GLF™

GLOBAL LEADERS' FORUM

2022

GLF Fraud Report

DEMONSTRATING ACCOUNTABILITY IN THE FIGHT AGAINST FRAUD

October 2022

Powered by

DELTA PARTNERS

an FTI Consulting company

This report has been commissioned by:

The ITW 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.

For more information please contact Annabel Helm at:

annabel.helm@euromoneyplc.com

DELTA PARTNERS
an FTI Consulting company

The report has been compiled and written by:

Delta Partners is a leading advisory and investment integrated platform globally. We are a unique hub for people, capital and knowledge to address challenges and opportunities in a transforming TMT industry. Our unique business model enables us to serve our TMT clients through our three business lines, Management Consulting, Corporate Finance and Private Equity.

For more information please contact Sam Evans at:

se@deltapartnersgroup.com

INTRODUCTION

Message from Judit Gerloczy Albers, Chair of the GLF Anti-Fraud Working Group

The 2022 GLF Fraud Report marks a continuation of the industry wide efforts to fight fraudulent traffic. As fraud continues to evolve each year, industry members are faced with a constantly changing environment which requires talent, dedication and most importantly collaboration within the industry.

This year is the fifth consecutive year in which the GLF has surveyed members for insights and trends on how fraudulent activity has affected their operations. For the first time ever, the GLF has also gained insight on messaging fraud, its effects on carriers and how fraud teams leveraging their knowledge on voice fraud to fight back. This has helped build a truly unique perspective on how carriers are affected by fraud throughout their entire product line. I would like to acknowledge the 35 fraud survey responses from GLF members and thank MEF for their insights on messaging fraud. MEF's actions and initiatives are a benchmark in the fight against messaging fraud. The 2022 fraud report has yielded some interesting conclusions:

1. In the voice fraud space, International Revenue Share Fraud is still the highest concern for the industry, with more than 50% of respondents acknowledging its high volume and impact. On the other hand we acknowledge that the impact of several use cases is declining, further proving the fact that good work and collaboration must continue to further mitigate the effects of fraudulent traffic
2. For messaging fraud, SMS phishing and impersonation are of most concern for the industry with 55% of our respondents seeing an increase in volume. Although tight measures have been applied which are reducing the impact on customers, it is clear that us as an industry should continue to educate our clientele and generate awareness.
3. We acknowledge the increase in carriers prioritising fraud management, with 43% of respondents stating fraud management as a top priority. This has translated into a notable increase in both investment (77% of respondents foreseeing an increase in the next 12 months) in fraud management tools and FTEs in the team, with 47% stating their intention to increase the team. We also observe how carriers structure voice and messaging anti-fraud teams, noting a lot of opportunities for synergies and increased internal collaboration. Additionally, we see an improvement in how the industry perceives their peer´s commitment to fight fraudulent traffic. Even though there is much work to be done, our efforts in increasing awareness for all members of the value chain have yielded positive results.

This is also the second year that we evaluate the adherence to the Code of Conduct published in 2018. I am proud to say that we have seen improvements from several carriers on applying the principles stated in the code of conduct as well as making clear operational improvements. Additionally we welcome members contributing for the first time who are setting goals to further improve their commitment to complying with the code of conduct. As we see the evolution of the application of these principles, we believe this process serves:

1. As a self-test to evaluate improvements, goals and specific actions to further develop their fight against fraud.
2. To provide confidence to the rest of the industry peers and third parties that carriers are taking concrete measures in their fight against fraud.

Finally, as my first publication as the Chair of the GLF Anti-Fraud Working group I would like to thank my industry colleagues for the trust they had placed in me. Although we have made good advances there is still much work to be done, I'm privileged to help spearhead these efforts and make sure we leave behind a better industry.

Judit Gerloczy Albers
Head of International Business, A1 Telkom Austria
October 2022

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

Organizations that responded to the survey or were interviewed

CONTENTS

EXECUTIVE SUMMARY

Voice Fraud

1. The volume of fraud has been increasing, **50%** of survey respondents see an increase in the volume and impact of fraudulent voice traffic versus the previous year.

   - **24 pp** increase from the **26%** of respondents in 2021.
   - Only **33%** of respondents experiencing a decrease in the impact of fraud.

   This indicates that fraud teams are increasing capabilities to detect fraudulent traffic and whilst bad actors are still driving a significant amount of fraudulent traffic through the carriers.

2. **IRSF** was listed as the highest in terms of volume (**50%** of respondents listed as **'high'** volume) and financial impact (**56%** of respondents listing **'high'** financial impact). As IRSF covers several techniques used by fraudsters the volume and traffic causing financial impact is higher than other use cases. Second to IRSF a popular application denominated **Missed Call / Wangiri Fraud** with **48%** listing 'high' volumes.

3. Historical trends indicate a constant decrease in the volume and financial impact of some fraud use cases:

   - Hijacking a reduction of **6 pp** from 2020.
   - Hacking of a customer's phone system a reduction of **8 pp** from 2020.
   - False answer supervision a reduction of **24 pp** from 2020.

   This illustrates the fact that voice fraud is a constantly changing environment from bad actors looking to fool systems to fraud teams that must continue to innovate and collaborate within the industry to stay one step ahead.

4. The increased sophistication and technology used by fraudsters have brought great challenges to the carriers' fraud teams. Although some use cases such as the financial impact of Missed Calls/Wangiri have been mitigated, **ISRF is still the main concern of the industry**, sparking new use techniques and methodologies to commit fraud. This concern should be translated to a further collaboration of fraud teams and the overall community, as this concerns many actors along the value chain.

Messaging Fraud

5. The growing messaging market has proven to be attractive to fraudulent actors. 35% of respondents observe an increase in the impact of fraudulent messaging traffic in the past 12 months. Respondents indicate **SMS Phishing** as the highest use case in volume and the growth (**55%** and **48%** of respondents respectively). As phishing messages increase in sophistication, it is crucial to both improve tools that detect and block fraudulent messages and double down on the efforts to educate customers in both detecting and reporting suspicious messages.

6. Despite high volumes in messaging fraud, effective firewall systems and the nature of the messaging fraud results in use cases having a low financial impact on respondents.

   - **42%** responded low financial impact on SMS Phishing and Originator Spoofing use cases.

   Although some use cases have no direct financial impact on carriers, they do have a negative impact on customer experience. Carriers must ensure the security and integrity of their network, making efforts to detect and fight against traffic intending to damage their end users.

7. Even though messaging traffic is a growing concern, **50%** of carriers who provided insights on both voice and messaging fraud see the **volume of fraudulent voice traffic higher than the volume of messaging traffic**. Although no consensus is reached given the data, additional points to consider are the varying volumes of messaging and fraud traffic each carrier experiences, the fact that some carrier´s messaging product is still novel to the market and that carriers have different thresholds to classify suspicious traffic.

Internal best practices

8. Diving into the carrier's internal practices, respondents show that fighting fraudulent traffic is an increasingly top priority.

   - **43%** of respondents listing fraudulent traffic as a **top priority** in their organization.
   - **17pp** increase from 2021.

   As indicated by the data this top priority translates into direct investment in internal resources, **77%** of respondents foresee an increase in investing in fraud prevention infrastructure in 2023 focused on process automation and efficiency. Additionally, **47%** of respondents forecast an **increase in FTEs** allocated to manage fraud in the next 12 months, hence the GLF expects continues investment in both manpower and technological solutions to support the fight against fraud.

Code of Conduct attestation process

9. The code of conduct established in 2018 sets the benchmark of behaviour that carriers should seek to attain to ensure that there is consistent action taken across the industry to fight against fraudulent traffic. It is broken down into **6 principles** related to targets and reporting, processes, destinations, payment flows, information sharing and contracting.

10. The attestation process kicked off in 2021 requires that participants prove their adherence to each of the six principles. To be compliant carriers must score over 70% in each of the six principles and provide evidence for their responses. Of the carriers that participated in the 2021 attestation process, **39% made improvements to their practices** improving their score, principally in the efforts made to roll out anti-fraud clauses in their new and existing contracts to comply with i3 forum standard anti-fraud clauses.

LIST OF EXHIBITS

PART 1

EVOLUTION OF FRAUDULENT TRAFFIC

Voice Fraud

1

The volume of fraud has been increasing, **50%** of survey respondents see an increase in the volume and impact of fraudulent voice traffic versus the previous year.

- **24 pp** increase from the **26%** of respondents in 2021.
- Only **33%** of respondents experiencing a decrease in the impact of fraud.

This indicates that fraud teams are increasing capabilities to detect fraudulent traffic and whilst bad actors are still driving a significant amount of fraudulent traffic through the carriers.

2

IRSF was listed as the highest in terms of volume (**50%** of respondents listed as **'high'** volume) and financial impact (**56%** of respondents listing **'high'** financial impact). As IRSF covers several techniques used by fraudsters the volume and traffic causing financial impact is higher than other use cases. Second to IRSF a popular application denominated **Missed Call / Wangiri Fraud** with **48%** listing 'high' volumes.

3

Historical trends indicate a constant decrease in the volume and financial impact of some fraud use cases:

- Hijacking a reduction of **6 pp** from 2020.
- Hacking of a customer's phone system a reduction of **8 pp** from 2020.
- False answer supervision a reduction of **24 pp** from 2020.

This illustrates the fact that voice fraud is a constantly changing environment from bad actors looking to fool systems to fraud teams that must continue to innovate and collaborate within the industry to stay one step ahead.

4

The increased sophistication and technology used by fraudsters have brought great challenges to the carriers' fraud teams. Although some use cases such as the financial impact of Missed Calls/Wangiri have been mitigated, **ISRF is still the main concern of the industry**, sparking new use techniques and methodologies to commit fraud. This concern should be translated to a further collaboration of fraud teams and the overall community, as this concerns many actors along the value chain.

Messaging Fraud

5

The growing messaging market has proven to be attractive to fraudulent actors. 35% of respondents observe an increase in the impact of fraudulent messaging traffic in the past 12 months. Respondents indicate **SMS Phishing** as the highest use case in volume and the growth (**55%** and **48%** of respondents respectively). As phishing messages increase in sophistication, it is crucial to both improve tools that detect and block fraudulent messages and double down on the efforts to educate customers in both detecting and reporting suspicious messages.

6

Despite high volumes in messaging fraud, effective firewall systems and the nature of the messaging fraud results in use cases having a low financial impact on respondents.

- **42%** responded low financial impact on SMS Phishing and Originator Spoofing use cases.

Although some use cases have no direct financial impact on carriers, they do have a negative impact on customer experience. Carriers must ensure the security and integrity of their network, making efforts to detect and fight against traffic intending to damage their end users.

7

Even though messaging traffic is a growing concern, 50% of carriers who provided insights on both voice and messaging fraud see the volume of fraudulent voice traffic higher than the volume of messaging traffic. Although no consensus is reached given the data, additional points to consider are the varying volumes of messaging and fraud traffic each carrier experiences, the fact that some carrier´s messaging product is still novel to the market and that carriers have different thresholds to classify suspicious traffic.

Internal best practices

Diving into the carrier's internal practices, respondents show that fighting fraudulent traffic is an increasingly top priority.

8

- **43%** of respondents listing fraudulent traffic as a **top priority** in their organization.
- **17pp** increase from 2021.

As indicated by the data this top priority translates into direct investment in internal resources, **77%** of respondents foresee an increase in investing in fraud prevention infrastructure in 2023 focused on process automation and efficiency. Additionally, **47%** of respondents forecast an **increase in FTEs** allocated to manage fraud in the next 12 months, hence the GLF expects continues investment in both manpower and technological solutions to support the fight against fraud.

1. VOICE FRAUD HAS BEEN GROWING AND NEW USE CASES ARE CATCHING ATTENTION

Overview of the different voice fraud methodologies observed in the survey:

1

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.

2

Missed Call Campaigns / Wangiri Fraud

A particularly popular application of revenue share fraud. The fraud involved bad actors generating quick calls to generate a missed call incite end users to return the call to a high-rate destination or premium rate number. The term originates from the Japanese world meaning "one ring and cut".

3

Call hijacking

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

4

Hacking of a customer telephone system

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

5

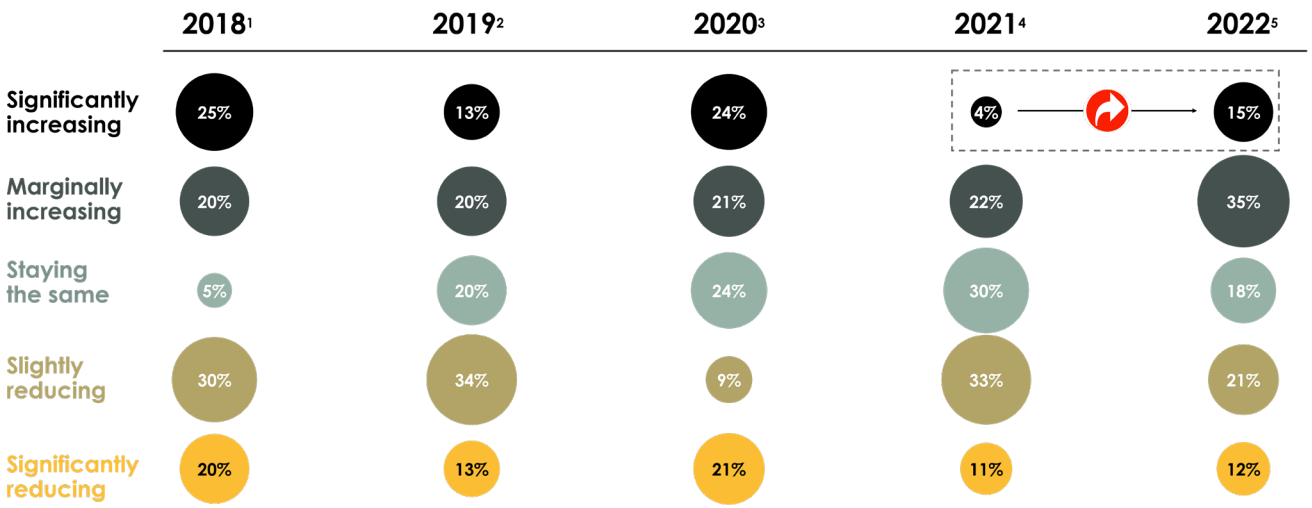
False Answer Supervision

When a bad actor returns a fraudulent answer signal to routing carriers therefore triggering the billing process of an otherwise uncompleted call.

Since 2018, the ITW Global Leaders' Forum's Annual Fraud Report has gathered data on different carriers' perspectives on fraudulent traffic and its effects on their network and users. The 2022 survey received 35 responses, the highest since 2019. The consensus from this year's responses is that the volume and impact of fraudulent voice traffic is increasing – as illustrated in Exhibit 1, 50% of respondents observed an increase versus 26% of respondents in the 2021 survey. The data also notes an overall decrease in the carriers that were observing a reducing trend, 32% of carriers in comparison to 44% of carriers in 2021.

EXHIBIT 1: ASSESSING THE CHANGE IN VOLUME AND IMPACT OF FRAUDULENT VOICE TRAFFIC

How has the VOLUME AND IMPACT of fraudulent voice traffic hitting your organization CHANGED in the past 12 months?
(% responses)



Notes: 1 n=20, 2 n=45, 3 n=32, 4 n=27, 5 n =35 ; Source: GLF Survey 2019-2020-2021-2022, Delta Partners Analysis

Speaking with carrier fraud teams whilst putting together this report, the perspective of increasing volume and impact of fraudulent traffic was a common theme. As three examples:

> *Even though we do see an increase in the volume of fraud trying to get through our network, the investments made on our fraud detection efforts have allowed us to minimize the impact for our clients.*

> *Although we see voice traffic volume as a whole slightly decreasing these last couple of years, we still see very innovative fraudsters that go undetected and still challenge us day to day.*

> *Thanks to the years of knowledge we have built up on our fraud teams, we have been more precise in detecting fraudulent traffic [that] we could not have been able to detect 18 months ago.*

As confirmed by some respondents, the capabilities and infrastructure developed by fraud and revenue assurance teams have allowed them to gauge the traffic through their network more precisely and as such have greater visibility of fraudulent activity in their network. Although carriers are continuing to focus on fraud identification and prevention, it is evident that fraudulent traffic is still a major concern for most of the carriers in the industry. The tide has not yet turned in the fight against fraudulent traffic.

Going into detail in Exhibit 2, which assesses the last 12-month trend of individual fraud use cases a majority of respondents have an ongoing challenge with International Revenue Share Fraud (IRSF) and Missed Calls / Wangiri Fraud. As illustrated in Exhibit 2, IRSF has been the use case that has shown the largest increase the past 12 months, with 43% of respondents acknowledging its increase in both volume and impact. This is followed by the missed call/ Wangiri fraud, which tallied up 37% of respondents agreeing on its increasing impact on their networks.

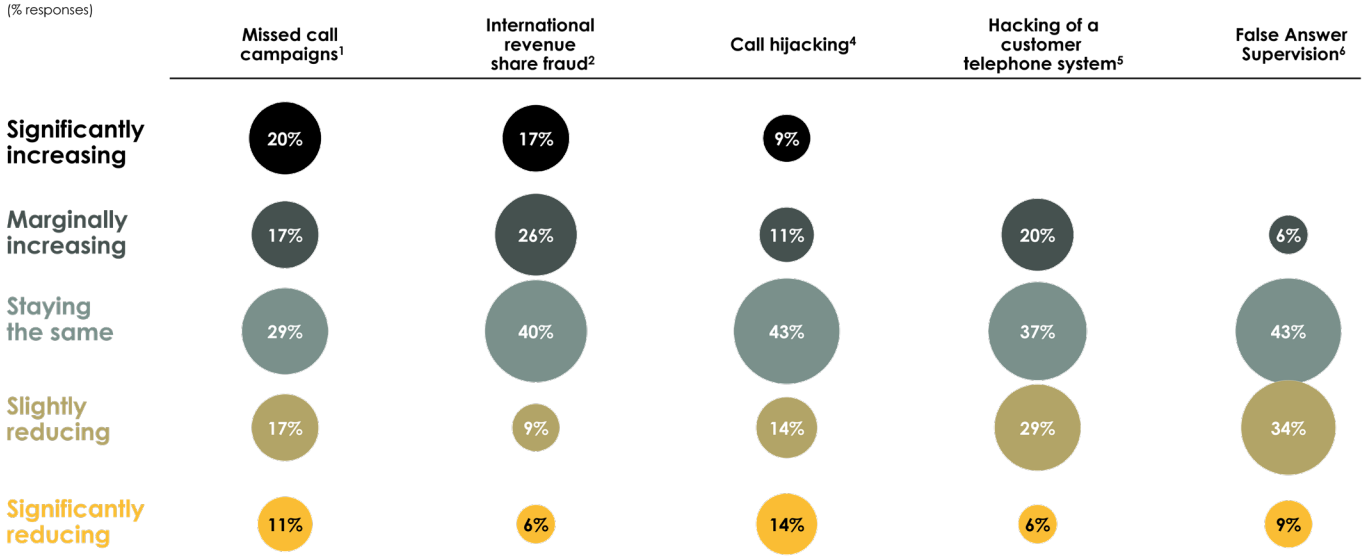
A new derivation of Wangiri fraud targeting enterprise customers on the network has been identified by a respondent. This new kind of Wangiri fraud, "Wangiri 2.0" as described by Lanck Telecom's Fraud Team, targets public contact forms from enterprises and brands via sending premium rate numbers and tricking the enterprise call centres or messaging systems into engaging with the premium number to collect high rates.

Regarding the other use cases such as Call Hijacking, hacking of telephone systems and False answer supervision, both 43% of respondents have stated that the volume and impact has stayed the same.

Another aspect of the results to highlight is the low level of responses that have seen reducing volume and impact on the different voice use cases, the highest one being a 43% decrease from False answer supervision, and the lowest being a 15% from IRSF. This indicates that only a minority of carriers are seeing the volume and value of fraudulent traffic reducing on their networks.

EXHIBIT 2: 12 MONTH CHANGE IN VOLUME AND IMPACT OF FRAUD USE-CASES

With respect to different fraudulent voice traffic use-cases how has their volume and impact changed over the past 12 months?
(% responses)



Notes: 1 n=33, 2 n=34, 3 n=32, 4 n=32, 5 n=32, 6 n=32; Omitted no responses; Source: GLF Survey 2022, Delta Partners Analysis

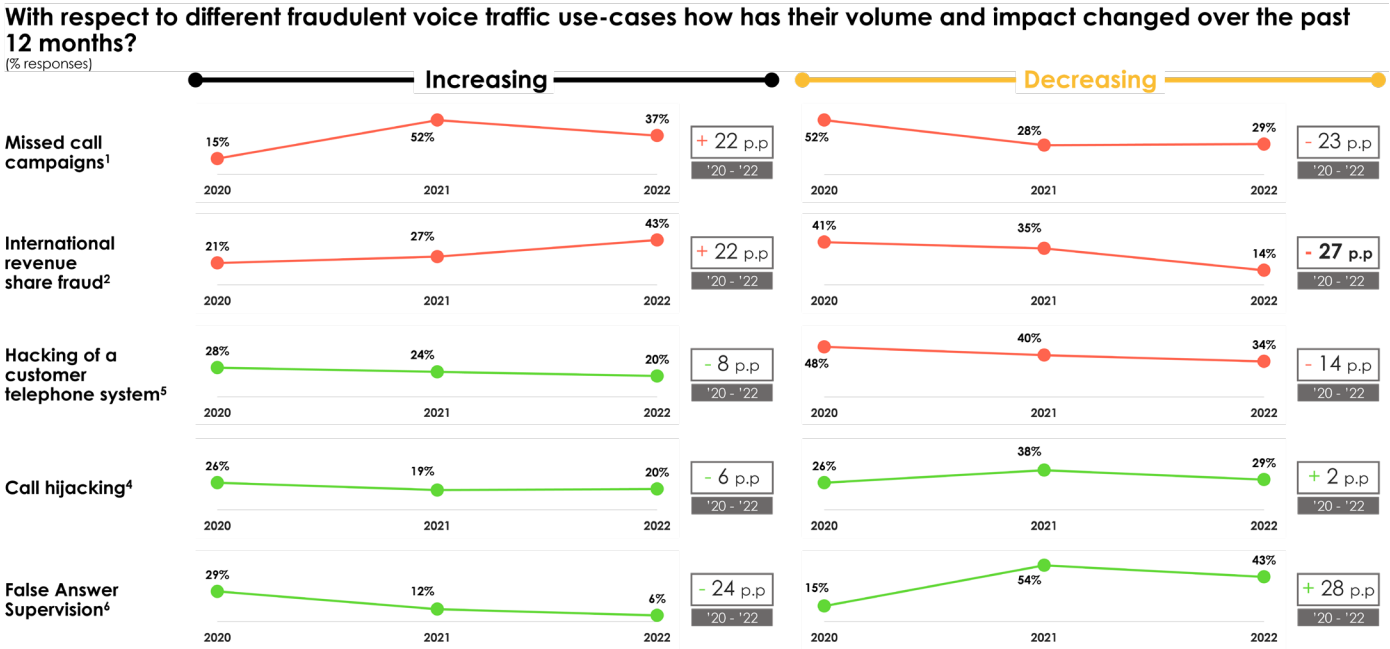
Given the data points gathered from the 2020 and 2021 GLF fraud reports, a time series assessment can be made to contextualize the historical trends of each voice fraud use case.

As showcased in Exhibit 3, the highest growing use cases have been Missed Call /Wangiri fraud and IRSF. Both IRSF and Missed Call / Wangiri use cases have seen a '20 – '22 growth of 22pp. The historical trend confirms the rising negative impact of both use cases on carriers.

The data also shows a constant decrease in trend of False Answer supervision (-24 pp since 2020), Hacking of customer phone system (-8pp since 2020) and call hijacking (-6 pp since 2020).

Highlighted in Exhibit 4 are the Volumes of each

EXHIBIT 3: HISTORICAL 12 MONTH CHANGE IN VOLUME AND IMPACT OF FRAUD USE-CASES



Notes: As % of total answers in the noted year; Omitted No Response Answers; Source: GLF Survey 2020-2021-2022, Delta Partners Analysis

fraud case, the highest being IRSF and the Missed Calls campaigns, being 50% and 48% of the total responses for each use case respectively.

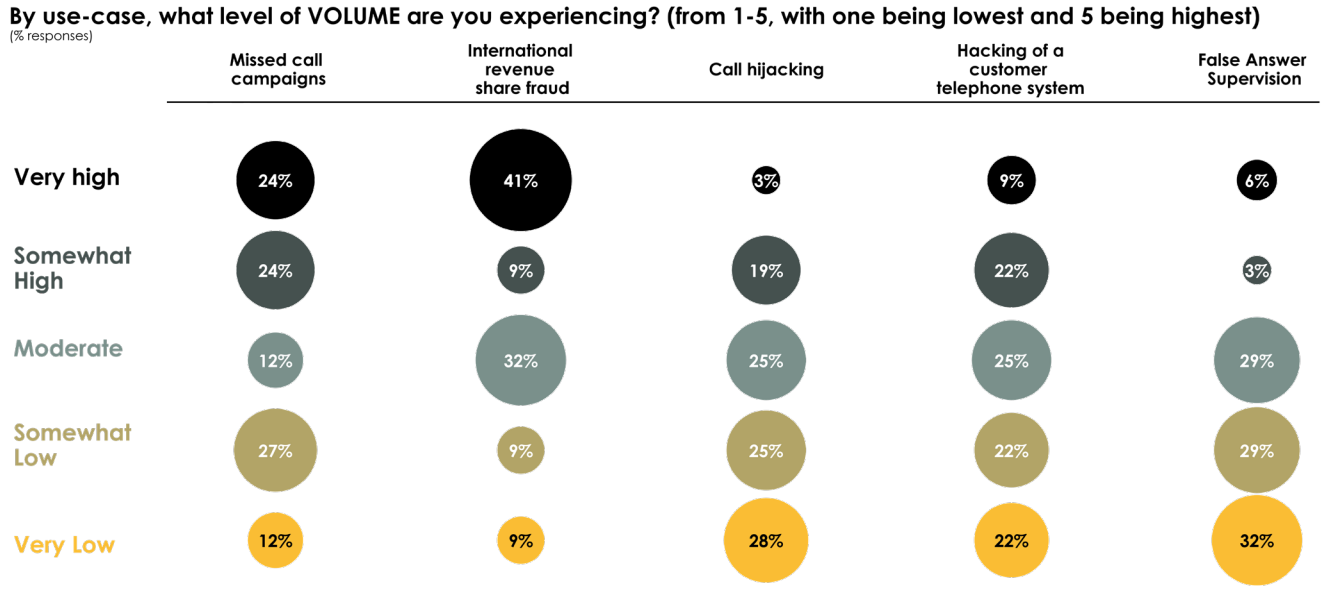
Although the consensus from respondents on the remaining use cases has been a low observation of high volumes, it is still notable to mention the comparatively small percentage of respondents that have reported 'Somewhat' and 'Very Low' volumes of each fraud case. From a volume perspective the data shows that carriers are still experiencing significant volumes of fraud from many of the use cases surveyed.

One interpretation of this trend is that increased experience and experimentation within fraud teams has resulted in better detection and thus the reporting of higher volumes of fraud. "The first step of a successful fraud team is to be able to spot as much unusual or suspicious activity as you can, as fast as you can" was cited by a respondent.

The ability to continuously spot and classify fraudulent traffic as it flows through the network is the key first step to control and prevention.

To get the most complete picture of the effect that different fraud use cases have on carriers, the responses on the financial impact of each use case must be contrasted to the reported volumes. As seen in Exhibit 5, a constant clear outlier in terms of the combination of volume and financial impact is IRSF which carriers have reported as the highest in financial impact with 56% of responses in the High category. Given that IRSF covers many fraud instances it is logical that carriers are seeing many

EXHIBIT 4: ASSESSING THE VOLUME OF FRAUD USE-CASES

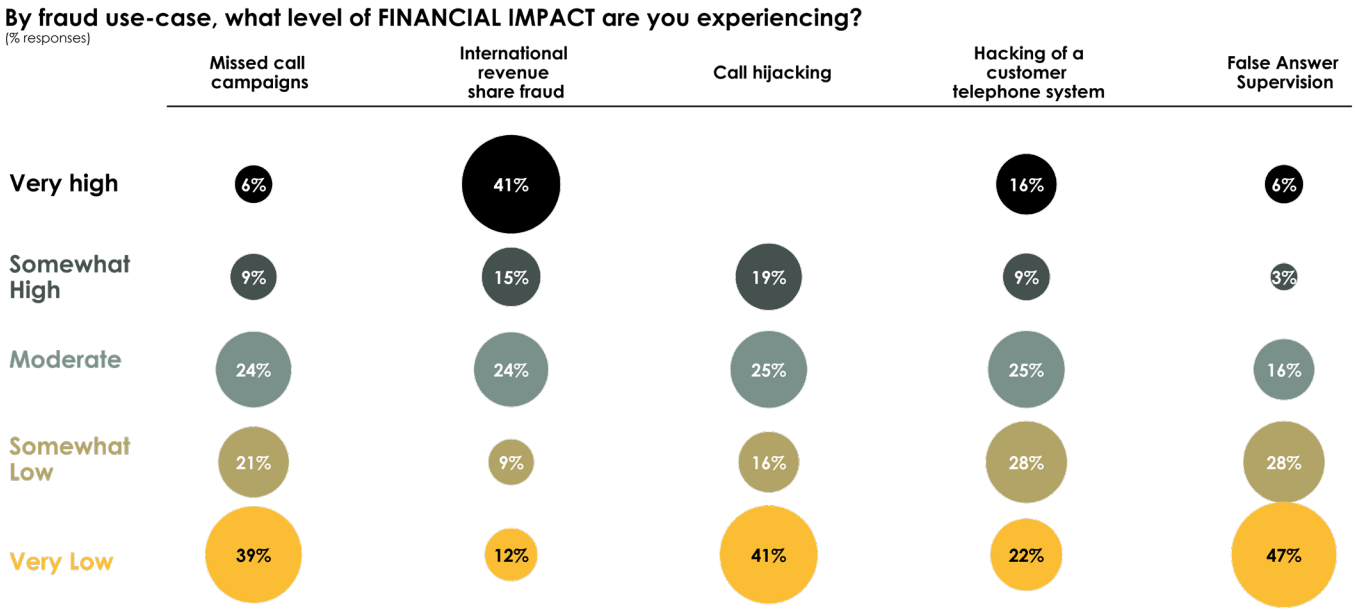


Notes: n=31; Omitted no responses ;Source: GLF Survey 2022, Delta Partners Analysis

variants of the same kind of fraud.

In contrast, Missed Call / Wangiri fraud has a reported low or very low impact of 60%, in line with the rest of the fraud use cases. This highlights a positive result of the efforts made by several respondents on the prioritisation of the minimisation of impact of Wangiri fraud, "definitely the priorities of our teams are changing, two years ago we were solely focused on lowering the impact of Wangiri as much as possible for our clients, now that we have succeeded, we can apply our learnings to other rising kinds of fraud" said one of the respondents.

EXHIBIT 5: ASSESSING THE FINANCIAL IMPACT OF FRAUD USE-CASES



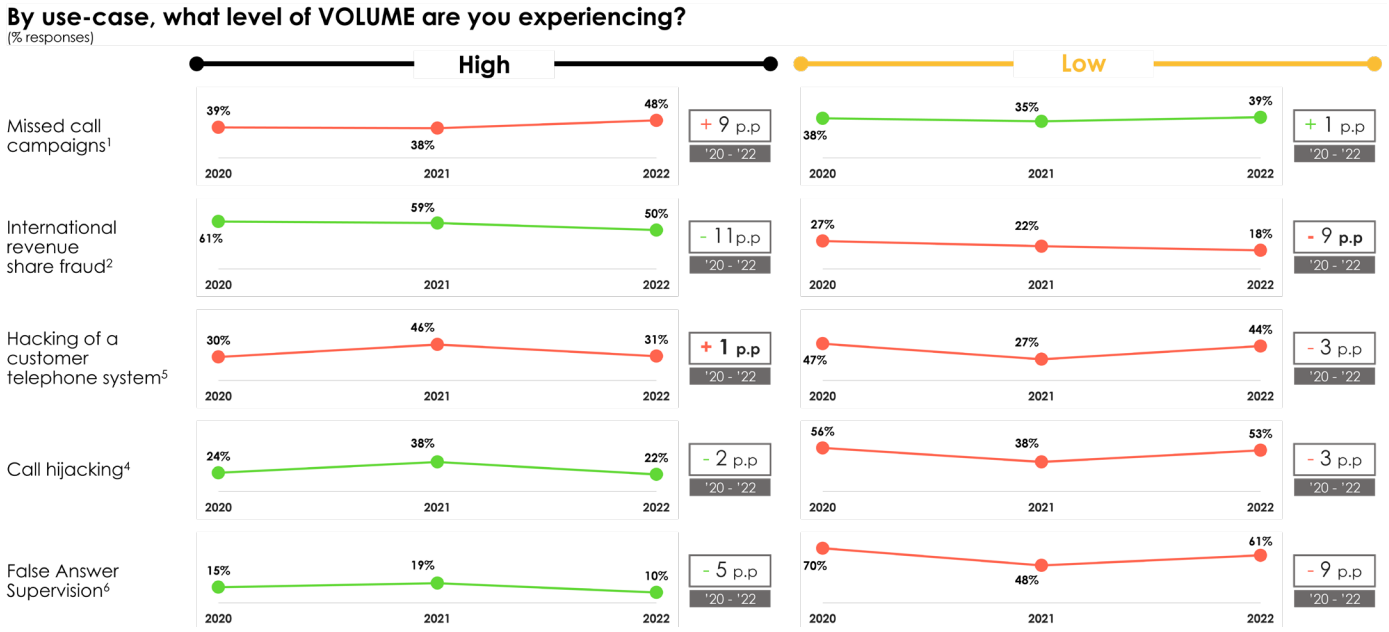
Notes: n=32; Omitted no responses ; Source: GLF Survey 2022, Delta Partners Analysis

Putting the trends into a historical perspective in Exhibits 6.1 and 6.2, the changing nature of the volume and impact of different use cases is clearly illustrated. The number of responders stating a high volume of IRSF has decreased 11pp since 2020, although it is still the largest use case of fraud volume and in contrast, financial impact of IRSF has increased 6 pp since 2020. The trend has made it clear that it is the highest value concern for the carriers since the data has been gathered in 2020.

Missed Calls/ Wangiri fraud has had a constant increase, up 9pp since 2021. On the other hand, the financial impact has increased slightly since 2020 but the data indicates that the high financial impact of Wangiri fraud reduced in 2022. This is confirmed by the detection and prevention systems implemented by the different carriers and their reported success of the successful detection and control of fraudulent traffic.

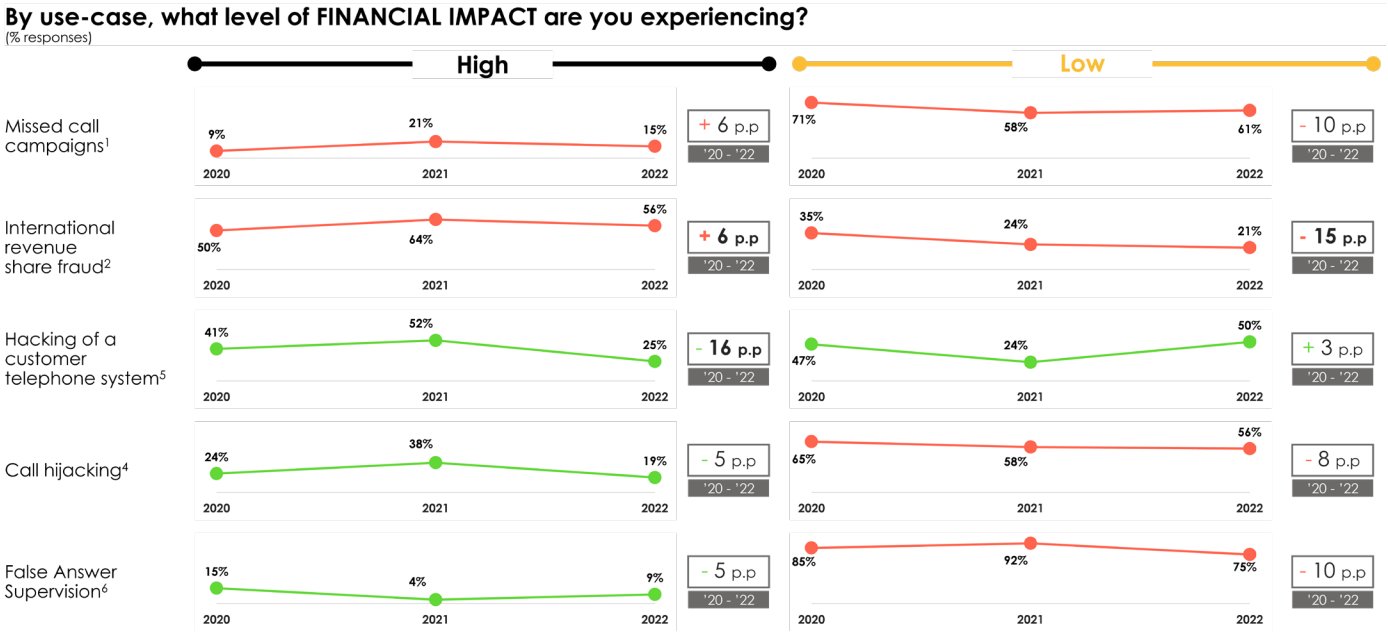
A point to acknowledge is the notable decrease of hacking, call hijacking and false answer supervision in both financial impact and volume. Although different responders did not list these types of fraud as a team priority or as a heightened concern, the increase of volume of Missed Calls/Wangiri and ISRF in comparison to the decline of volumes in hacking, hijacking and false answer supervision indicates that fraudulent parties are evolving their preferred methods to commit fraud.

EXHIBIT 6.1: HISTORICAL ASSESSMENT OF THE VOLUME OF FRAUD USE-CASES



Notes: As % of total answers in the noted year; Omitted No Response Answers; Source: GLF Survey 2020-2021-2022, Delta Partners Analysis

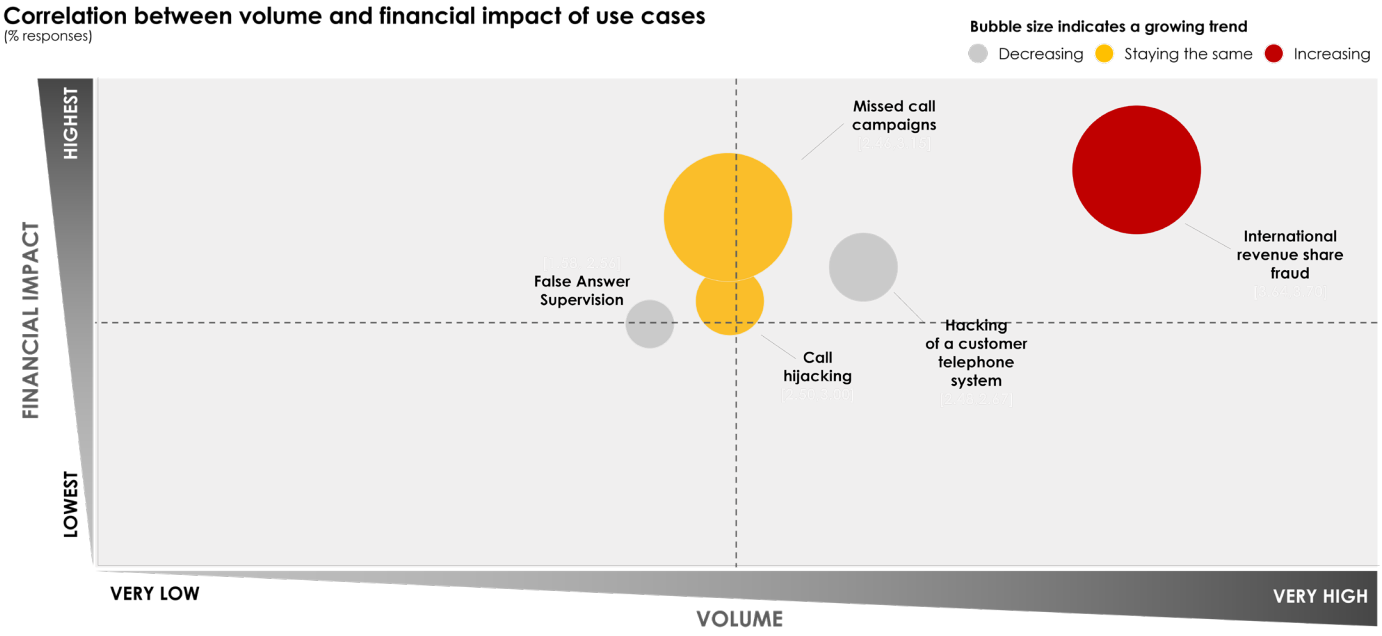
EXHIBIT 6.2: HISTORICAL ASSESSMENT OF THE FINANCIAL IMPACT OF FRAUD USE-CASES



Notes: As % of total answers in the noted year; Omitted No Response Answers; Source: GLF Survey 2020-2021-2022, Delta Partners Analysis

When mapping the volume, financial impact and the trend of each use case, Exhibit 7 showcases that the use case that generates the highest concern is IRSF. Carriers are observing both an increase in the "sophistication and creativity of many bad actors" as mentioned by some respondents. The quick adoption of automated tools such as number range generators (as noted by one respondent) illustrate the advanced new type of fraudster that carrier fraud teams confront in their daily operations. This has caused fraud teams to tighten tolerance levels and policies and to continue experimenting with pattern detection and prevention measures.

EXHIBIT 7: MAPPING THE VOLUME AND VALUE IMPACT OF FRAUD USE-CASES



Notes: n=35; Source: GLF Survey 2022, Delta Partners Analysis

CONCLUSIONS

1. The main concern of the industry is the value impact and growth of IRSF. The increased sophistication of the technology being used by fraudsters has created challenges for carrier fraud teams. The financial impact of Wangiri fraud has been mitigated through better detection and prevention tools, however volume is still increasing.

2. The year-on-year reduction of the impact from other voice fraud use cases illustrates the fact that voice fraud is a constantly changing market, for both bad actors in the system looking for ways to innovate and implement different, sophisticated tools to the carrier fraud teams that must rely on the creation of policies and procedures based on collaboration and knowledge sharing with different players throughout the value chain.

2. A DEEP DIVE INTO MESSAGING FRAUD

Context on the messaging market

The messaging market is one of the most lucrative and fastest growing sectors in the telecom industry. The most notable subsector of the market being A2P (application to person) messaging that has enabled a variety of products and use cases such as:

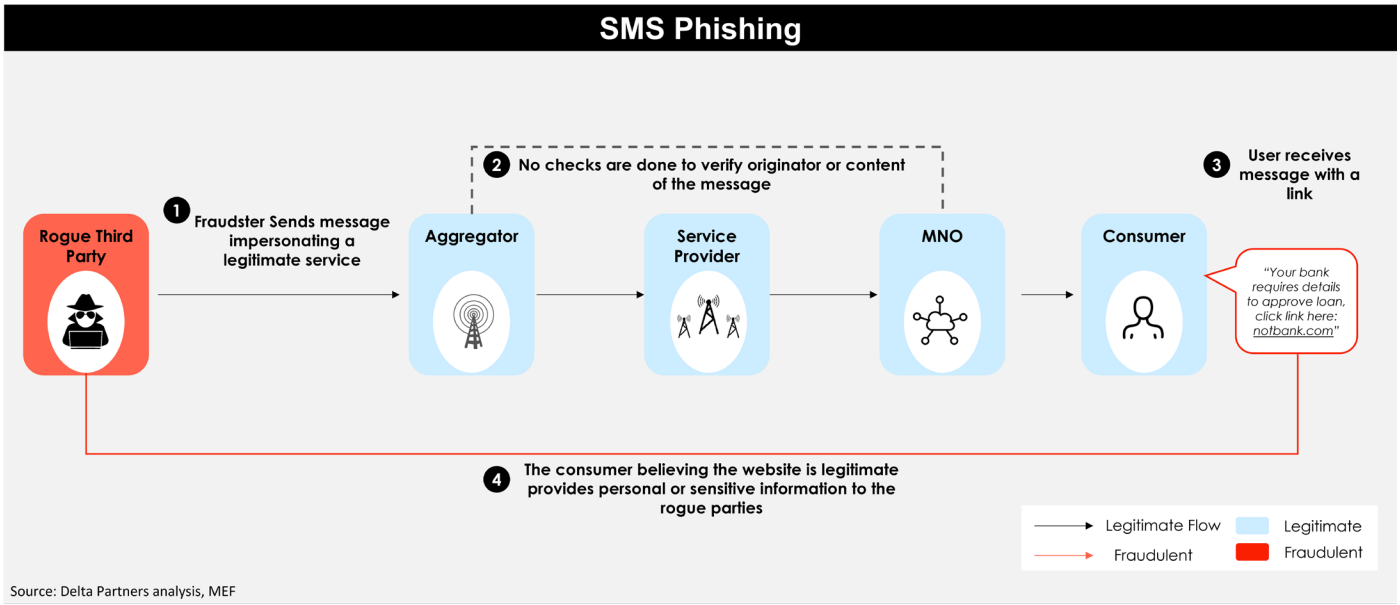
- Cheap and reliable communication with a brand's client base
- The implementation of authentication products such as OTP (One-time passwords)
- Enablement of a rich customer interaction through chatbots.

It is estimated that the A2P Messaging market is projected to grow 2.1% CAGR up to 3.2 trillion messages in 2026 and USD $77bn in revenue (Omdia Data). The facility and cost effectiveness to generate messaging fraud makes this sector attractive to bad actors in the system, for both new entrants and known fraudsters. According to some carrier fraud teams, identified bad actors that generate fraudulent voice traffic are also attempting to bypass the carrier's sanctions by driving fraudulent messaging traffic.

For the scope of the survey the following messaging use cases were considered:

1. SMS Phishing (Smishing)

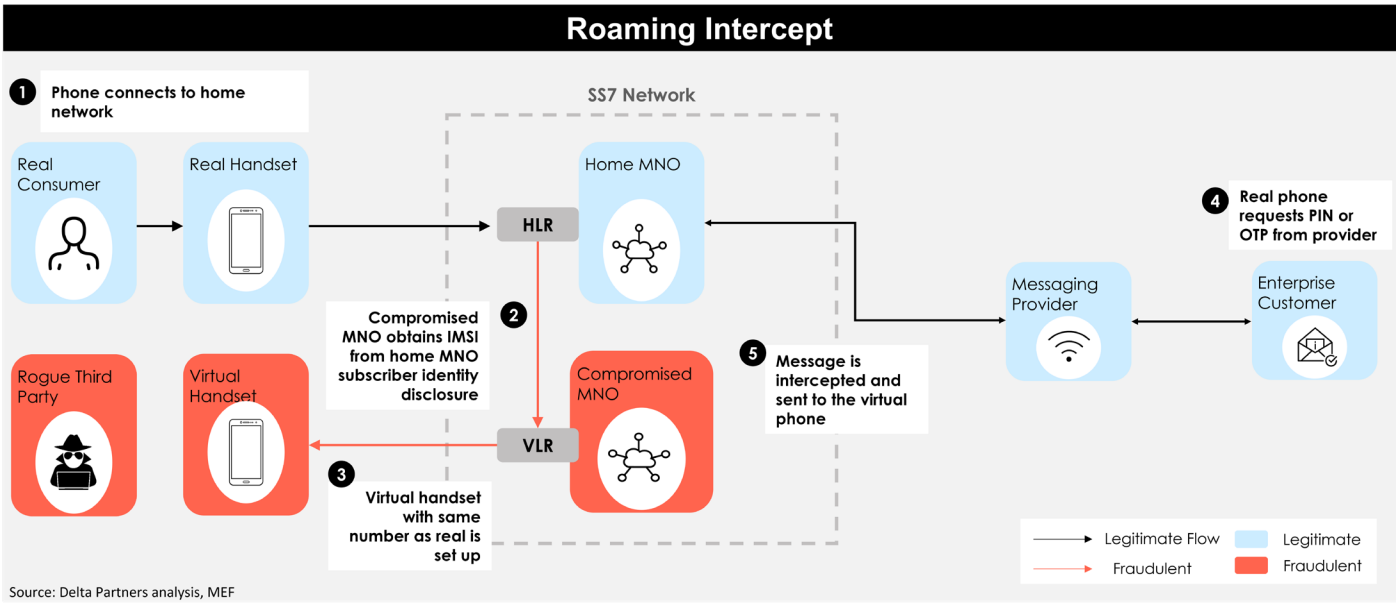
SMS Phishing creates a legitimate-looking message impersonating a legitimate entity to obtain through deception and social engineering the end user personal information or other sensitive data. In some cases, smishing can lead to a compound of voice fraud, when a number is originally listed in a smishing message, and the user calls a high-cost destination.



Source: Delta Partners analysis, MEF

2. SMS Roaming Intercept

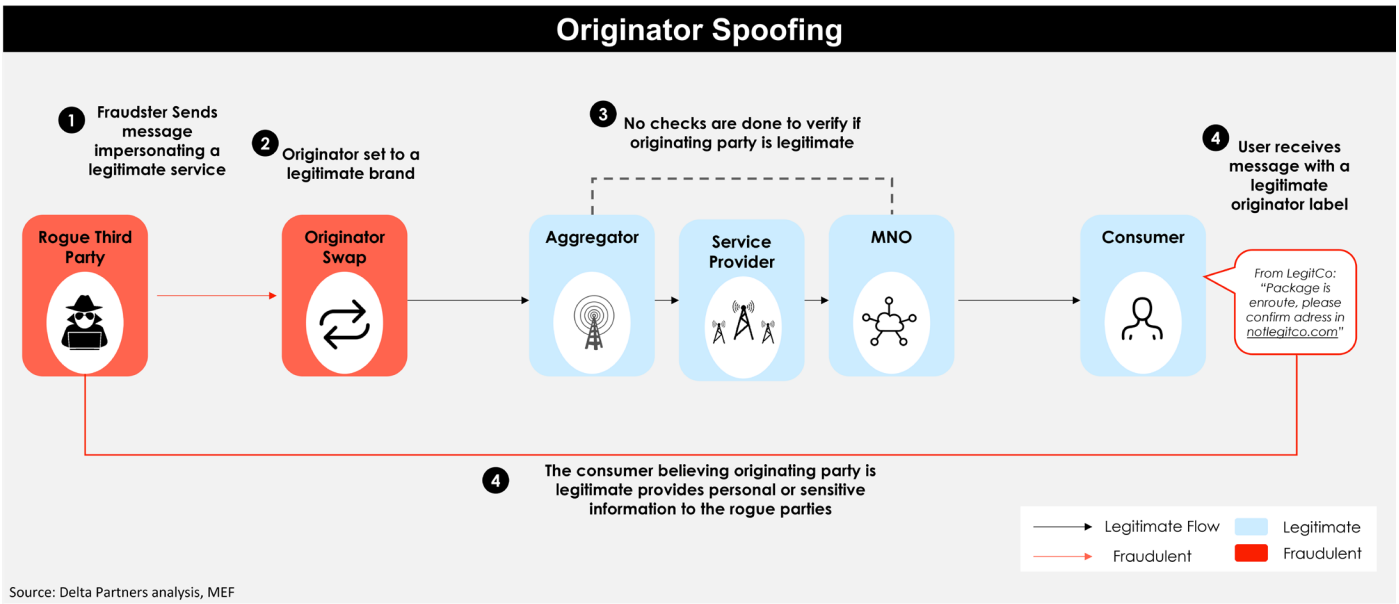
Interception of legitimate messaging traffic when user is roaming on another network. It is mostly used to intercept two factor authentication messages or OTPs to access the final-user's banking or mailing accounts.



Source: Delta Partners analysis, MEF

3. SMS originator Spoofing

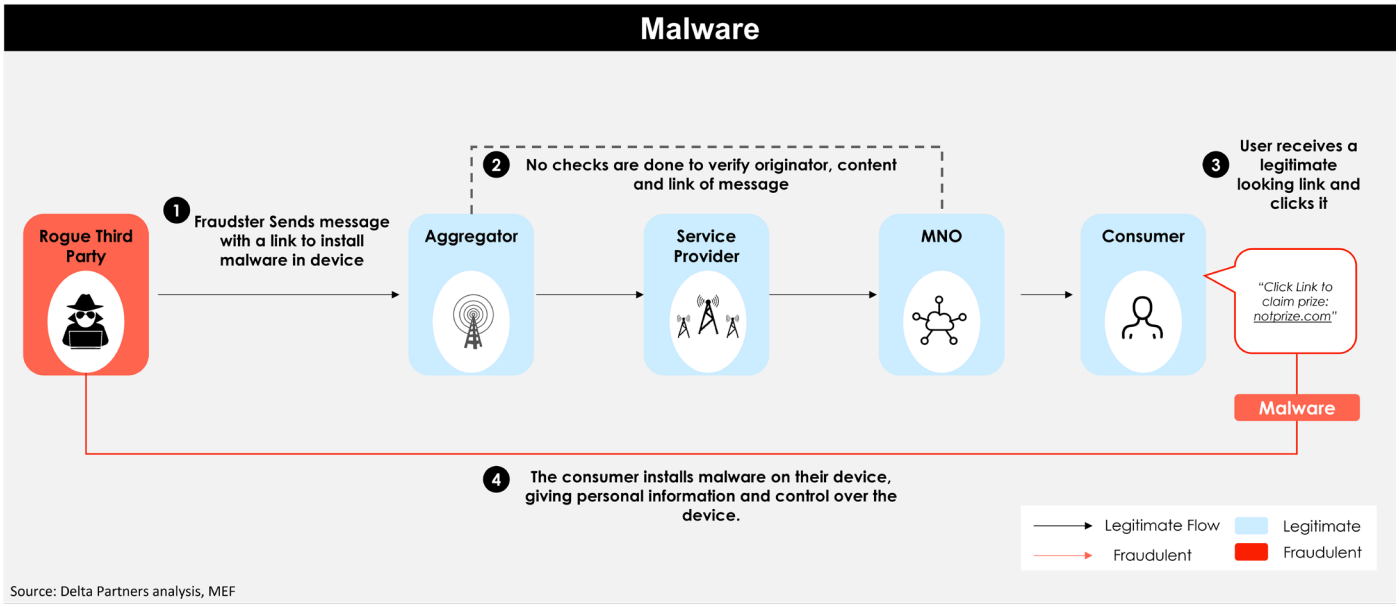
The use of aggregation routes and unchecked parts of the system to hide originator's identity and trick the receiving party into believing it is a legitimate originator. Used in combination with phishing to make message appear more legitimate to victim.



Source: Delta Partners analysis, MEF

4. SMS Malware

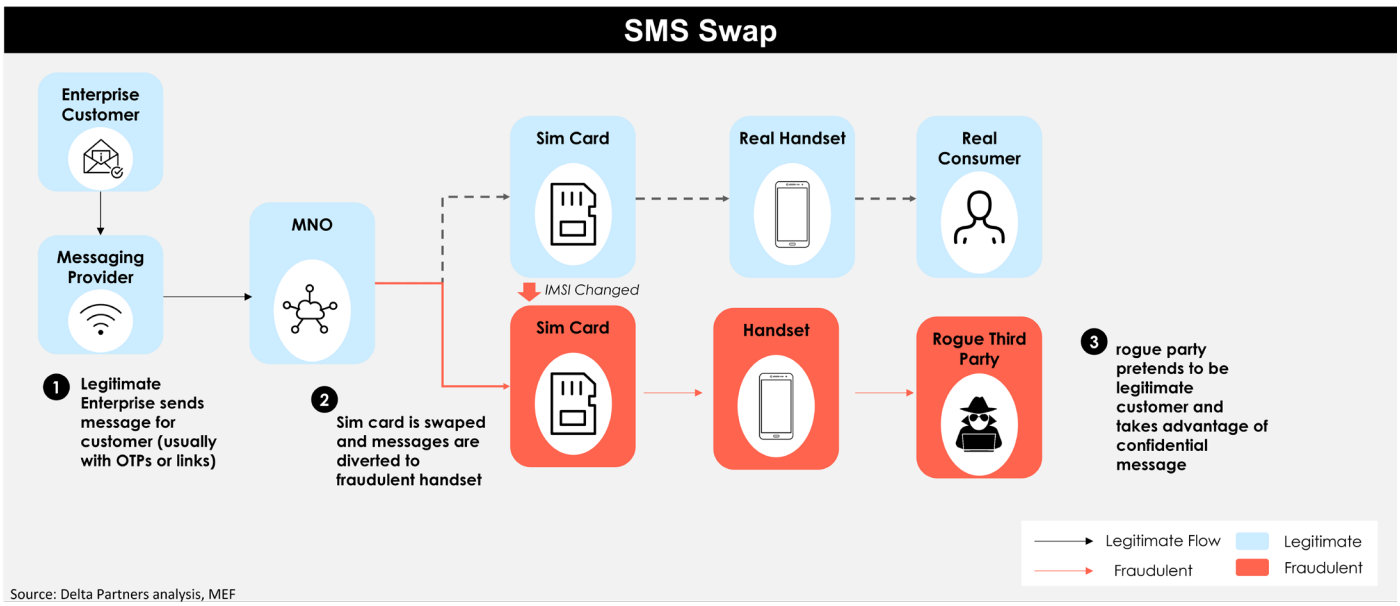
Malware installed via clicking on a link sent by a legitimate looking message from a rough party. A noted case by several respondents was the Flubot spyware software. The software gains control of the mobile phone's data and might steal sensitive information such as banking details or account passwords.



Source: Delta Partners analysis, MEF

5. SMS Swap – OTP intercept

The fraudster gains control of the victim's sim card to intercept incoming legitimate text traffic that may include sensitive data such as OTPs or sensitive banking information that might be used to commit further fraud.



Source: Delta Partners analysis, MEF

In further conversation with participants, other use cases of messaging fraud where mentioned:

1. Flash Calling

An alternative to OTP and messaging authentication, several carriers mentioned that they noticed several short, missed calls in their network that did not fit the pattern of regular missed call campaigns or wangiri fraud. A flash call is produced by a legitimate provider that generates a short call to a number user to authenticate it as an alternative to the traditional A2P messaging route. The position of some respondents is that this type of product is "abusing the voice network and should not be allowed". Although upon further discussion most of the carriers see this as an opportunity to be developed as a new product if it is correctly monetised and regulated.

2. Artificial Traffic Generation (ATG)

An emerging use case, it involves the generation of multiple messages with no end-user and the route is validated and charged by the generation of a fake DLR (Delivery report).

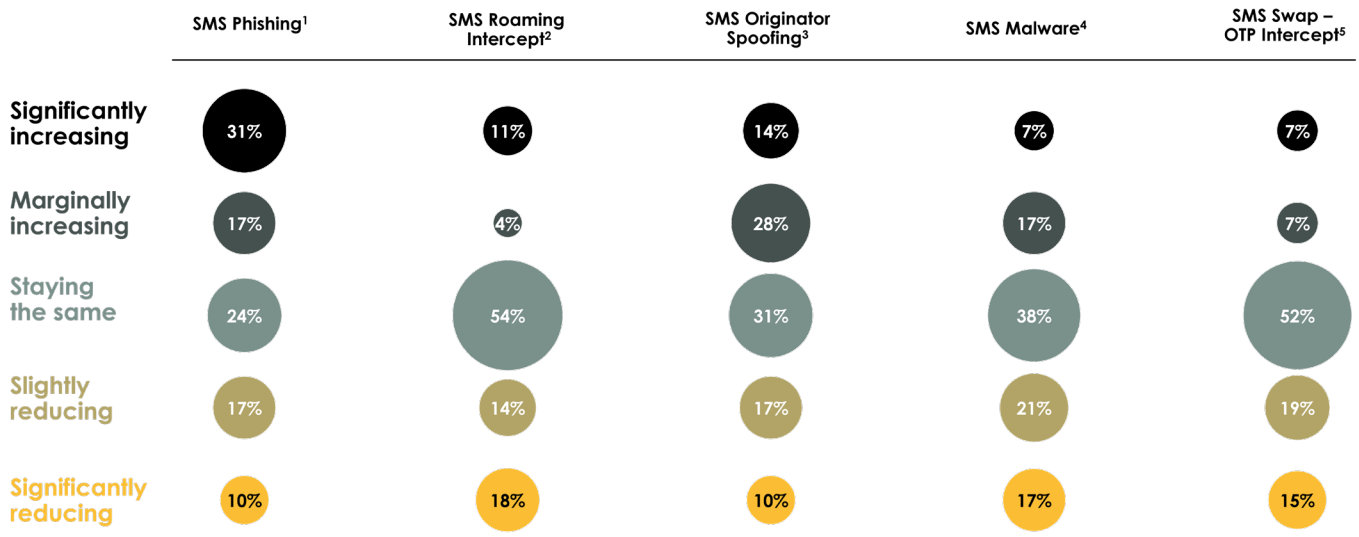
3. A2P (application to person) messages routed in P2P (person to person) routings

A less evident but no less concerning use case observed by some respondents is the detection of A2P messages in P2P specific routes. Since the different firewalls, reporting tools and prevention measures are well in place for A2P routing channels the impersonation or leakage of application-generated messages in a routing with different firewall rules may result in the failure to detect fraudulent traffic.

Results from the messaging Survey

The 12-month change in volume and impact of the messaging fraud cases shown in Exhibit 8 shows that the largest growth in messaging fraud use cases are SMS Phishing (smishing) with 48% of respondents seeing an increase and SMS Originator spoofing with 42% of respondents experiencing increases in their networks.

EXHIBIT 8: 12 MONTH CHANGE IN VOLUME AND IMPACT OF MESSAGING FRAUD USE-CASES



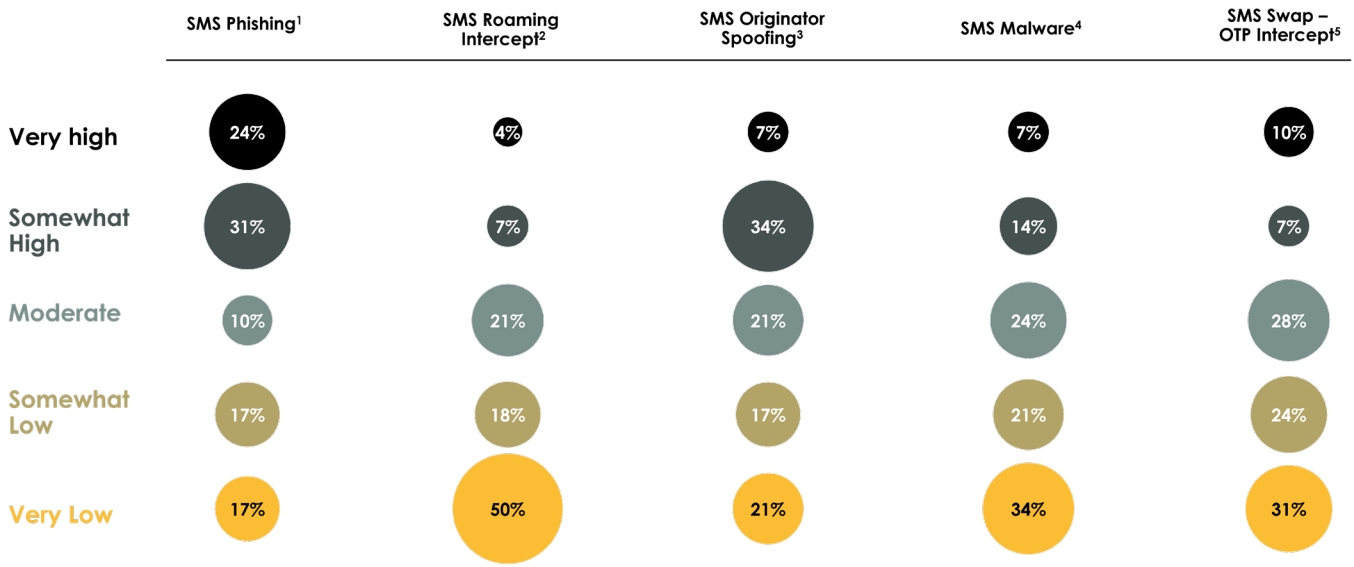
Notes: 1 Also known as "SMISHING" n=29, 2 n=28, 3 n=29, 4 n=29, 5 n=27; Omitted not answered; Source: GLF Survey 2022, Delta Partners Analysis

Moving into the assessment of the volume observed of fraudulent SMS traffic showcased in Exhibit 9, Phishing and Originator Spoofing take the lead with 55% and 41% of respondents seeing high volumes respectively, while Roaming Intercept and Malware are listed as the lowest in terms of traffic.

Carrier fraud teams have developed various processes and techniques such as pattern recognition in certain fraudulent messages, link verification and routing analysis. "Most fake messages have clear tell-tales that we can identify immediately", "our stringent firewall rules make it really simple to immediately detect suspicious messaging traffic and we continuously tweak and change them" mentioned some of the respondents. It is worth highlighting that in contrast to the voice volume assessment, more respondents observe a reduction in fraudulent messaging volumes. Extending on the financial impact assessment

EXHIBIT 9: ASSESSING THE VOLUME OF MESSAGING FRAUD USE-CASES

By use-case, what level of VOLUME are you experiencing? (from 1-5, with one being lowest and 5 being highest)
(% responses)



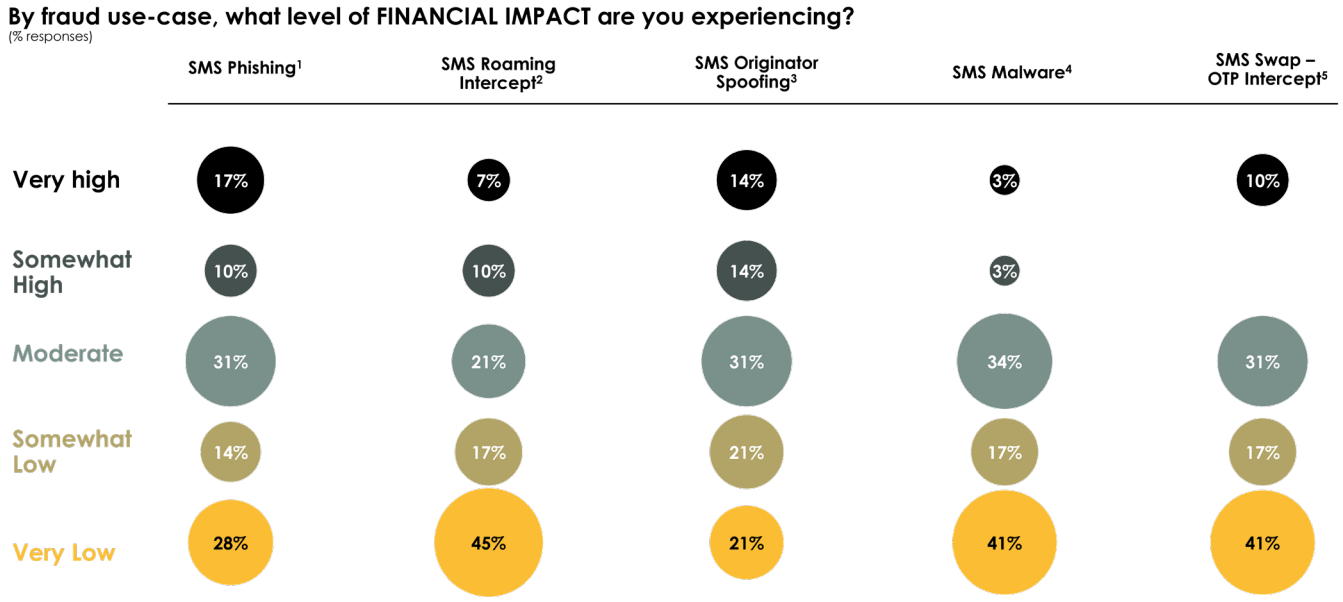
Notes: 1 Also known as "SMISHING" n=29, 2 n=28, 3 n=29, 4 n=29, 5 n=27; Omitted not answered; Source: GLF Survey 2022, Delta Partners Analysis

according to Exhibit 10, the highest financial impact is seen in SMS Phishing (27%) and SMS Originator Spoofing (28%), in line with the volumes observed in the previous exhibit.

In contrast with volumes showcased in Exhibit 9, the highest volume use cases have a relatively low financial impact, with 42% of respondents stating that SMS Phishing has a low financial impact as well as Originator Spoofing with 42%. In discussion with many carriers it was highlighted that the low direct financial effect that these types of fraud have in contrast to direct voice fraud is due to the fact that Phishing and Originator Spoofing are regarded as gateways to commit fraud vs. actual revenue loss, the financial impact is sometimes not directly felt by the carrier but by the consumer. It is this impact on the end-user that can generate reputational damage and lead to a degraded user experience.

"Our integrity of the network and to ensure the end-to-end protection of our customers is our priority" said one of the respondents when asked on the subject. This also highlights the importance of prevention measures such as end-user education. Effective education campaigns for end-users showing them how to be more alert to messaging fraud not only reduces the opportunities for a customer to be a victim, but it also creates a direct feedback loop with the carrier on how to further improve the prevention of such messages.

EXHIBIT 10: ASSESSING THE FINANCIAL IMPACT OF MESSAGING FRAUD USE-CASES

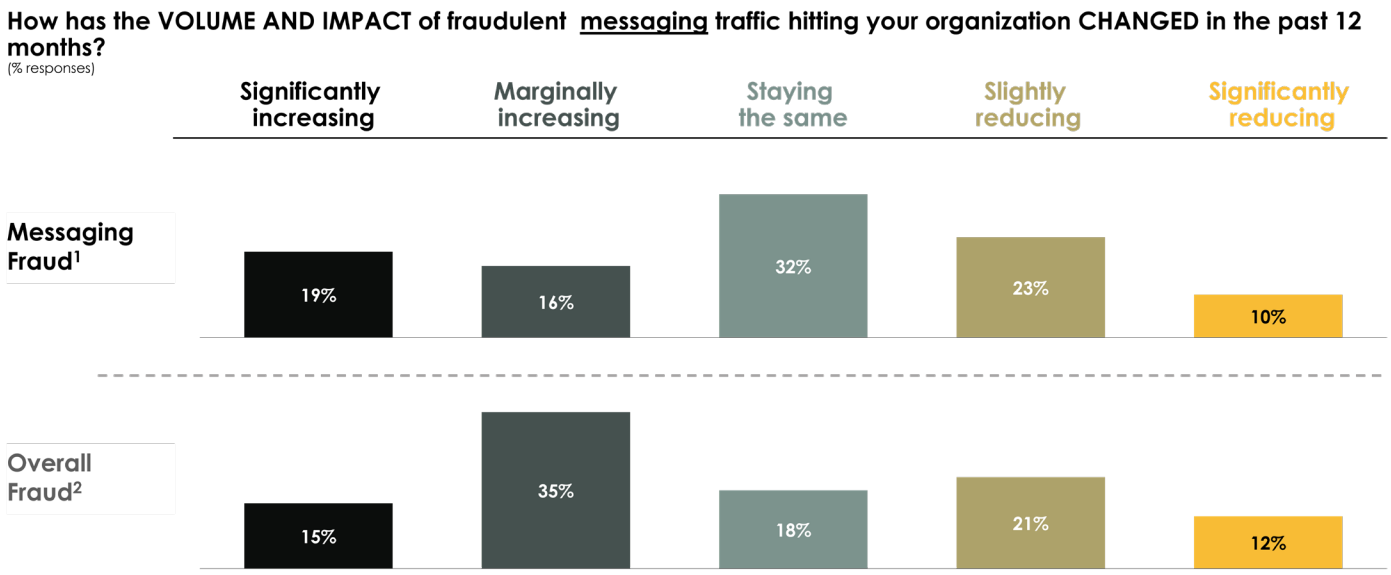


Notes: 1 Also known as "SMISHING" n=29, 2 n=28, 3 n=29, 4 n=29, 5 n=27; Omitted not answered; Source: GLF Survey 2022, Delta Partners Analysis

Contrasting Perception of Messaging and Voice Fraud

The data gathered in the 2022 GLF Fraud Survey allows us to compare the carriers' concerns on both voice and messaging fraud. When comparing in Exhibit 11 the overall volume and impact trend on both messaging and voice fraud, it is observed that besides 19% more respondents agreeing that overall fraud is marginally increasing there is no significant difference between the perspective of the carriers.

EXHIBIT 11: COMPARING MESSAGING FRAUD WITH VOICE FRAUD

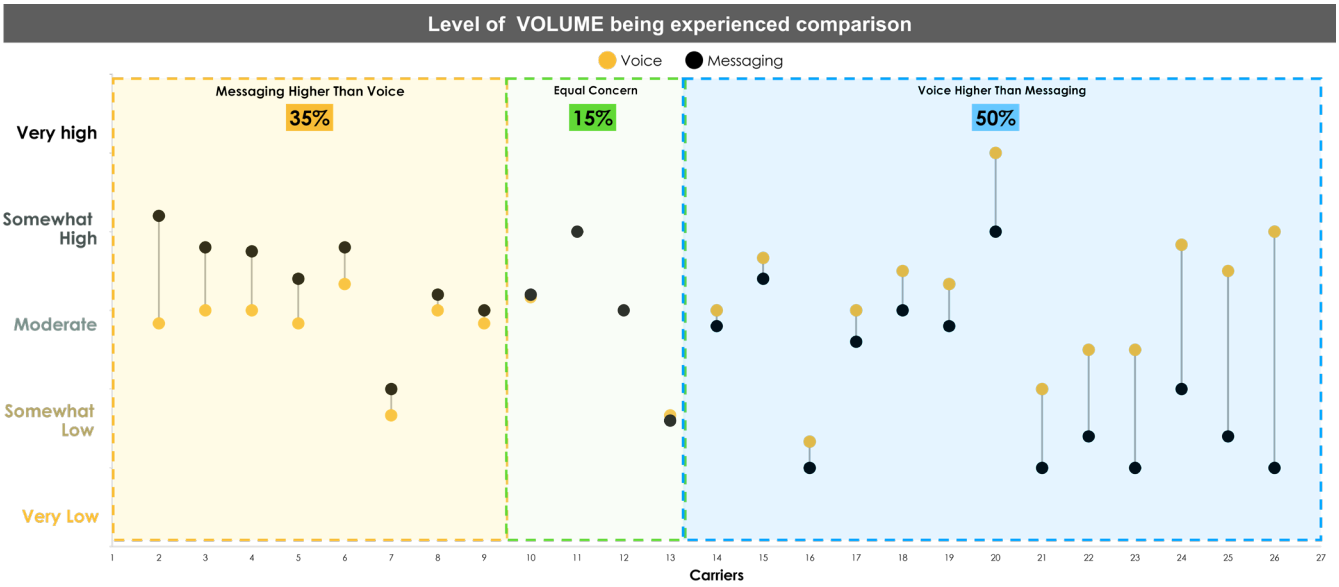


Notes: 1 n=31, 2 n=35; Source: GLF Survey 2022, Delta Partners Analysis

A further deep dive in the carrier-by-carrier responses on volume and financial impact concludes that there is no consensus on whether messaging or voice traffic is of higher concern, as shown on the total volume and financial impact of each carriers responses on both voice and messaging, illustrated in exhibits 12.1 and 12.2. Regarding the level of volume being experienced, 35% of carriers listed messaging fraud volume as a being higher overall than voice volume while 50% listed voice volume as being higher than messaging (15% listed having equal overall fraudulent volume). Regarding financial impact, 54% listed messaging as having higher impact while 46% listed voice as having a higher financial impact.

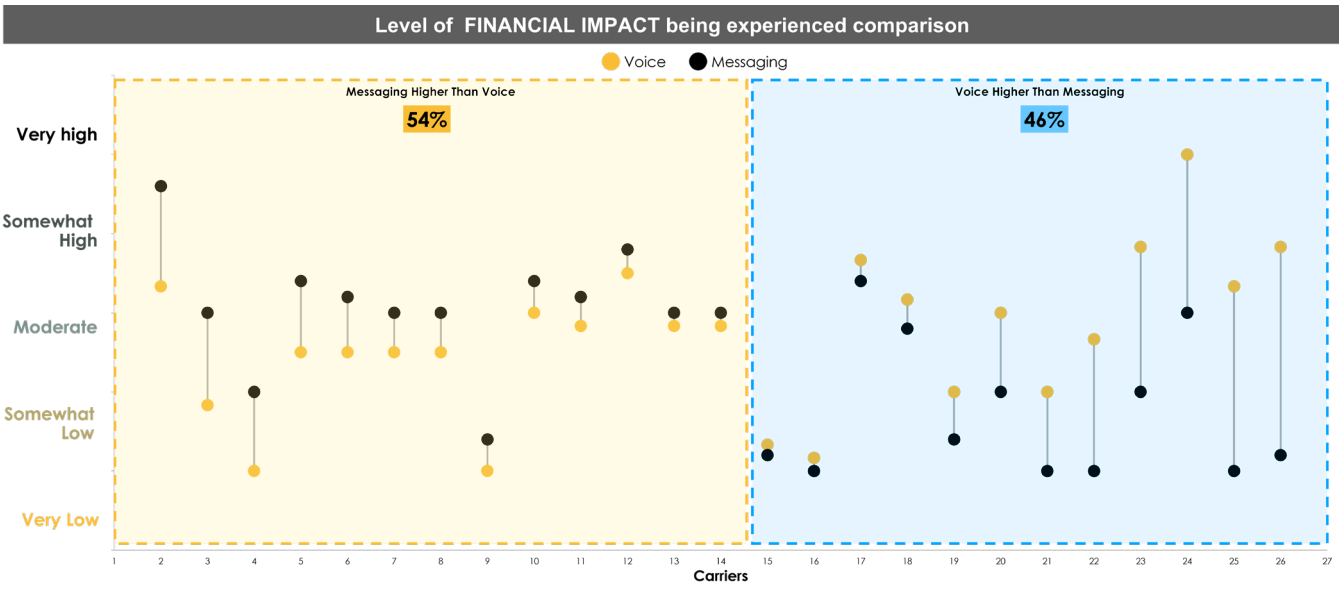
This could be explained by the fact that different carriers have different tolerance thresholds, in both volume and financial impact, that trigger automatic blocking. It is also worth adding that many respondents of the survey have a relatively new messaging product and are still in the process of deploying the proper detection and blocking tools to fully prevent fraud traffic in their networks.

EXHIBIT 12.1: COMPARING MESSAGING FRAUD WITH VOICE FRAUD – Individual responses



Notes: Source: GLF Survey 2022, Delta Partners Analysis

EXHIBIT 12.2: COMPARING MESSAGING FRAUD WITH VOICE FRAUD – Individual responses



Notes: Source: GLF Survey 2022, Delta Partners Analysis

Illustrating Regulatory Pressures on Fraud Management

The respondent carriers of the 2022 GLF Fraud survey operate in multiple jurisdictions covering five continents. Although the regulation varies significantly, most of the respondents listed common rules that fall under the Firewall prevention, Sender ID and Privacy categories.

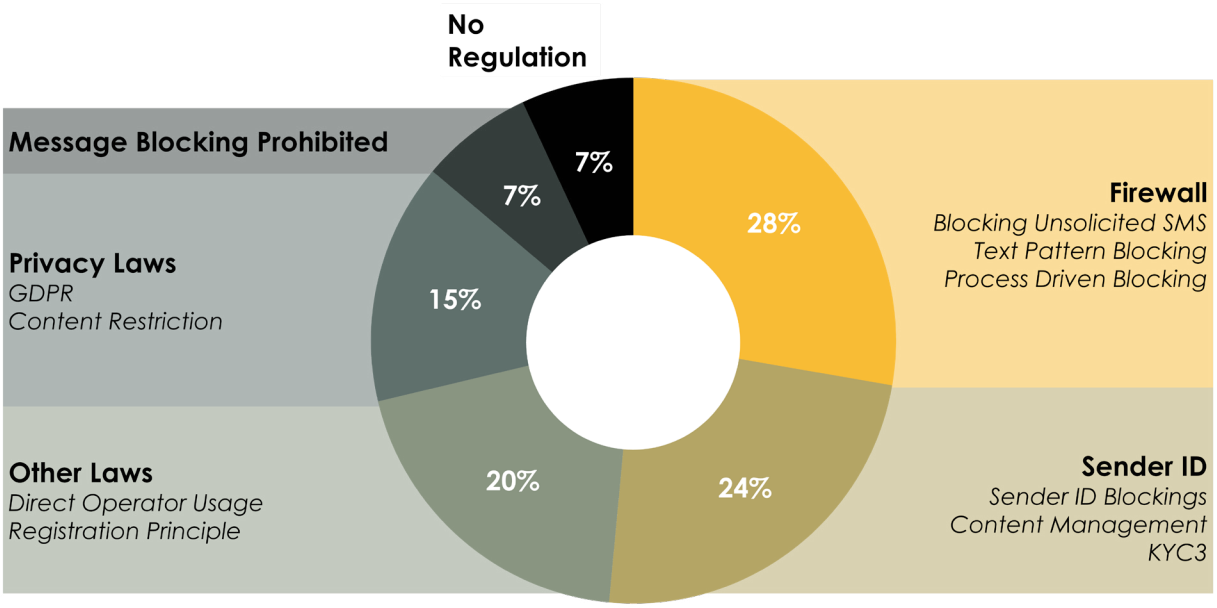
Feedback from the respondents has been varied as demonstrated in exhibit 13. While in some cases the enforcement of clear firewall rules assists the ecosystem via creating safety nets, in others privacy laws such as content restriction prevent carriers from obtaining and analysing suspicious message content.

Some respondents have seen success by analysing metadata and risky origin numbers, "we have never seen the privacy regulations as an obstacle, we have learned the patterns and metadata of fraudulent messages and we have been successful in detecting them while strictly adhering to privacy rules" stated one respondent.

A notable application of innovative messaging regulation is the Indian Telecom Regulator's (TRAI) Distributed Ledger for Bulk SMS messages. Businesses that wish to distribute bulk SMS register in an open distributed ledger which later validates every SMS message to go through the network. Although its initial operational period took some adjustment it shows that regulatory bodies can implement innovative technologies to further improve the health of the messaging ecosystem.

EXHIBIT 13: Regulatory Obligations for Messaging Traffic

What are the key regulator rule categories regarding messaging that you must adhere to in your market?
(% responses)



Notes: n=46; Source: GLF Survey 2022, Delta Partners Analysis

CONCLUSIONS

1. The messaging market represents a huge commercial opportunity for carriers and is therefore a very attractive market for fraudsters. The biggest concern throughout the community is the increased sophistication of SMS Phishing messaging. However, the implementation of strong prevention measures such as customer education and awareness campaigns, can enable use cases to be better prevented in comparison to voice fraud.

2. Although having a solid process to prevent messaging frauds such as a solid firewall has proven effective, regulatory innovations can push the ecosystem forward and can further help in the control of fraudulent traffic.

3. BEST PRACTICES PUT TOGETHER

Building and Scaling Fraud Teams: A directive that translates to action.

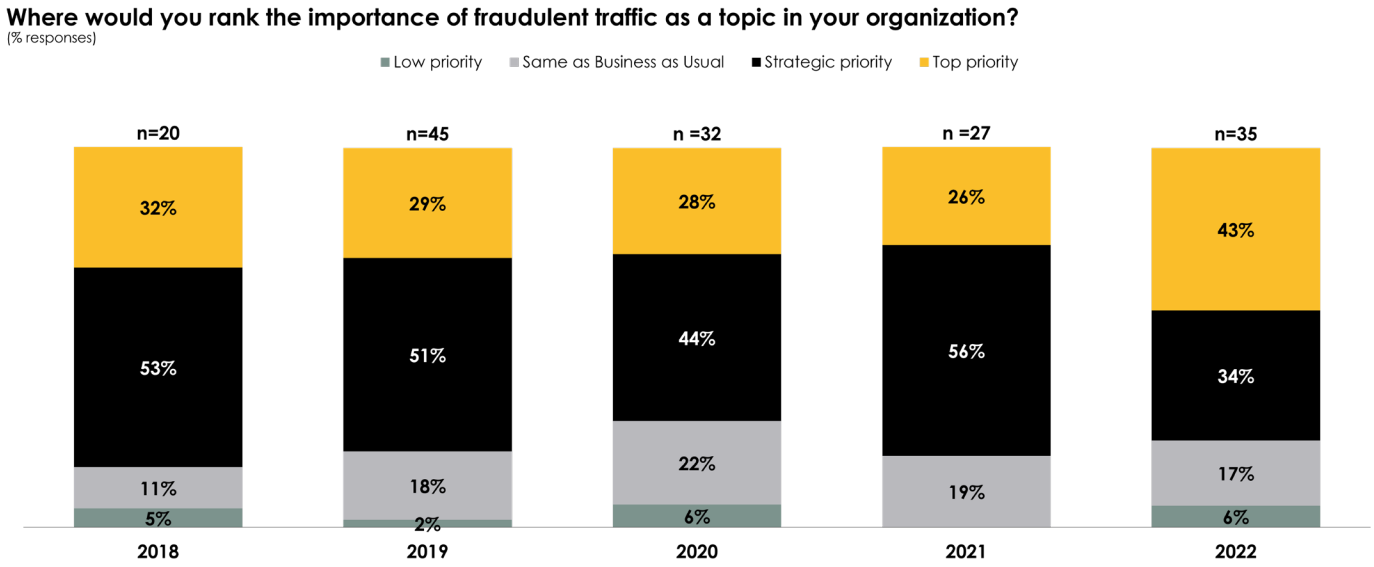
Over the past two years, fraud prevention has received an overall increase in interest from all levels inside carrier organisations.

Respondents noted that thanks to collaborative spaces and awareness programmes, anti-fraud measures have garnered increased visibility from all levels of the organization, including leadership. Some explained that: "We have been increasing our metrics reporting to top management, as well as being more involved with new product teams to make the next generation offering fraud-proof" as well as "There has been an increase in interest of how we manage revenue risk and how healthy is our business with different players" stated two respondents.

This heightened interest has been reflected in the data, Exhibit 14 showcases the evolving importance of fraudulent traffic in the respondent's organization. 43% of the respondents see fraudulent traffic as a top priority in their organization, an increase of 17pp in comparison to 2021. All respondents from the 2021 survey have answered that either the importance of fraudulent traffic has increased or has stayed the same.

The 6% of respondents that answered that the importance is a low priority represent carriers new to the GLF Fraud Report who are familiarising themselves with the GLF's anti-fraud process. The progress of these new carriers will be monitored in the following years to see their progress and the GLF welcomes more carriers to join this critical cross-industry initiative.

EXHIBIT 14: COMPARING IMPORTANCE OF FRAUDULENT TRAFFIC IN CARREIRS

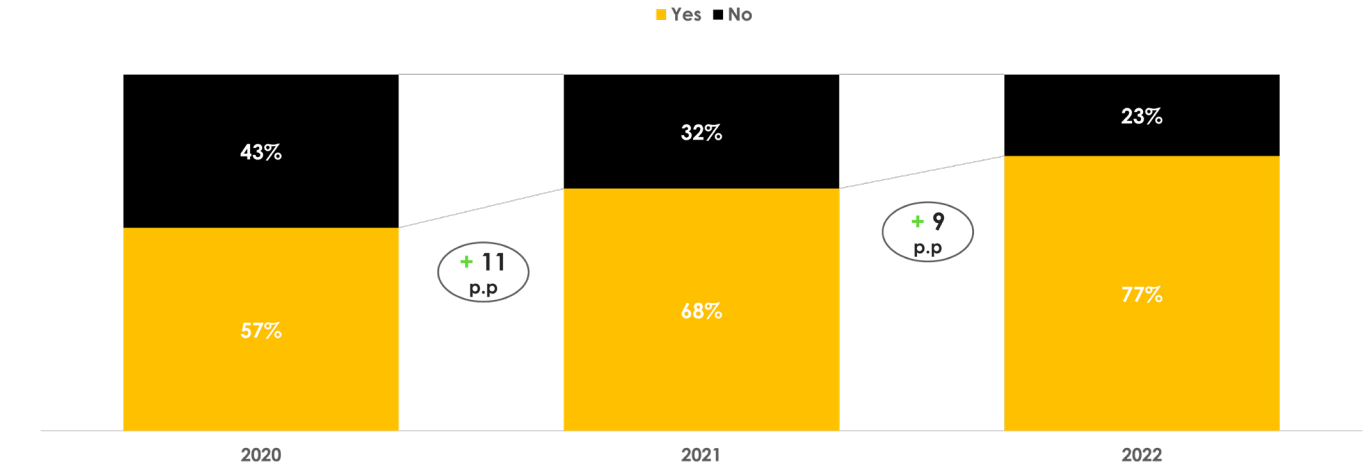


Notes: Respondents without a response more not counted; Source GLF Survey 2019-2020-2021-2022, Delta Partners Analysis

According to the data showcased in Exhibit 15, 77% of respondents see an increase in investment in fraud monitoring and prevention infrastructure for next year. When probing on this topic, respondents mostly answered that the priorities for the next couple of years is to make investments into process automation and refining fraud tools. By automating most of the reporting processes "my team members can spend more time further developing their knowledge of new trends instead of reviewing the tools for alerts" as one respondent mentioned. Another point illustrated by Exhibit 15 is that irrespective of the respondent's importance ranking, GLF members are investing more in their fraud infrastructure. These investors include the 9% that responded, "same as BAU priority" and the 6% that responded "low priority".

EXHIBIT 15: INVESTMENT OUTLOOK IN FRAUD

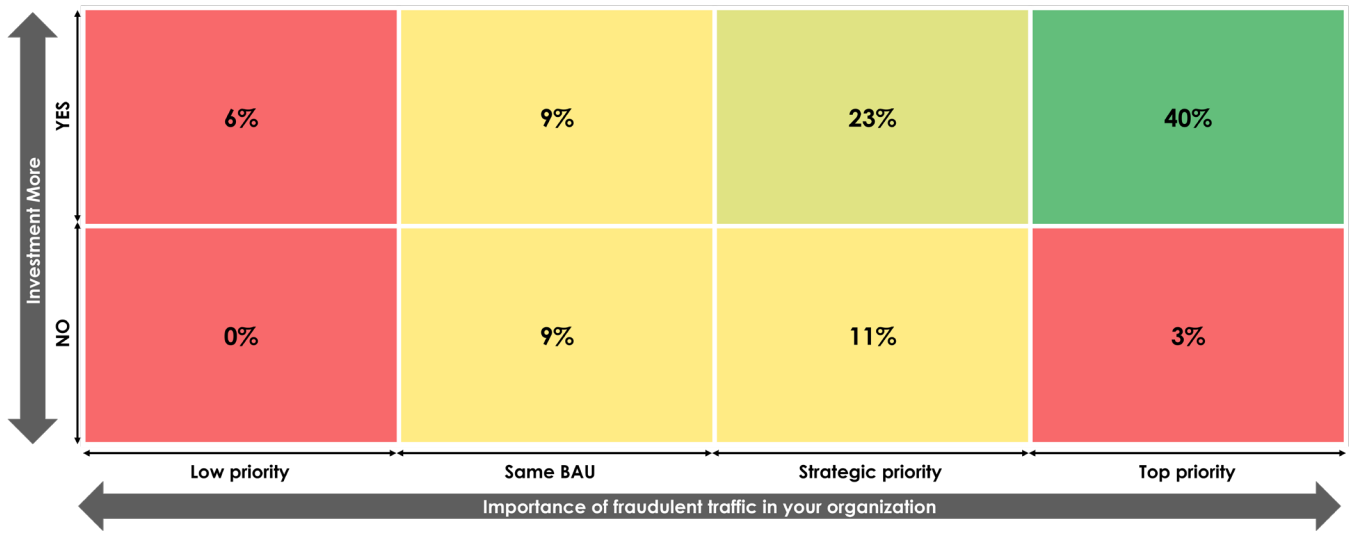
Do you foresee investing more in fraud monitoring / prevention infrastructure in the next 12 months?
(% responses)



Notes: 2020=n=28, 2021=n=25; 2022=n=35; Source: GLF Survey 2020-2021-2022, Delta Partners Analysis

EXHIBIT 16: COMPARISON OF FRAUD PRIORITY AND INVESTMENT

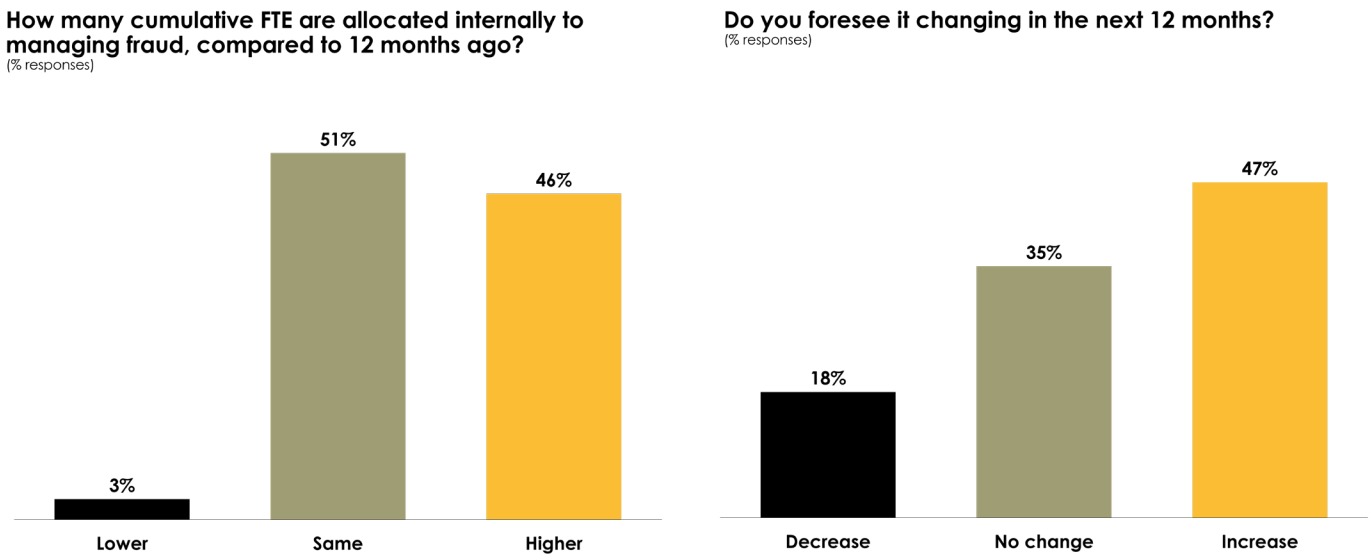
Do you foresee investing more in fraud monitoring / prevention infrastructure in the next 12 months?
(% responses)



Notes: 2020=n=28, 2021=n=25; 2022=n=35; Source: GLF Survey 2020-2021-2022, Delta Partners Analysis

This increase in investment also translates into the growth of FTEs assigned to the fraud team. As showcased in exhibit 17, although the majority (51%) of respondents have stated that their fraud teams have not grown, 47% plan to increase the FTEs assigned to their fraud teams.

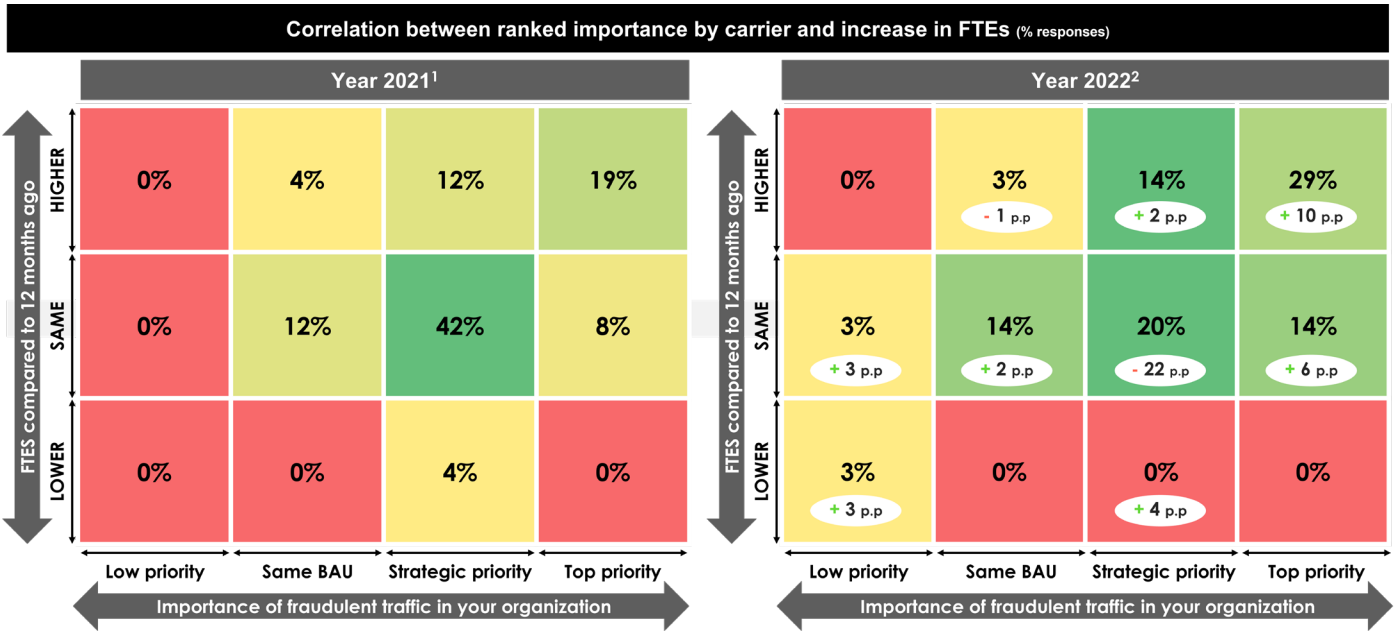
EXHIBIT 17: EVOLVING THE RESOURCE ALLOCATED TO MANAGE FRAUD



Notes: n=34; Source: GLF Survey 2022, Delta Partners Analysis

The data also indicates a clear correlation between the strategic priority of the respondent carrier and the resource allocation of FTEs in the fraud team. As shown in Exhibit 18, carriers that list fraudulent traffic as a 'Strategic' or 'Top' priority intend to increase their FTEs (14% of respondents in strategic priority and 29% of respondents in top priority). When compared to the same correlation done in the 2021 GLF report, more members of the 2022 group of strategic or top priority responders are intending to grow the FTEs assigned to their teams. In contrast, 3% of carriers that answered low priority are intending to decrease their fraud teams showing that even in low priority cases a reduction of FTE allocated to fraud is not in plan.

EXHIBIT 18: MAPPING CHANGES IN RESOURCE ALLOCATION AND FRAUD PRIORITY IN A CARRIER



Notes: 1 n=35,2 n=21, it excludes "non answered"; Source: GLF Survey 2022-2021, Delta Partners Analysis

Anti-fraud innovation within carriers is also driving organisational change. Carriers have evolved both their fraud detection tools and processes and their fraud team's structure. Many have experimented outside of the conventional structure of fraud teams and have applied different management models. Some interesting case studies from respondents include:

1. **Carrier 1:** Distributed responsibility, every member in the revenue value chain has access to Fraud management system and has own metrics for their part of the process. No exclusive fraud teams.
2. **Carrier 2:** Besides core fraud team, fraud members are active members in different areas such as new product & service development (fraud-proof by design) and as contact points with authorities.
3. **Carrier 3:** Extensive and documented technical due diligence process for new customers. Developed minimum technical standards to connect to the network and allow for smooth flow of data through the fraud management system.

Diving into the different organisational structures of the carriers' fraud teams there was a notable separation of teams, processes, and information flows between teams in charge of monitoring voice traffic and teams in charge of monitoring messaging traffic. As the nature of fraud keeps changing, teams must have the agility to receive and act on information that is generated in their own organisation. Thus, teams need to be more targeted on combining efforts and knowledge, finding synergies and unifying priorities. This unification of efforts can result in a faster identification of bad actors, more efficient correlation of origin/destination pairs and fraudulent traffic and an increase in data flows used to calibrate and improve the anti-fraud tools. As mentioned by one of the respondents "we are now actively looking to combine our efforts, our recent interactions finding common bad actors had made us realize the lack of coordination both our teams had, and we are definitely improving it".

As carriers grow fraud teams, the hunt for talent to fill the positions has become more complex. Respondents highlighted that candidates must have strong analytical skills in addition to anti-fraud experience and knowledge. This gap in market skills could be addressed by collaborating in training, awareness, and talent development in order to educate and prepare the next generation of anti-fraud teams.

CONCLUSIONS

1. A constantly growing strategic priority in fraud prevention does translate into an increase of both manpower and infrastructure resources for fraud teams to be more precise and efficient.
2. Fraud teams are constantly innovating in organisational structures, processes, and technological tools in order to increase agility, capabilities, and coverage.

GLF's Role in fraud prevention

The GLF and its members are active warriors in the collective fight against fraud. It has enabled productive collaborations to increase awareness of fraud and anti-fraud best practice across the industry in addition to providing a platform for members to openly participate and share key knowledge.

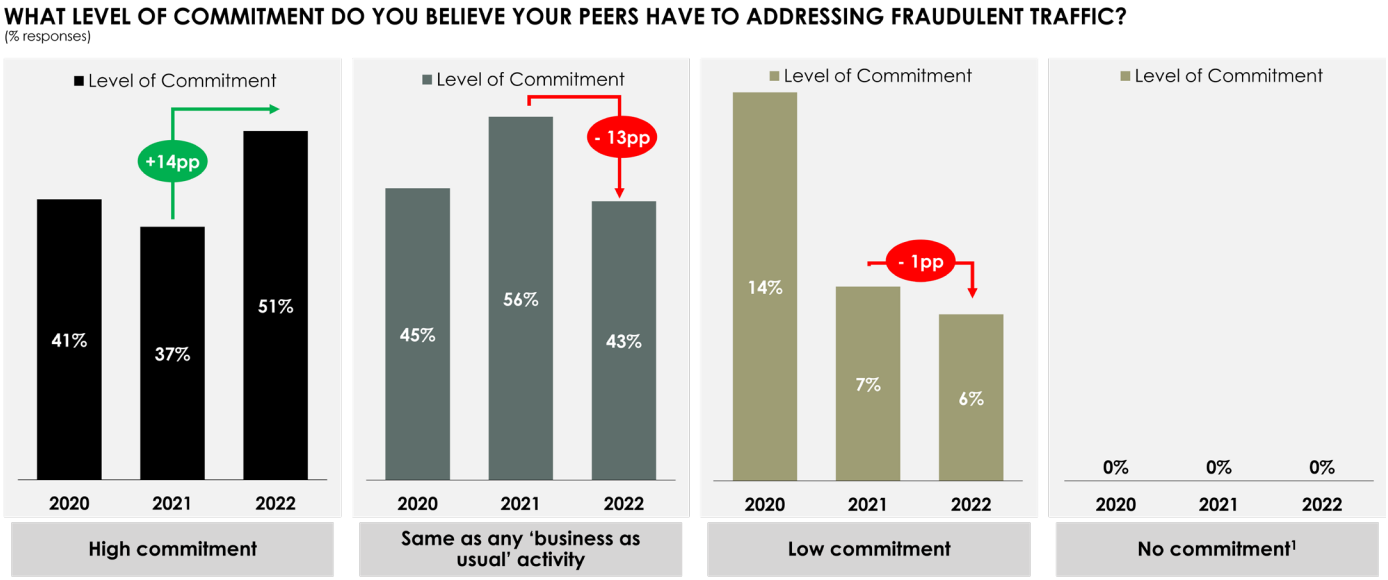
The GLF has also been an active participant in gathering and sharing the overall perspective of the community. For five years now the GLF Fraud Report has tracked industry trends and enabled the community to distribute knowledge on the evolution of fraud and areas for collective focus.

Besides the publication of insights gathered from the community, since 2018 the GLF in collaboration with the i3 forum has created and distributed a Code of Conduct that delineates the best practices a carrier should adopt and adhere to in order to minimise fraudulent traffic. In 2020, GLF members agreed to implement a Code of Conduct Adherence Process in which each carrier member's adherence to the six principles outlined in the code of conduct was evaluated through an evidence-based, self-attestation survey. This process has set up a framework to evaluate how members of the community translate intentions of fighting fraudulent traffic into actions within their daily operations.

Although progress remains to be made carriers recognise the efforts made as an industry. Exhibit 19 showcases that 51% of respondents believe peers have a high commitment of addressing fraudulent traffic, an increase of 14pp from the 2021 Survey. As mentioned by many of the respondents, collaboration spaces and initiatives such as the ones led by the GLF create opportunities where "we can confidently know that our goals as a community are aligned" and "allow for members of different teams to share best practices, techniques and be constantly educated on how to best improve our work".

Besides knowledge sharing, initiatives such as the fraud report have increased awareness of the severity of the fraud problem many carriers still face. From

EXHIBIT 19: PERCEPTION OF PEER COMMITMENT TO FIGHTING FRAUD



Notes: : 1: No answers ; 2020=n=29,2021=n=27,2022=n=35; Source: GLF Survey 2020,2021,2022 Delta Partners Analysis

an internal perspective, awareness of the problem has aided top level decision makers in companies to increase the priority and reporting of fraudulent activity within the organisation. Externally increased visibility and awareness aids external parties such as regulatory bodies to be better informed when designing effective policies and regulations in order to prevent and reduce fraud within their jurisdictions.

Although positive progress has been made, more remains to be done. Suggestions from respondents for new collaborative initiatives include:

a. Increase commitment to share information on bad actors (Blacklisted numbers, suppliers, and originators).

b. Training spaces for new methodologies/procedures to detect new types of fraud.

c. Agree on a list of uniform KPIs or metrics to measure self-performance of carrier fraud teams.

d. Create a "Peer Review process" to sit alongside the existing attestation of compliancy against the Code of Conduct to ensure a more robust and vigorous approach to anti-fraud activities.

PART 2

ADHERING TO THE GLF CODE OF CONDUCT 2022

Code of Conduct attestation process

1

The code of conduct established in 2018 sets the benchmark of behaviour that carriers should seek to attain to ensure that there is consistent action taken across the industry to fight against fraudulent traffic. It is broken down into **6 principles** related to targets and reporting, processes, destinations, payment flows, information sharing and contracting.

2

The attestation process kicked off in 2021 requires that participants prove their adherence to each of the six principles. To be compliant carriers must score over 70% in each of the six principles and provide evidence for their responses. Of the carriers that participated in the 2021 attestation process, **39% made improvements to their practices** improving their score, principally in the efforts made to roll out anti-fraud clauses in their new and existing contracts to comply with i3 forum standard anti-fraud clauses.

1. WHY CODE OF CONDUCT ATTESTATION MATTERS

In 2018, the ITW Global Leaders Forum worked alongside the i3 Forum to create a Code of Conduct which international carriers could sign-up to demonstrate their commitment to fighting against fraudulent traffic. As of September 2022, more than 30 carriers have signed up.

EXHIBIT 20: GLF CODE OF CONDUCT SIX PRINCIPLES

Principles	
1	Targets for prevention of fraudulent traffic to be included within management reporting
2	Carriers to adhere to i3 Forum recommended processes to detect and avoid fraud
3	Identified fraudulent number ranges and destinations to be blocked
4	All reasonable action to be taken to avoid payment flows to the instigators of fraudulent traffic
5	Commitment to share information regarding fraudulent traffic flows with carrier peers
6	Adoption of standard contracting terms addressing fraudulent traffic management

Source: GLF 2018

In 2020, GLF members agreed that commitment to the Code of Conduct should progress beyond purely stating public support – their adherence to the principles should be assessed. As such, in the 2020 GLF Fraud Report, a process was undertaken to test carriers' adherence. This was achieved by answering a survey that asked questions about carriers' actions with regards to the six principles. Given 2020 was the first year such an activity took place, it was agreed that whilst individual carriers would have access to their own results benchmarked against the anonymized and aggregated industry data set, no announcement of which carriers were "compliant" would be made.

In 2021, it was agreed by GLF members that the names of the carriers that were attested as 'compliant' on all six Principles would be published. In total 19 carriers attested compliant in the 2021 code of conduct attestation process, 83% of the carriers surveyed in the exercise.

In 2022, 23 carriers participated in attestation process, including three new carriers that had not previously responded. The data showed that whilst there was a high level of compliance across principles, there was still work to be done to ensure consistency across all six principles above high threshold levels based on the findings from the 2021 attestation process.

2. THE PROCESS OF ATTESTATION

This year the GLF has repeated the attestation process, using a consistent methodology to 2021.

The process for the Code of Conduct attestation had the following five steps:

EXHIBIT 21: CODE OF CONDUCT ATTESTATION PROCESSS

To be "compliant" a carrier must:

1. Score over 70% in each of the six principles within the attestation
2. Provide evidence that the GLF team views satisfactory to demonstrate adherence

In addition to the self-attestation survey, each carrier must submit evidence proving their adherence to each principle in the attestation process. Documentation of the fraud management system, internal documents regarding different processes and evidence of alerts and reports are required from each of the respondents. To compliment the survey and evidence submission, an interview with the carrier fraud teams takes place to further elaborate on the evidence provided, clarify points and to keep an open dialogue with each of the members.

The purpose of the attestation process is to promote the carriers that are actively working to stop fraudulent traffic. It does not seek to publicly accuse carriers of failing to be compliant with the Code of Conduct. As such only the names of the compliant carriers are publicly announced. No full list of carriers that either submitted data but were not compliant or declined to participate in the process is announced.

This report represents the second announcement of Code of Conduct compliant carriers. The GLF hopes that this process attracts additional carriers from across the industry to publicly demonstrate to their customers, suppliers, and peers the stance and actions taken against fraudulent traffic.

GLF recognises the potential limitations of such a self-attestation process as the provision of data points and survey responses could be manipulated to seek a specific outcome. However, through the deep engagement with the participating carriers, GLF trusts that the information provided has been done so truthfully and with the right intentions. As both GLF and the participant carriers are familiarised with the process, further action is evaluated to make the process more robust and increase the involvement of members of the community to collaborate and learn how to apply best practices on preventing fraud.

3. COMPLIANT CARRIERS FOR 2022

GLF confirms that the following 20 carriers are compliant with the GLF Fraud Code of Conduct:

* Special Acknoledgement

The GLF welcomes MTN GlobalConnect as a new compliant carrier for the 2022 process. As the code of conduct attestation process continues to drive momentum and become increasingly important to the industry. Carriers utilise the process as a self-evaluation for the performance of their anti-fraud operations and the GLF believes the increased awareness will further progress the overall community involvement to prevent the effects of fraudulent traffic. To-date participation within the process has enabled GLF members to identify areas for improvement, increase investment in FTE and fraud management systems in addition to supporting the fraud team's visibility to senior management.

Additionally we acknowledge the carriers that provided robust documented and live evidence in this year's process, further reassuring their intent to not only comply with the principles of the Code of Conduct but also putting them into practice. The GLF calls on all members of the attestation process to further collaborate with the process by delivering robust evidence on how the principles detailed in the code of conduct are put into practice.

When the carrier compliance is reviewed against minimum scores required to demonstrate compliance on each principle some differences could be observed from the 2021 Attestation process, showcased in Exhibit 19. At the listed 70% threshold for compliance, we see an increase in carriers that fully comply with both the contracting clauses listed in principle 6 and the reporting initiatives listed in Principle 5, an increase of 8 p.p and 4 p.p is observed. On the other hand, the changing priorities of the participant's carriers anti-fraud teams such as the frequency of reporting, depth of information reported and blocking thresholds of some participants resulted in a different level of compliance in comparison to last year.

EXHIBIT 22: TABLE OF CARRIERS' COMPLIANCE AT DIFFERENT THRESHOLDS

2022	Number of compliant Principles					
Threshold	**6**	**5**	**4**	**3**	**2**	**1**
100%	26%	30%	70%	74%	9%	78%
90%	26%	48%	87%	87%	65%	83%
80%	78%	83%	87%	96%	91%	87%
70%	91%	91%	87%	96%	96%	100%
60%	91%	91%	91%	96%	96%	100%
50%	96%	91%	91%	96%	96%	100%

2021	Number of compliant Principles					
Threshold	**6**	**5**	**4**	**3**	**2**	**1**
100%	0%	17%	30%	65%	78%	87%
90%	17%	52%	78%	87%	87%	100%
80%	52%	78%	87%	87%	100%	100%
70%	83%	87%	91%	96%	100%	100%
60%	87%	91%	96%	96%	100%	100%
50%	87%	91%	96%	100%	100%	100%

Note: n = 23; Source: Code of conduct survey 2022, Delta Partners Analysis

4. ANALYSIS OF THE ATTESTATION DATA

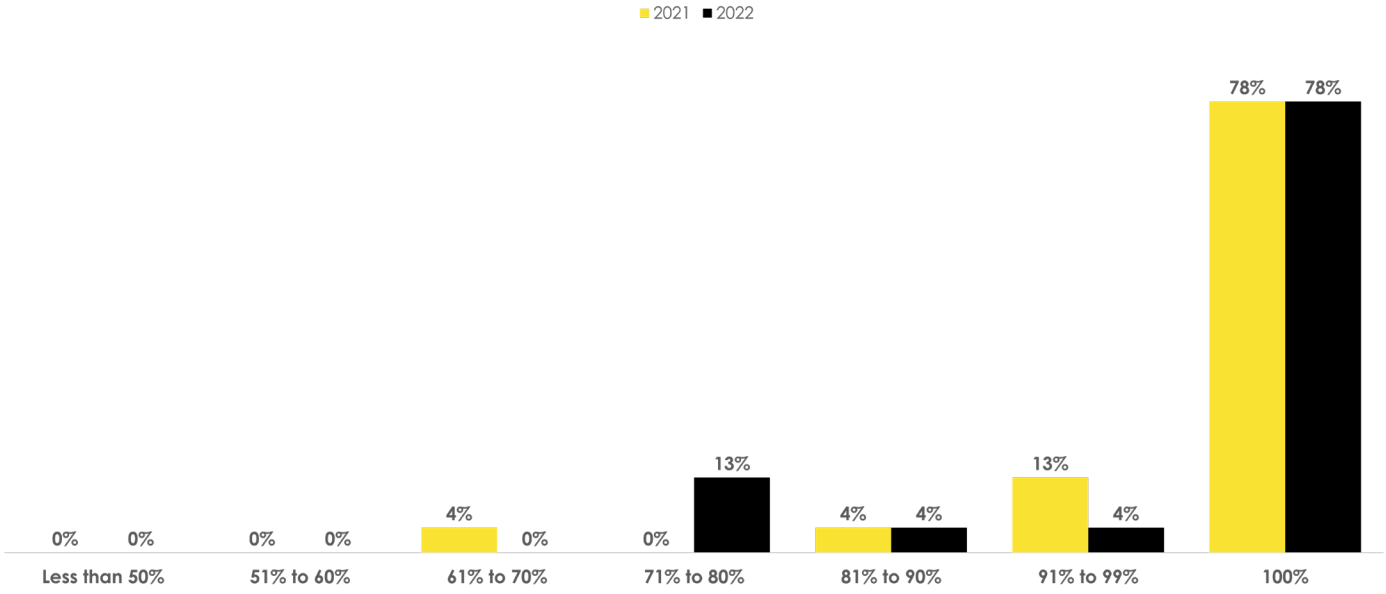
Principle 1 – Targets

Targets for prevention of fraudulent traffic to include within management reporting.

The same 78% of carriers attested 100% compliant in 2021 and 2021. Overall, Principle 1 showed the highest level of compliance of all the six principles. 100% compliance means that these carriers are:

1. Providing management teams with reports on at least a monthly basis regarding issues including the number of fraud alerts, blocked traffic, and disputes.
2. Updating the directly responsible executive for the international wholesale business on at least a monthly basis regarding the instances of fraudulent traffic.
3. Ensuring that fraudulent traffic reports and information are directly shared and/ or included in fraud-specific meetings (as opposed to being parts of wider agendas).

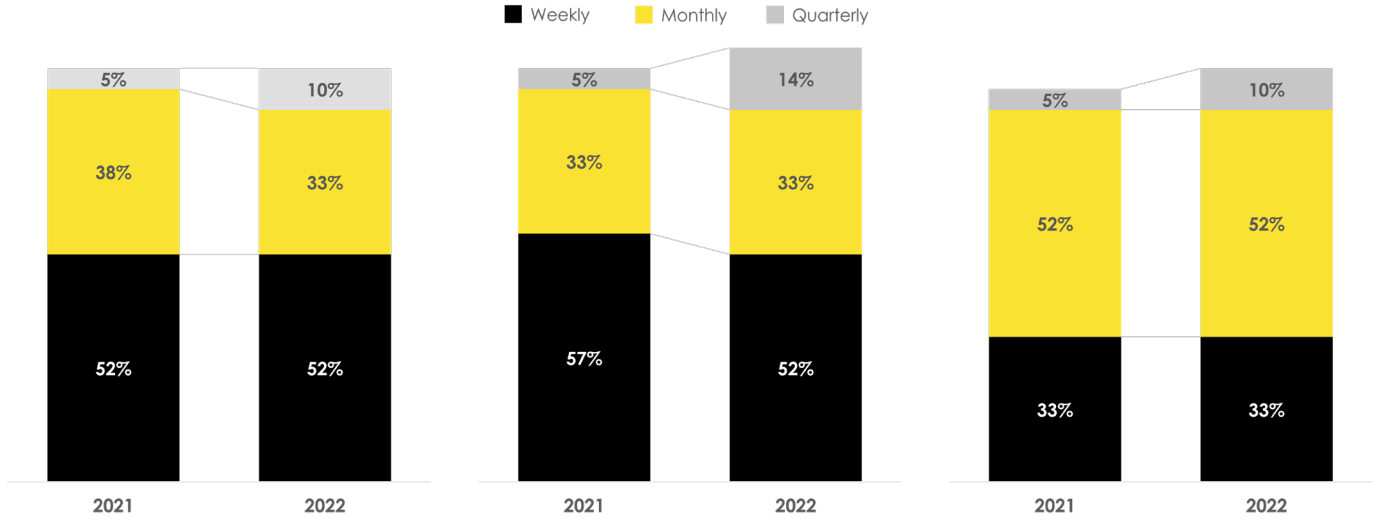
EXHIBIT 23: DISTRIBUTION OF CARRIER COMPLIANCE TO PRINCIPLE 1 – REPORTING 2021 - 2022



Note: 2022 = n = 23, 2021 = n = 23; Source: Code of conduct survey 2022 & 2021, Delta Partners Analysis

An observed trend regarding the frequency of reporting was a change in the frequency and content of the reports generated by the fraud teams. The data showcased in exhibit 24 states an increase of quarterly reports in fraud alerts, blocked traffic reports and fraud disputes while showing a decrease in monthly and, in the case of blocked fraud traffic, weekly reporting. In conversations with respondents that stated a reduction in their reporting frequency they mentioned that this originated from senior management requests to have less frequent but more informationally dense reports.

EXHIBIT 24: FREQUENCY OF FRAUDULENT TRAFFIC REPORT DISTRIBUTION 2022 vs 2021



Note: n = 23; Source: Code of conduct survey 2022 & 2021, Delta Partners Analysis

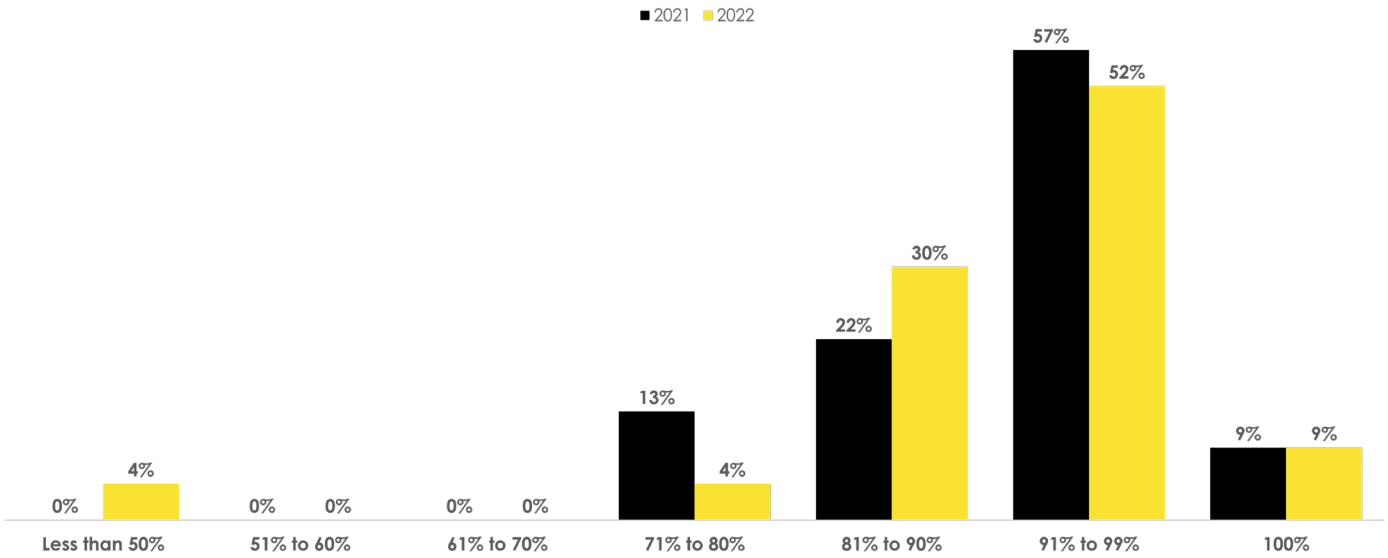
Principle 2 – Processes

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

Overall, carriers demonstrated a high adherence to Principle 2 – Processes, with 52% scoring over 90% compliance. Full compliance to Processes means that carriers:

1. Have a near real-time fraud prevention system or platform that detects and alerts customers when suspicious traffic arises.
2. Have a team of more than one FTE with direct responsibility for monitoring the fraud prevention system.
3. Have real-time end-to-end processes covering from detection to reporting regarding fraudulent activity.
4. Can implement actions immediately upon detection, including notifying the supplier, notifying the customer, reporting to police/ law enforcement, notifying internal account managers, and blocking the suspected number ranges.

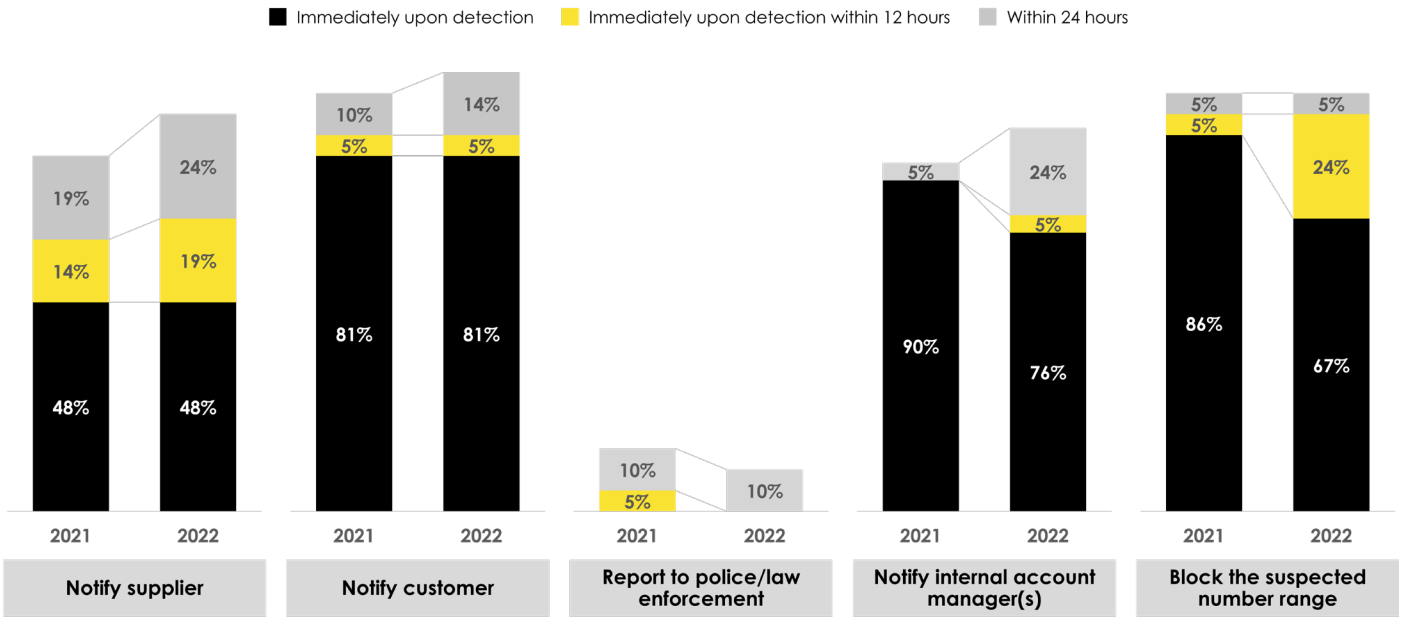
EXHIBIT 25: DISTRIBUTION OF CARRIER COMPLIANCE TO PRINCIPLE 2 – PROCESSES 2022 vs 2021



Note: 2022 = n = 23 ; 2021 = n = 23; Source: Code of conduct survey 2021 & 2020, Delta Partners Analysis

In some cases, the speed of reporting has changed due to management preferring less frequent but more complete reporting. Highlighted by several respondents and showcased in exhibit 26 was the fact that the ability to report to police/law enforcement varies by jurisdiction. In some countries the regulation does not allow the carrier to report fraud directly. This further highlights the issue of creating an industry-wide standard to interact with law enforcement authorities in different jurisdictions. Additionally, there was a notable decrease in the speed of reporting blocked of suspicious number ranges with 67% immediate report upon detection, down from 86% in 2021.

EXHIBIT 26: PRESENCE AND SPEED OF FRAUD PROCESSES 2022 vs 2021



Note: n = 23; Source: Code of conduct survey 2022 & 2021, Delta Partners Analysis

Principle 3 – Destinations

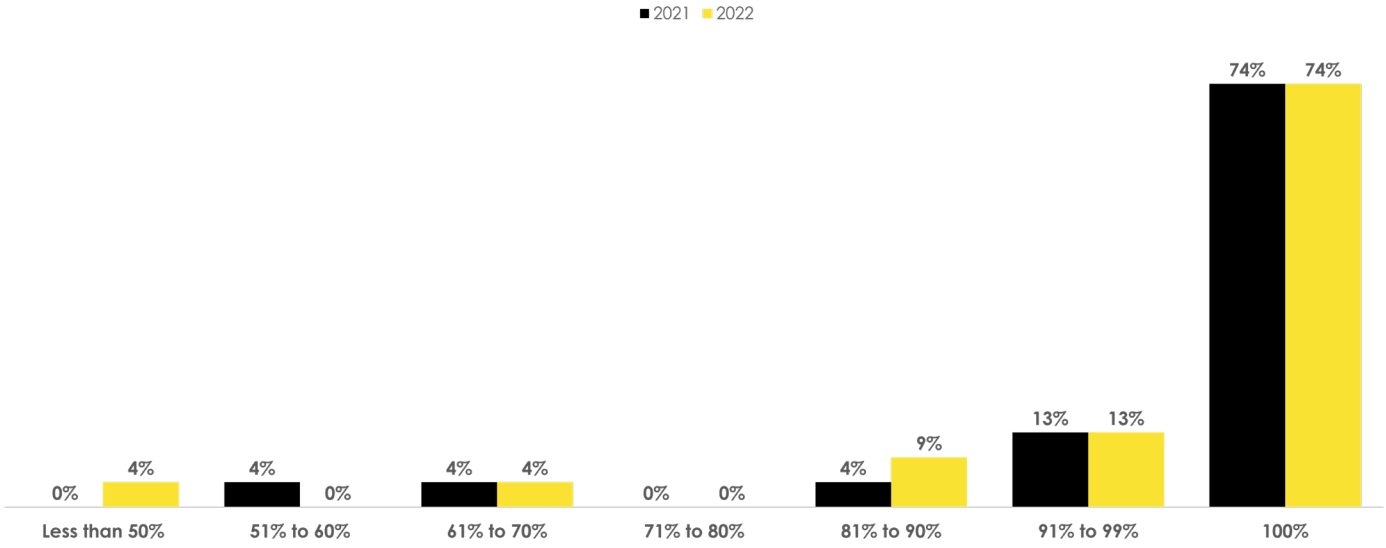
Destinations Identified fraudulent number ranges and destinations to be blocked.

Whilst Principle 1 and Principle 2 focus on the reporting of fraud instances and initiating processes on the identification of fraudulent traffic, Principle 3 relates to taking specific action – blocking fraudulent number ranges and destinations. 70% of carriers reported 100% compliance with this principle meaning that:

1. Where contractually and legally permitted, they immediately block B-number ranges and destinations for wholesale traffic.
2. Where contractually and legally permitted, they immediately block A-number ranges and destinations for wholesale traffic.
3. They have a standard written process to identify fraudulent number ranges.

The 4 p.p reduction in the 51% to 60% compliance from the survey came from the adjustment in the speed of blocking and the number of times the carrier decided to block different number ranges. In conversations with carriers this happened due to a change in the blocking thresholds of their tools and contractual requests from some of their customers.

EXHIBIT 27: DISTRIBUTION OF CARRIER COMPLIANCE TO PRINCIPLE 3 – DESTINATIONS 2022 vs 2021



Note: 2022 = n = 23 ; 2021 = n = 23; Source: Code of conduct survey 2021 & 2020, Delta Partners Analysis

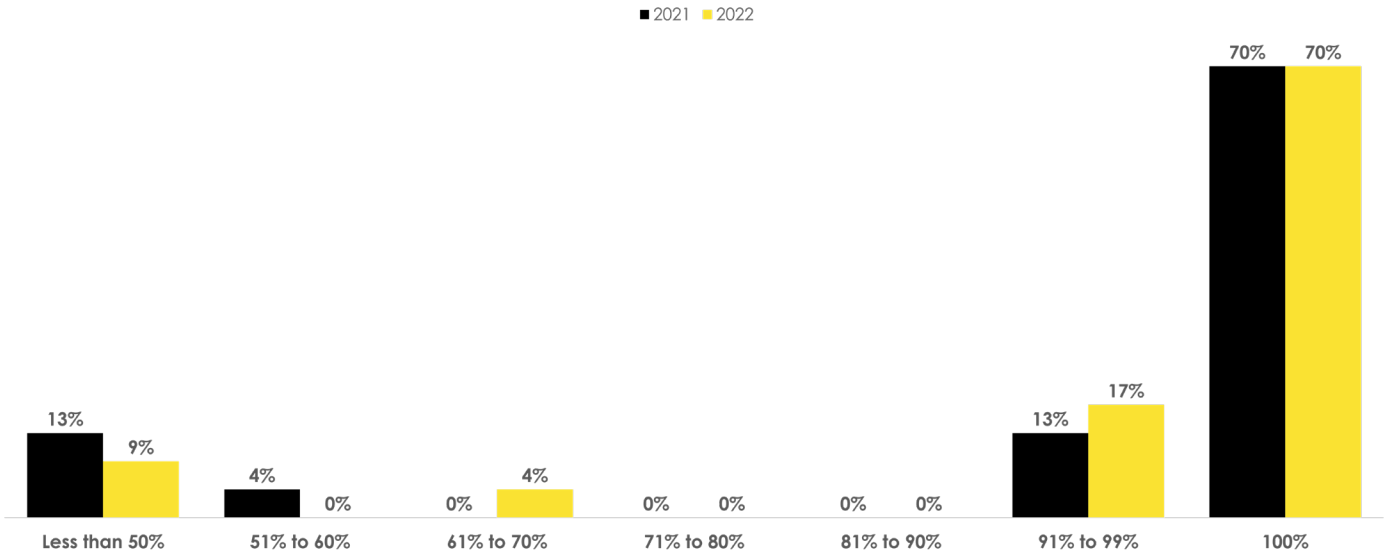
Principle 4 – Payment Flows

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

Beyond blocking fraudulent traffic, which is the purpose of Principle 3, it is critical that payment flows are stopped to prevent fraudsters from monetizing traffic. 87% of respondents scored over 90% compliance with 57% scoring 100%. This represents an increase of 4 pp from the 2021 survey, further illustrating the commitment of carriers to implement processes to actively block fraudulent payments. To be fully compliant, carriers must:

1. Have a process in place to handle payment withholding in the case of fraudulent traffic.
2. Use a process that is aligned with i3 Forum guidelines.
3. Apply this process to all cases of fraudulent traffic.

EXHIBIT 28: DISTRIBUTION OF CARRIER COMPLIANCE TO PRINCIPLE 4 – PAYMENT FLOWS 2022 vs 2021



Note: 2022 = n = 23, 2021 = n = 23; Source: Code of conduct survey 2022 & 2021, Delta Partners Analysis

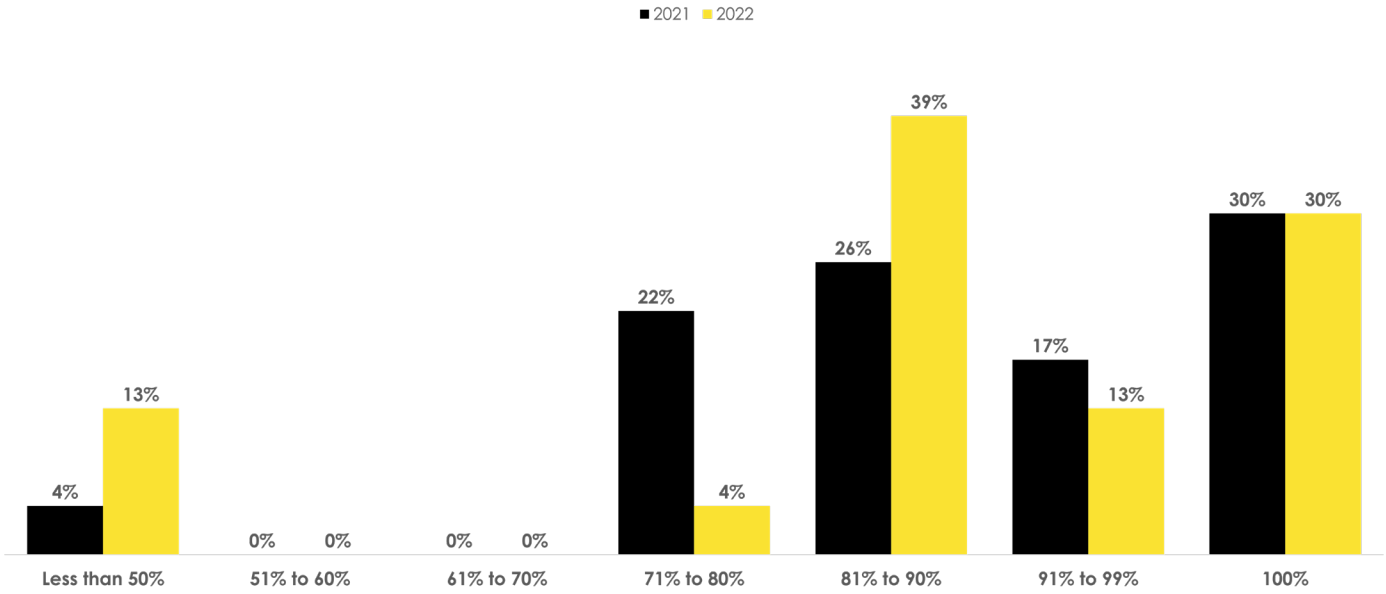
Principle 5 – Reporting

Commitment to share information regarding fraudulent traffic flows with carrier peers.

Carriers were asked to demonstrate the level to which they share information on a regular basis with peers. 43% of respondents demonstrated over 90% compliance compared with 47% in 2021. To be fully compliant, carriers are expected to:

1. Share information on at least a monthly basis with peers on topics including suspected fraudulent B-number ranges, and newly identified fraud types.
2. Share information by way of email, bi-lateral calls, group calls and discussions at conferences.
3. Be a member of a fraud working group or fraud- focused industry association, such as the GLF Anti-Fraud Working Group, i3 Forum, CFCA, and GSMA Fraud and Security Working Group.

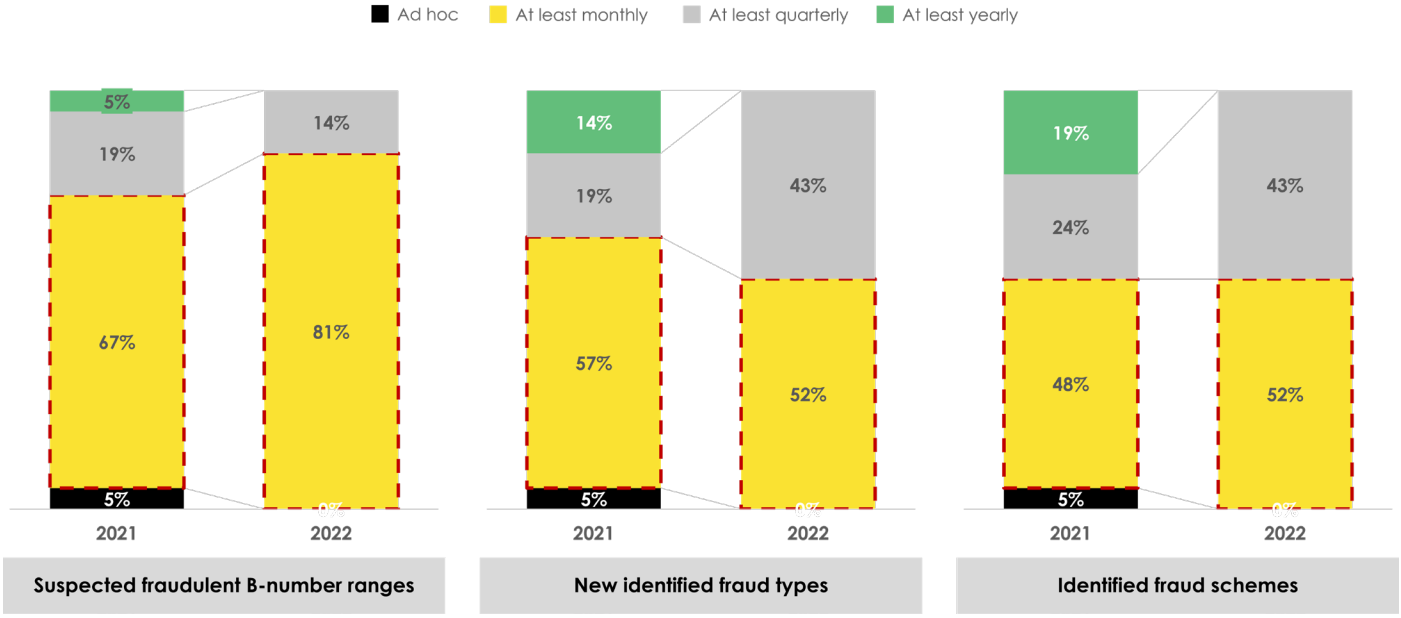
EXHIBIT 29: DISTRIBUTION OF CARRIER COMPLIANCE TO PRINCIPLE 5 – INFORMATION SHARING 2022 vs 2021



Note: 2022 = n = 23, 2021 = n = 23; Source: Code of conduct survey 2022 & 2021, Delta Partners Analysis

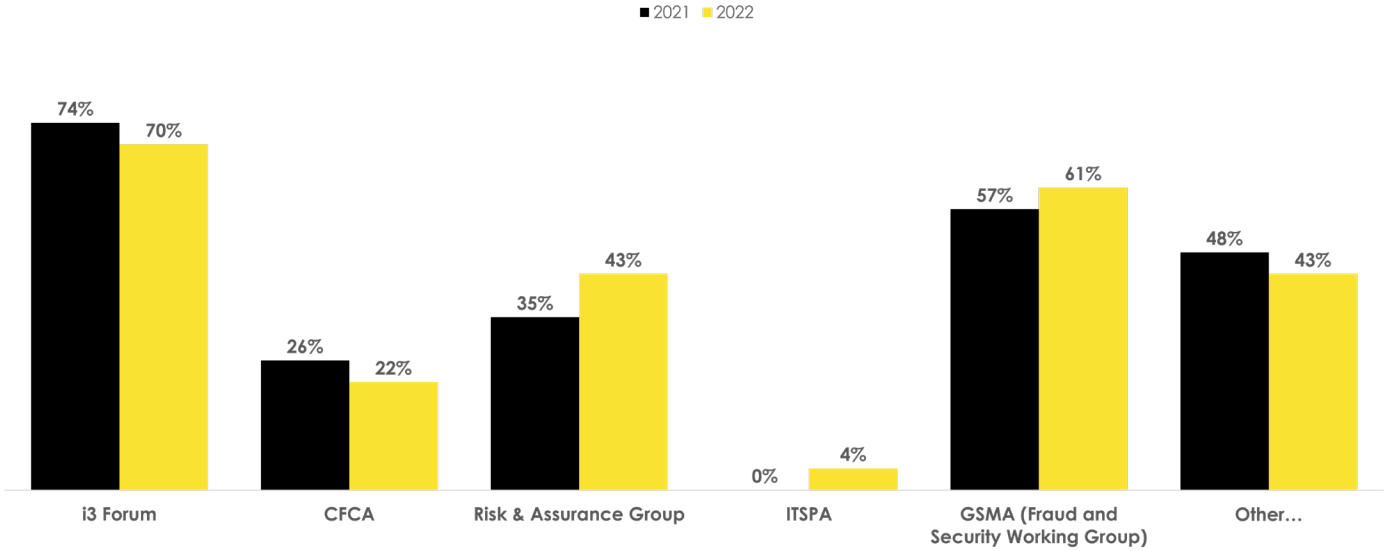
Responses from carriers suggest an increase in the frequency of information sharing between peers. As shown in exhibit 30, there is a heightened monthly reporting frequency of suspected fraudulent B-ranges (14 pp) and Identified fraud schemes (4pp). As well as an increase of quarterly reporting of identified fraud types and schemes. Although the data is reassuring that carriers are increasing collaboration, discussions with some respondents suggested that there is still a lot of room to improve spaces to share information and they highlighted the importance of the participation of industry forums. As illustrated in exhibit 31, The Risk & Assurance group and GSMA have seen a slight increase in participation while the i3 forum and CFCA have seen a slight decrease.

EXHIBIT 30: PREVALANCE OF INFORMATION SHARING BETWEEN PEERS 2022 vs 2021



Note: n = 23; Source: Code of conduct survey 2021 & 2022, Delta Partners Analysis

EXHIBIT 31: PARTICIPATION IN INDUSTRY FORUMS 2022 vs 2021



Note: 2022 = n = 23, 2021 = n = 23; Source: Code of conduct survey 2021 & 2022, Delta Partners Analysis

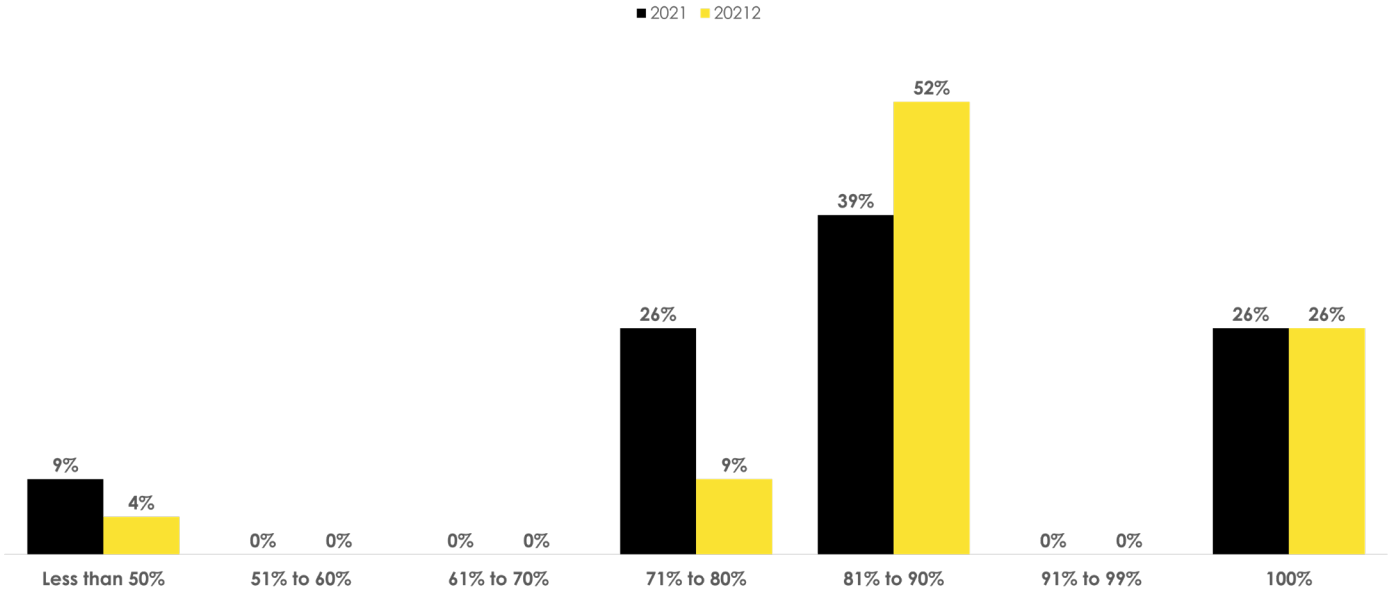
Principle 6 – Contracts

Adoption of standard contracting terms addressing fraudulent traffic management.

Ensuring uniform inclusion of standard anti-fraud clauses in contracts is a critical step to structurally fight against fraudulent traffic. In 2022, 26% of carriers were identified to be fully compliant, which means that they:

1. Require the inclusion of anti-fraud clauses in all contracts with customers.
2. Have a roll-out process/plan to include the i3 Forum related contract clauses or their own clauses that are at least as strong in your standard contracts.

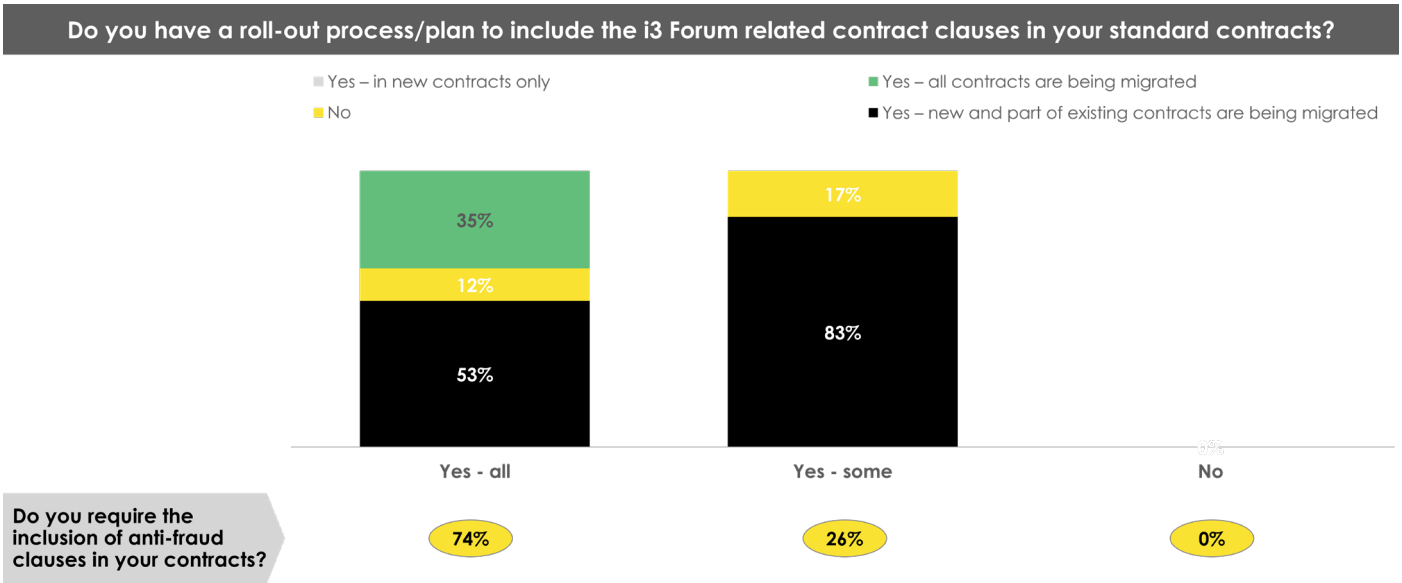
EXHIBIT 32: DISTRIBUTION OF CARRIER COMPLIANCE TO PRINCIPLE 6 – CONTRACTS 2022 vs 2021



Note: 2022 = n = 23, 2021 = n = 23; Source: Code of conduct survey 2021 & 2022, Delta Partners Analysis

Although the implementation of anti-fraud clauses and renegotiation of existing contracts pose a challenge from a legal and operational perspective, compliant carriers had made it a priority and are making interesting advances. In some cases, coordinating with international legal, compliance and operational teams to methodically ensure contract clauses are added into existing contracts. As illustrated in exhibit 33, this group represents 35% of respondents, while 53% are still focused on the implementation of the clauses in the contracts.

EXHIBIT 33: CONSISTENCY OF FRAUD CLAUSE CONTRACT ADOPTION 2021



Note: n = 23; Source: Code of conduct survey 2022, Delta Partners Analysis

Powered by

DELTA PARTNERS

an FTI Consulting company