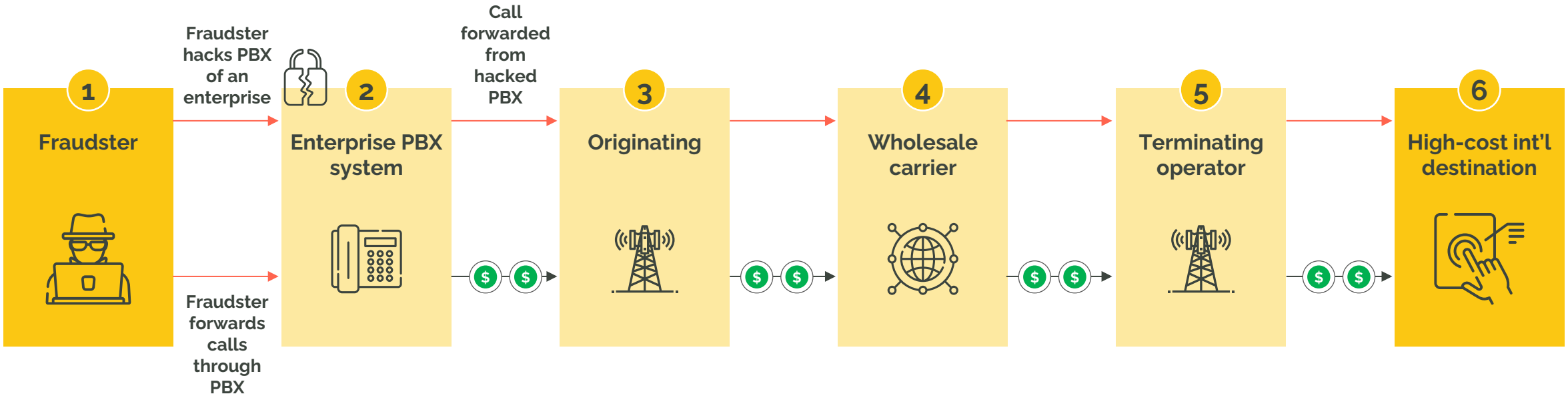
Source: https://i3forum.org/wp-content/uploads/2023/05/Fraud_Classification_v4.0.pdf

E. Missed Call Campaigns / Wangiri Fraud

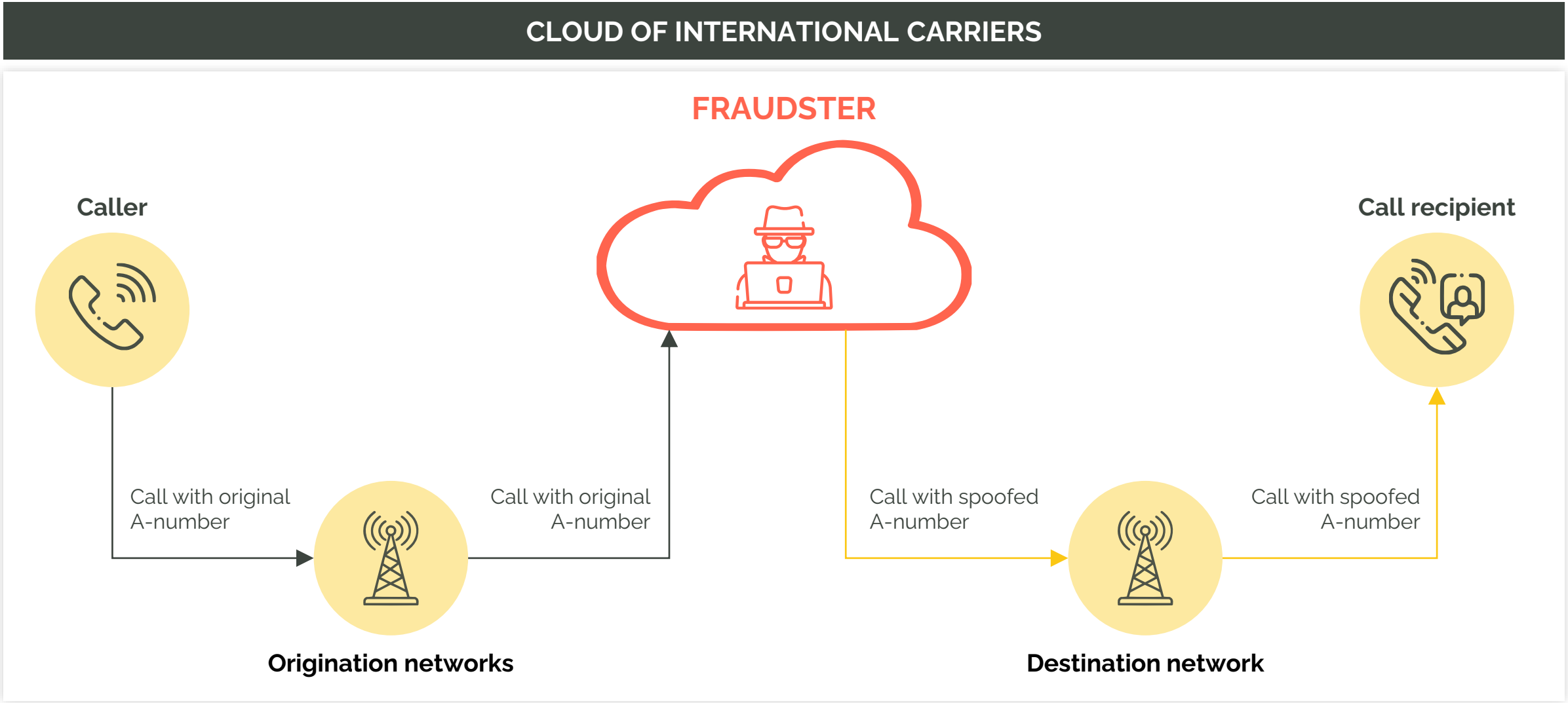
MISSED CALL CAMPAIGNS



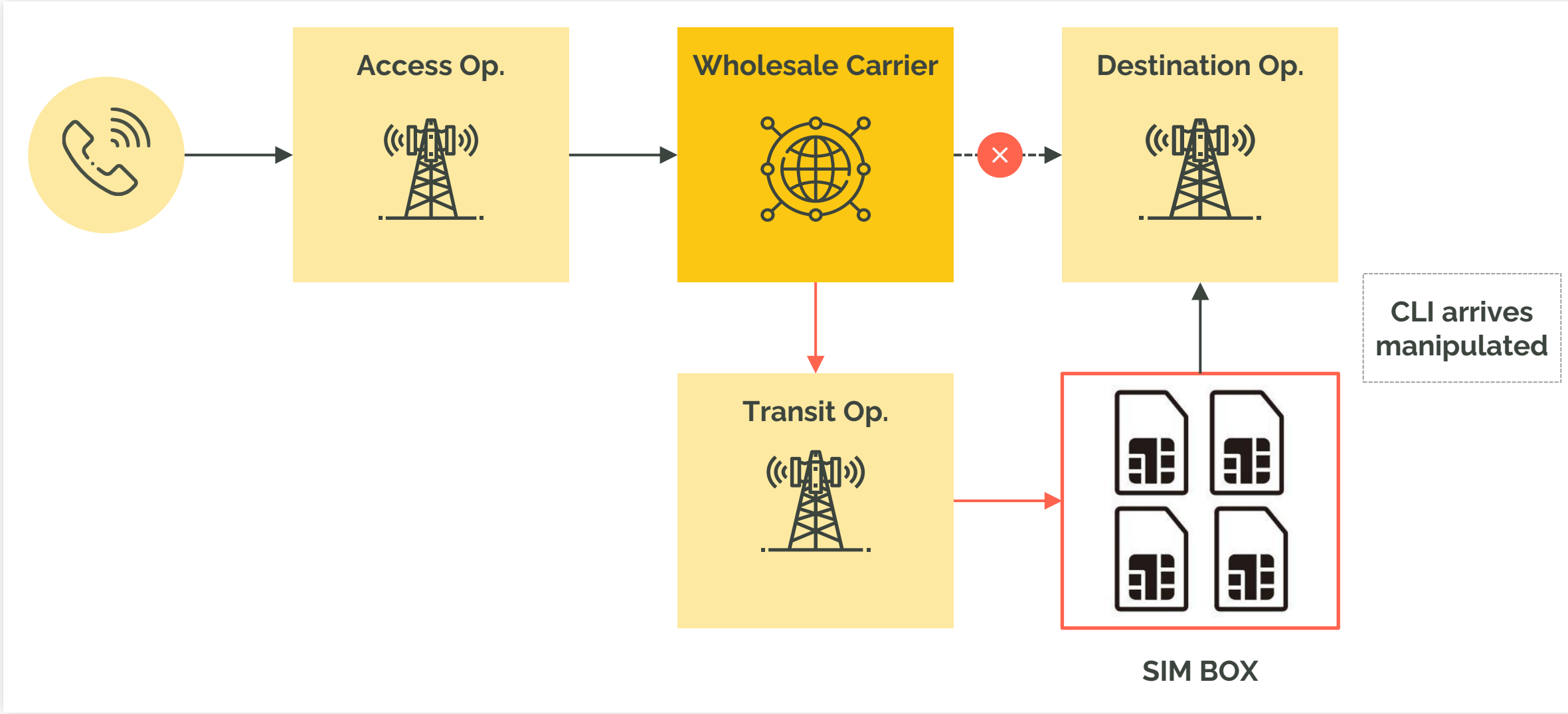
HACKING OF A CUSTOMER TELEPHONE SYSTEM



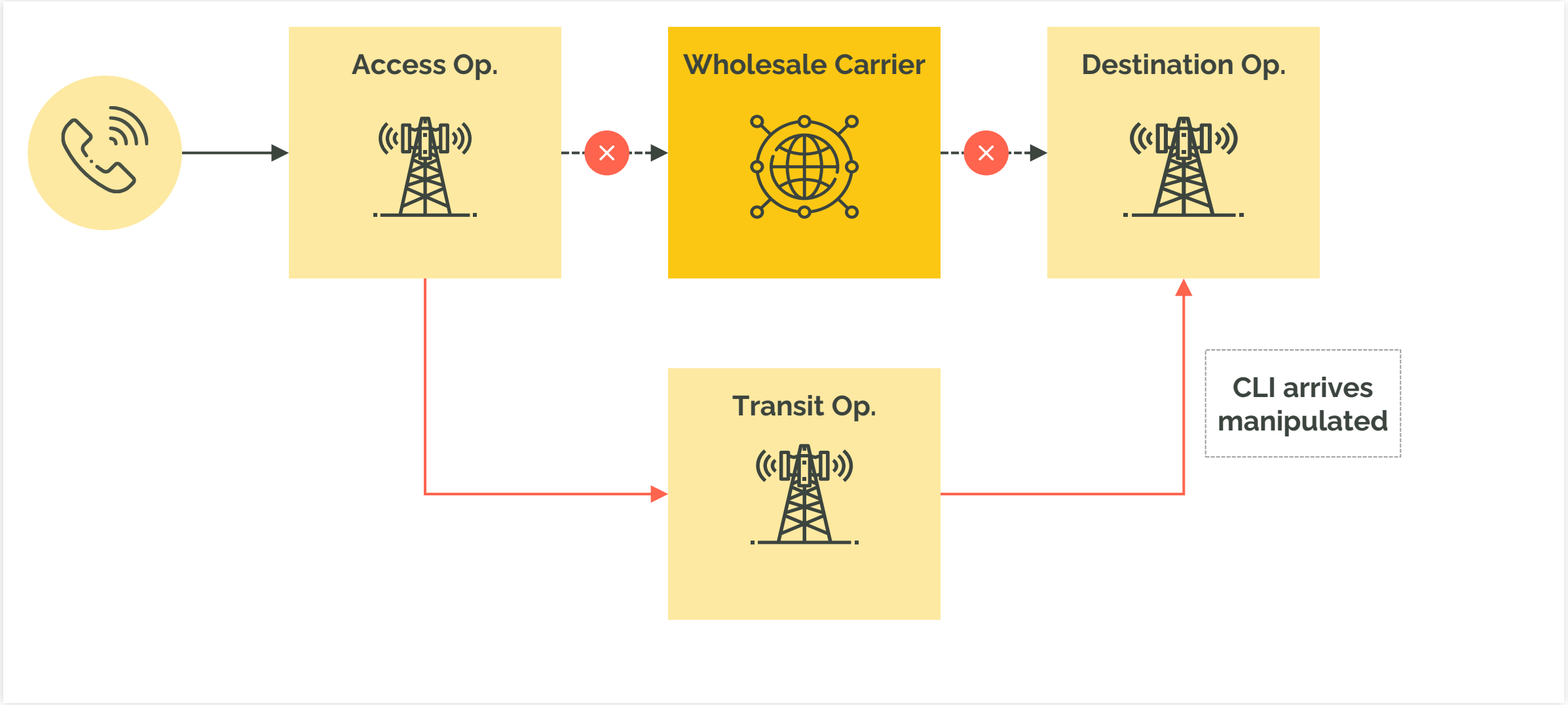
G. CLI Spoofing



F. Bypass 1/2

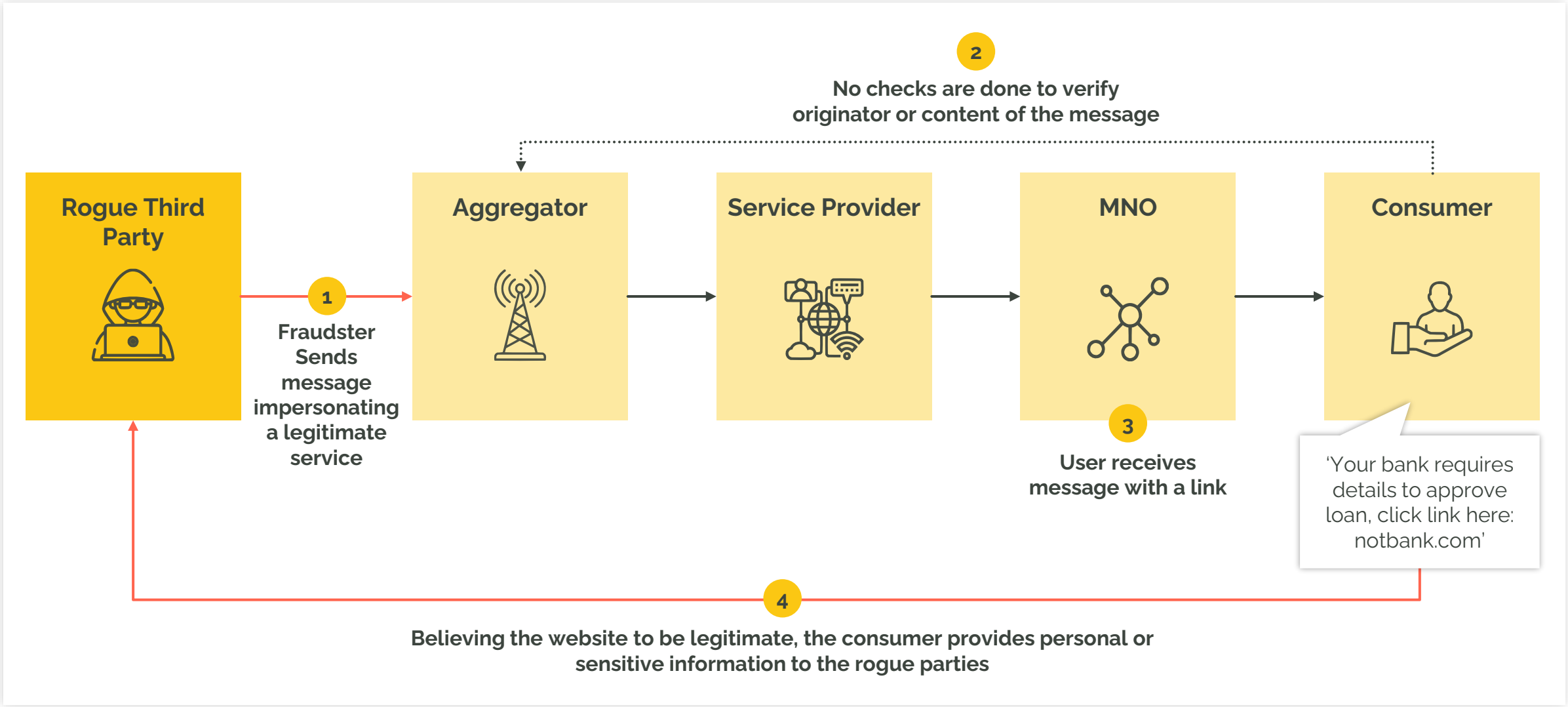

Access Op.
Wholesale Carrier
Destination Op.
Transit Op.
CLI arrives manipulated
SIM BOX

F. Bypass 2/2


Access Op.
Wholesale Carrier
Destination Op.
Transit Op.
CLI arrives manipulated

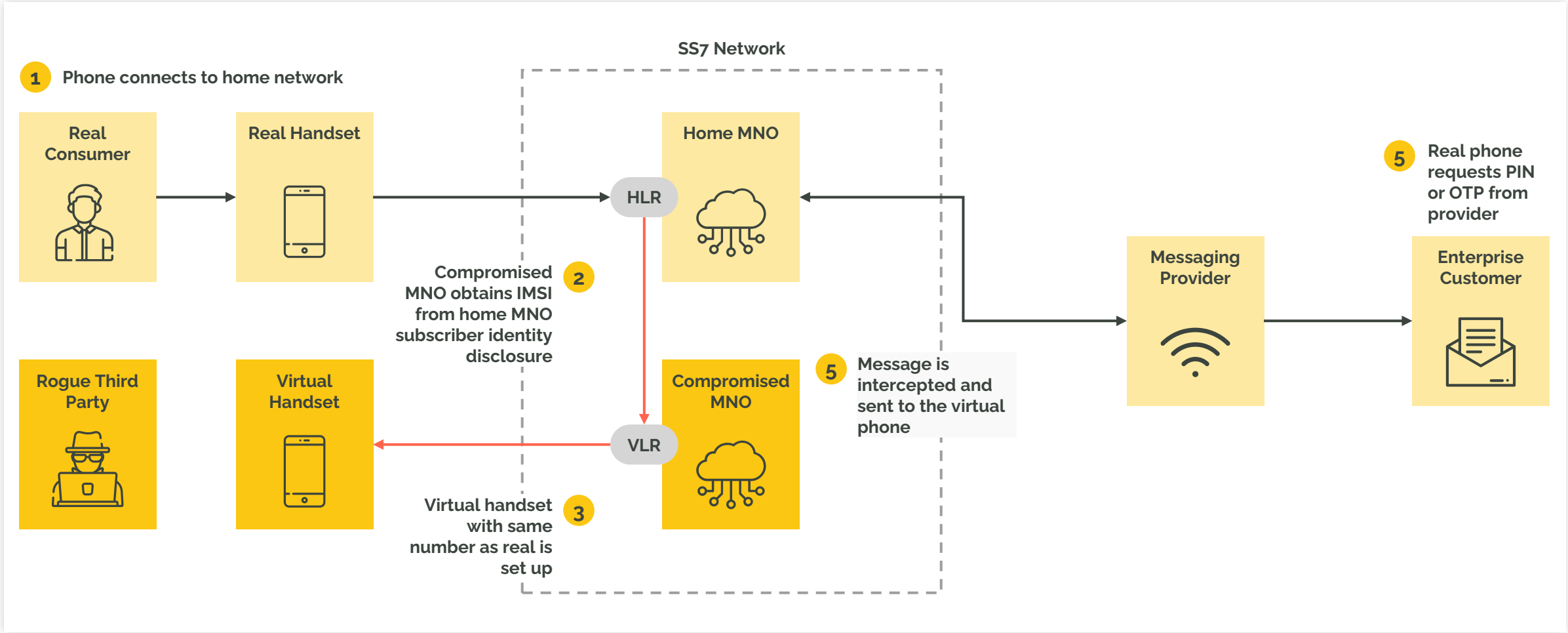
Fraud Definitions - SMS

A. SMS PHISHING (SMISHING)

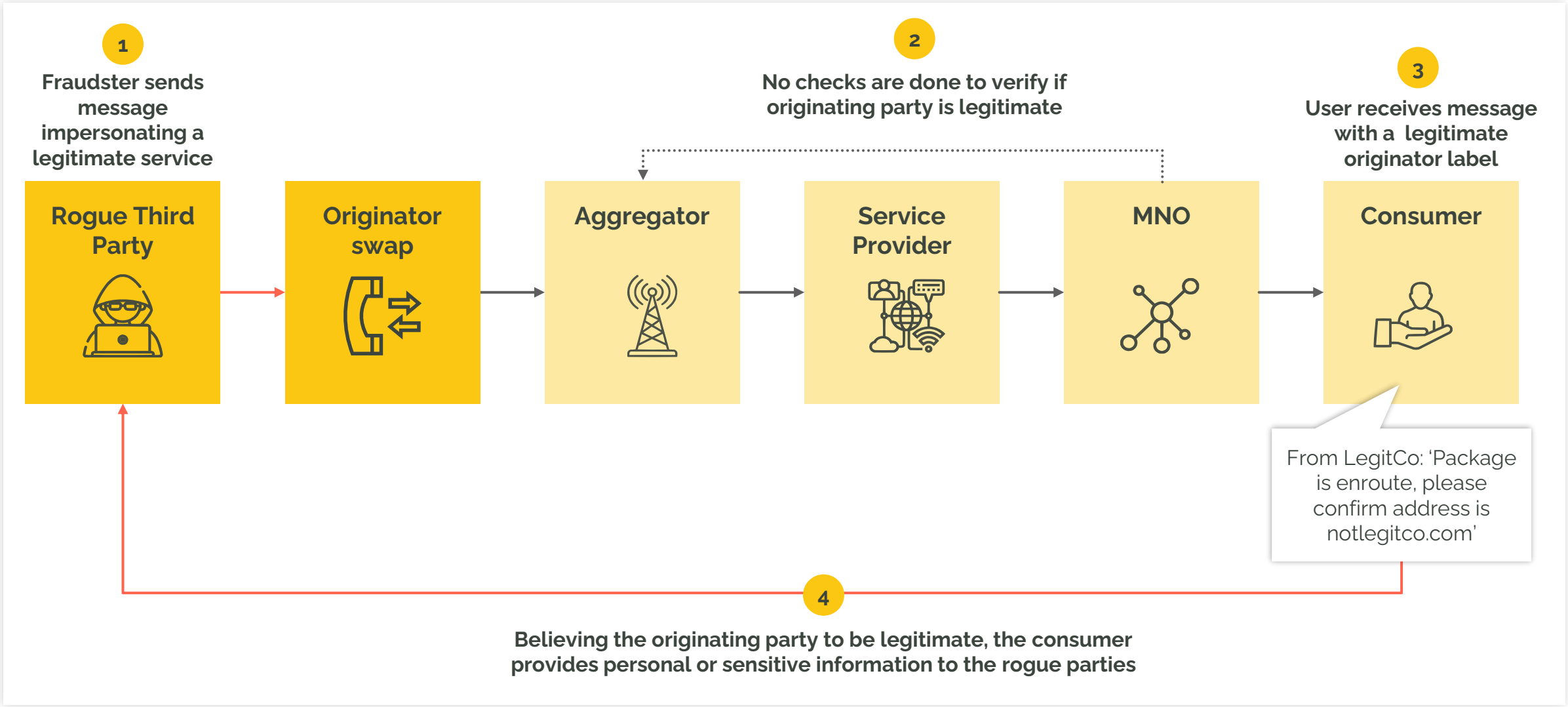


B. SMS Roaming / Sender ID intercept

ROAMING INTERCEPT

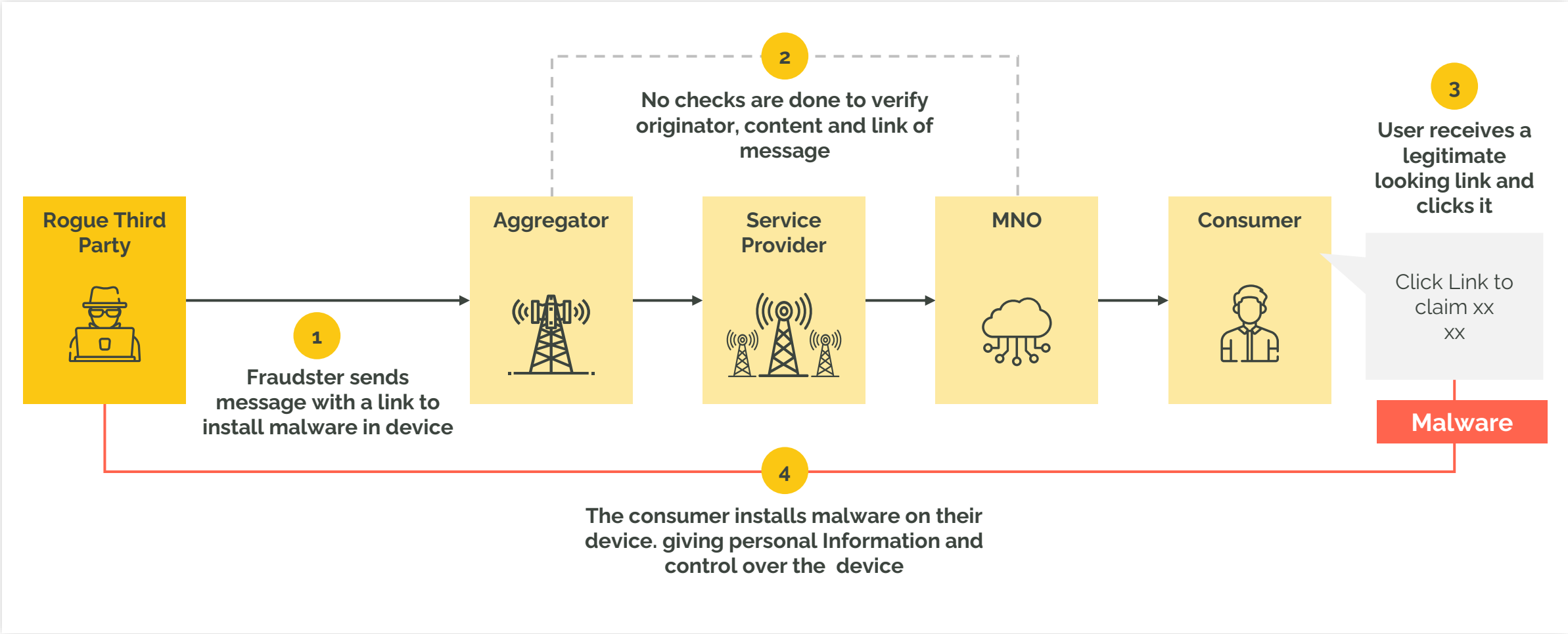


C. SMS ORIGINATOR SPOOFING



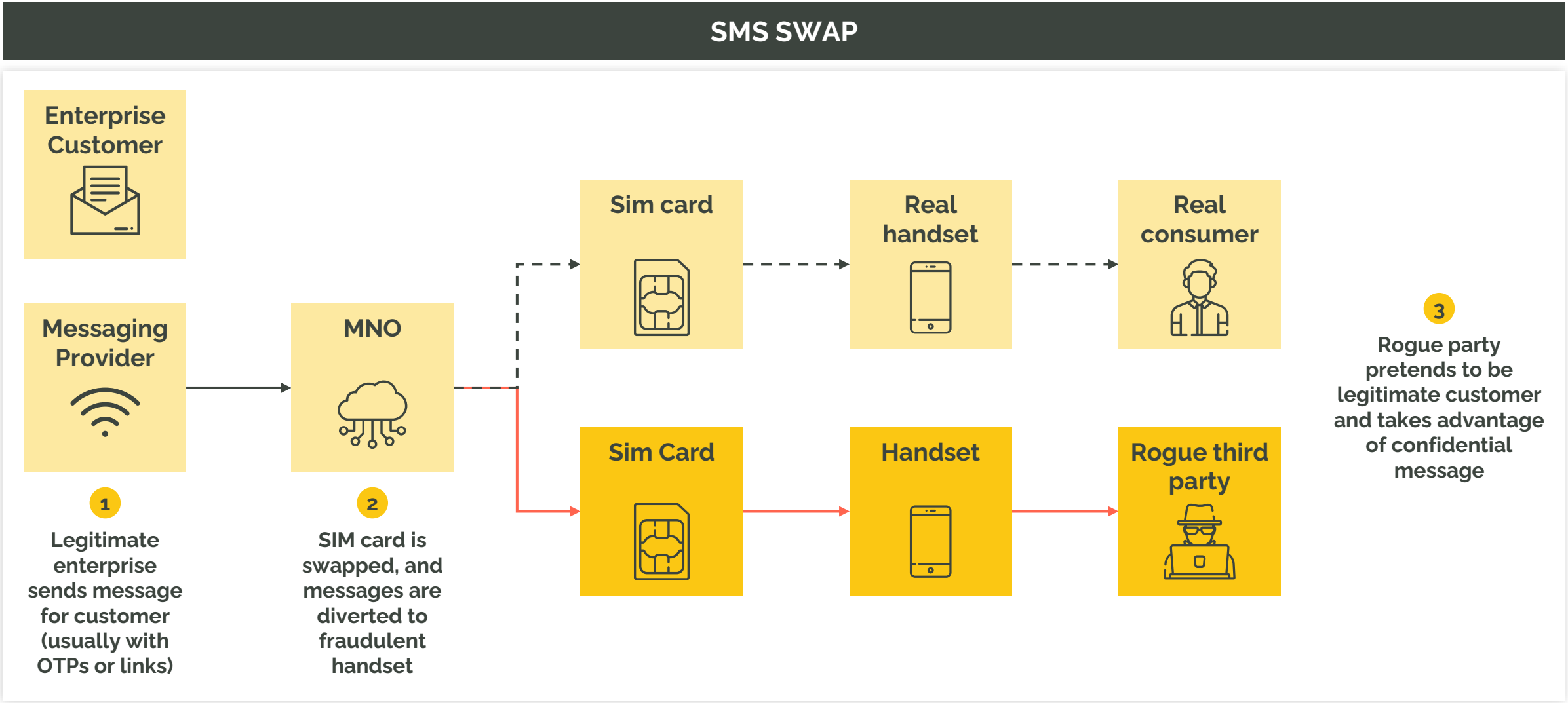
D. SMS Malware

SMS MALWARE

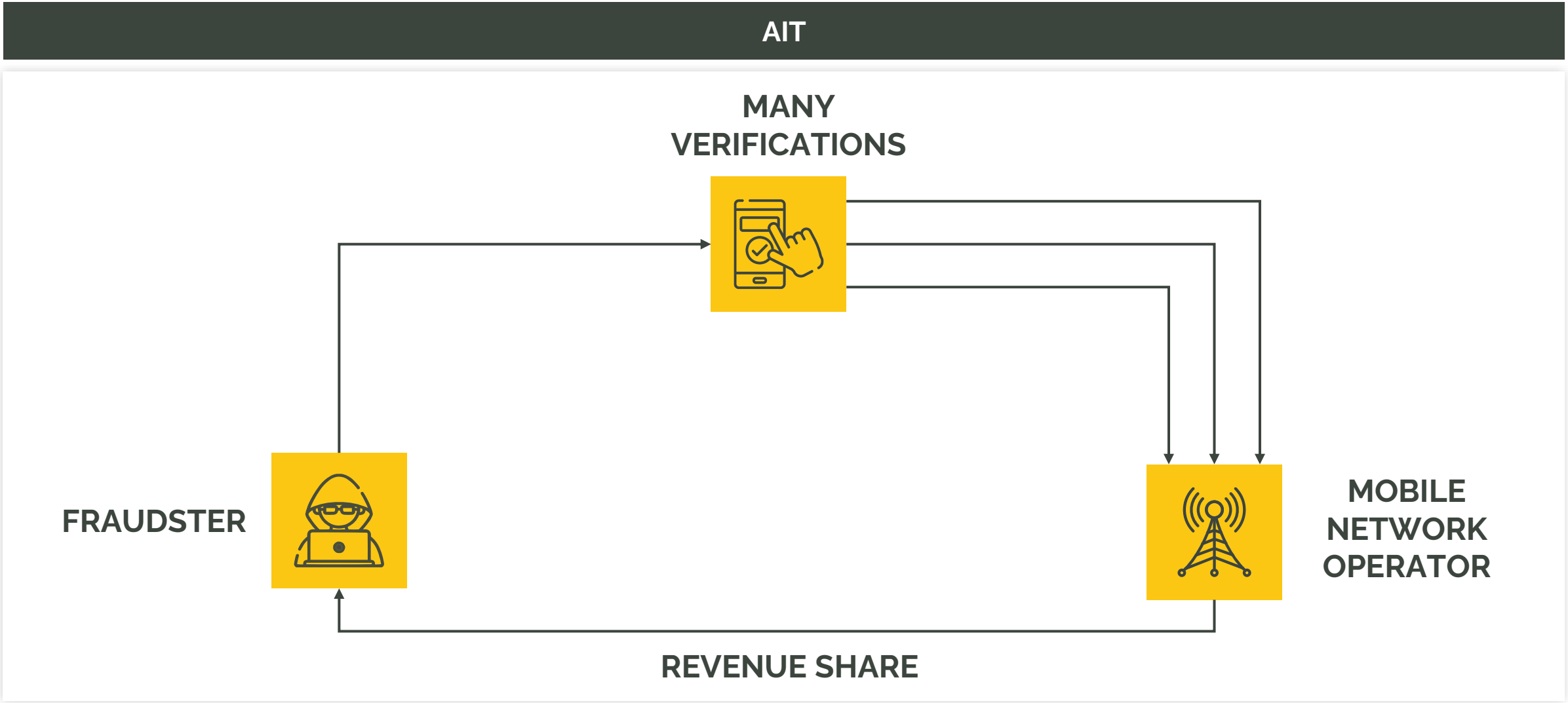


Fraudulent Legitimate flow Fraudulent Legitimate

E. SMS Swap – OTP intercept



F. ARTIFICIAL INFLATED TRAFFIC (AIT)



GLOBAL LEADERS' FORUM

GLF™

a techoraco brand

FTI CONSULTING™