I3 Forum – RAG
Fraud Survey 2022

GOAL OF THE SURVEY

The aim with this questionnaire - organized and executed by the i3Forum Fight Against Fraud working group and the Risk and Assurance Group (RAG) - is to gain insights from telecommunication professionals (in the fraud, risk managers and revenue assurance areas) on what are their challenges and the trends they see regarding fraud.

The i3 Forum wishes to improve the overall understanding on fraud dynamics in the wholesale carrier space to establish and communicate realistic guidelines for the reduction of fraud globally. Wholesale and retail carriers in different geographies were invited to complete the survey.

The survey covers 6 main themes:

1. *General*
2. *i3 Forum*
3. *Fraud General*
4. *FMS/Monitoring/Detection*
5. *Reporting*
6. *Dispute*

ABOUT THE ORGANIZERS - I3FORUM

i3Forum is an industry body that enables and accelerates transformation across the international telecommunications wholesale carrier ecosystem. Our members promote industrywide collaboration with an open and inclusive model focused on enabling success in a changing market. We develop, curate and share practical recommendations and best practices provided by the carrier members.

i3Forum has 6 different working groups which are:

1. *Fight against fraud*
2. *Messaging*
3. *Technology*
4. *Market data*
5. *Numbering plan initiative*
6. *eCare*

"By the Carriers - for the Carriers"

http://i3forum.org/

ABOUT THE ORGANIZERS – Risk and Assurance Group (RAG)

“Established in 2004 by UK telcos with the help of Cartesian, the RAG (originally the Revenue Assurance Group) is the longest running event in the world of business assurance. Our scope has evolved to reflect the remit of a modern risk and assurance professional. All we ask is that people come with an open mind, and a willingness to share their knowledge.

RAG now cover the increasingly complicated web of risk and assurance work in fraud management, enterprise risk management, law enforcement liaison, credit risk, margin assurance, capex analysis, and security. Our scope has evolved to reflect the remit of a modern risk and assurance professional.”

“By the Experts – for the Experts”

https://riskandassurancegroup.org/

EXECUTIVE SUMMARY 1/2

- **Large representation and response rate:** 46 professionals completed the survey. The respondents represented organizations active in both the wholesale and retail areas.
- **Fraud trends:** 80% of the respondents thought fraud either remained stable or increased over the past year
- **Fraud monitoring and protection**: 80% of the respondents have implemented fraud management systems to protect their customer base from fraud, 70% have developed their own tools and 50% apply Artificial Intelligence (AI) and machine learning to improve the detection. The respondents understand the need to mitigate fraud diligently and almost 50% of them implement blocking within 2 hours from the detection. The carriers surveyed allocate 1 to 5 full time employees (FTE) to run anti-fraud operations
- **Internal processes:** 80% of the respondents thought that raising awareness to **s**enior management is important and have developed internal fraud reports**.** Half of the carriers stated it is not in line with their business rules to work with suppliers that do not take adequate steps to prevent fraud
- **Prevalent fraud types:** International Revenue Share Fraud (IRSF) is the top threat. Wangiri and CLI spoofing follow in 2nd and 3rd position respectively.

EXECUTIVE SUMMARY 2/2

- **Fighting fraud:** A powerful tool to discourage bad actors from generating fraud is payment withholding. This requires proper internal processes at carrier level, industry alignment to handle fraud related disputes in such a way that they impact only the faulty parties. 60% of the respondents reported that they managed to get a full credit note for disputed amounts, if the disputes are issued timely and that all required supporting documentation is provided.
- **Regulation** is another powerful tool. A proper regulation would allow to override commercial agreements and non-disclosure agreements in case of fraud and would help identify the faulty parties. Such regulation is still missing.
- **Collaboration**: Respondents thought one of the keys to success is collaboration and that there are still improvements to be made to share details on fraud events swiftly. The i3Forum is working to improve the information share within its community.
- **i3Forum** : 70% of the respondents thought the i3Forum has had and continues to have a positive impact in fighting fraud in the wholesale space thanks to its white papers, recommendations, educational activities etc.

All the positive feedback and showing the way for improvement

give us the tools and determination to continue our work!

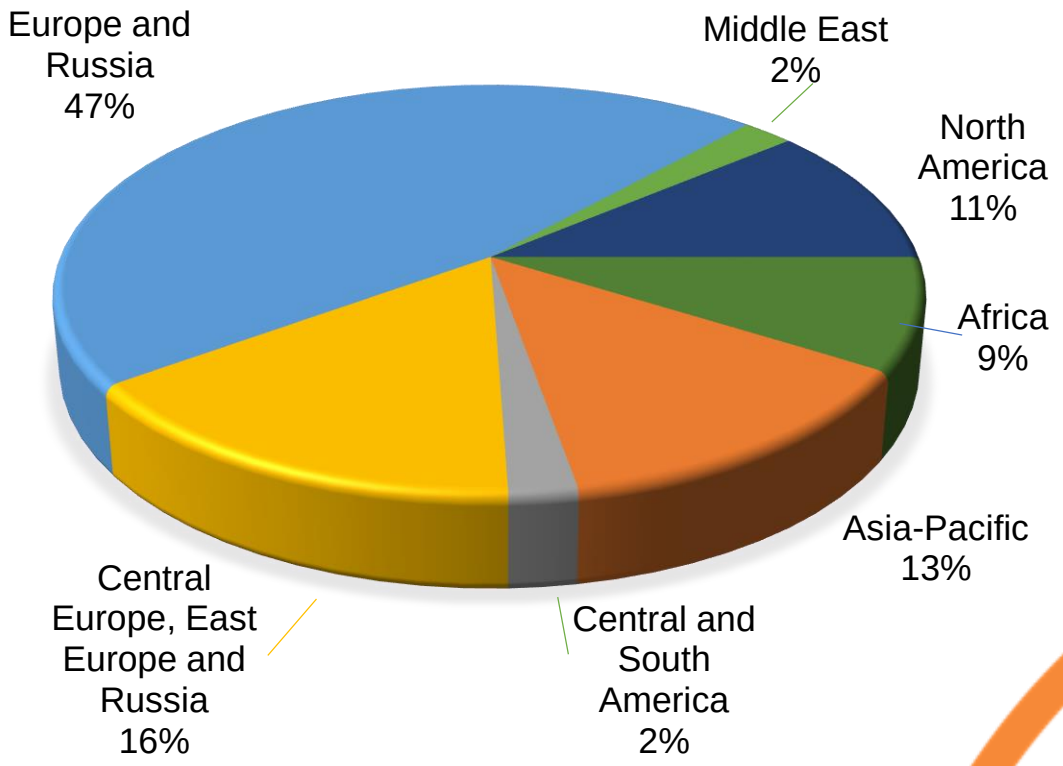
GENERAL - Question 1: I which region are you located?

The majority of the answers received come from Europe-based telecommunication companies: 28 respondents.

This is probably due to the fact that i3F is membership is primarily from this region.

North, Central and South America : 8 respondents

Asia : 6 respondents.

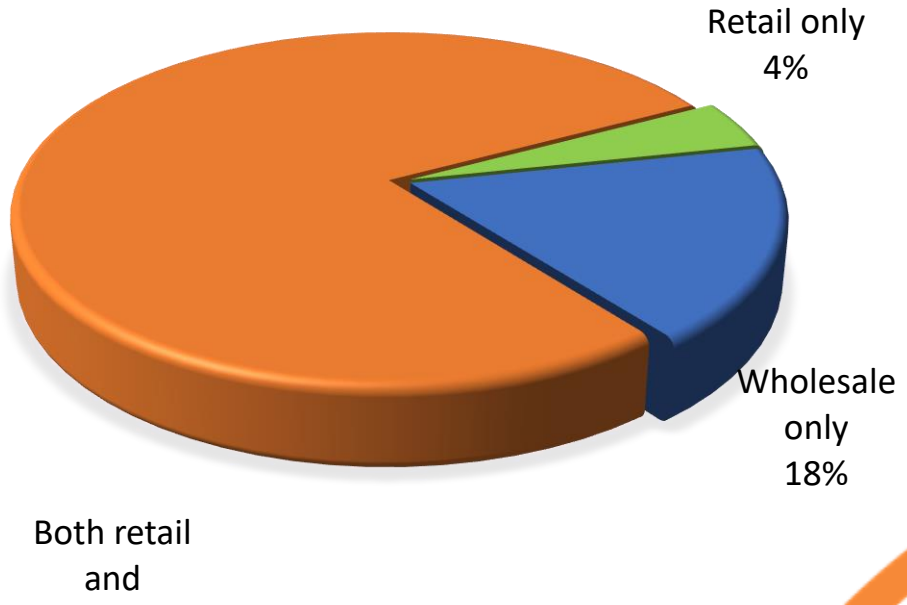


GENERAL – Question 2: What kind of services does your company provide?

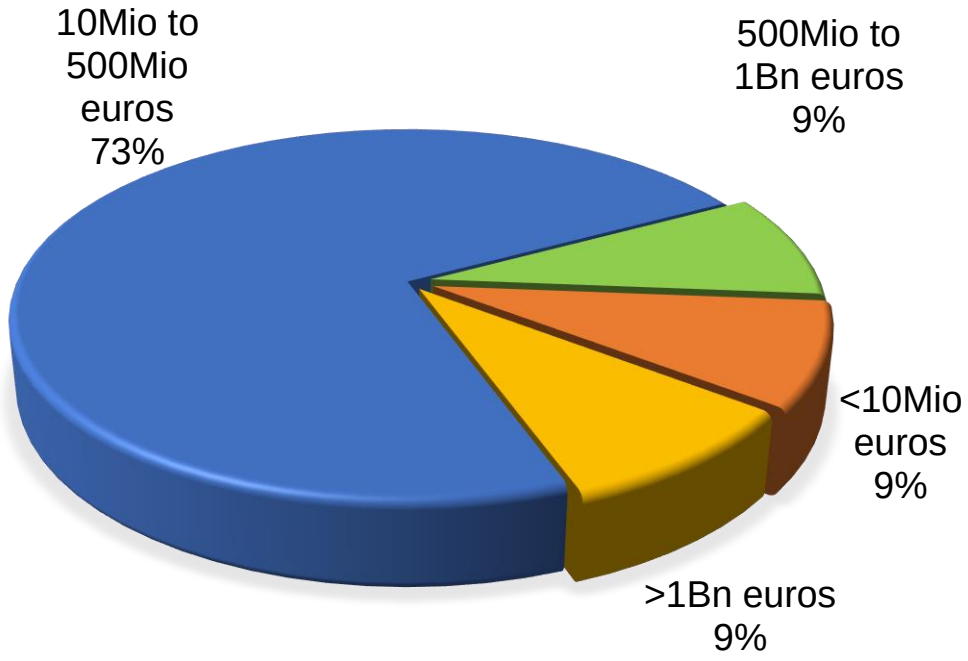
Most of the respondents are involved in both retail and wholesale related activities

Only wholesale activities: 8 respondents

Only retail activities: 2 respondents



GENERAL – Question 3: How much of your annual revenue is generated from International wholesale services?



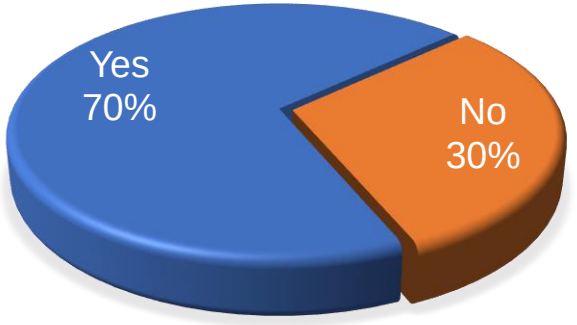
43 of the respondent carriers are active in the wholesale business (confer question 1).

Out of this group, 8 of the respondents belong to the Tier1 community. They are the large international wholesale players.

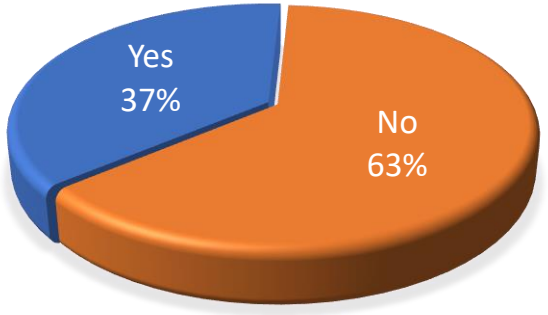
But most of the answers came from Tier2-3 carriers whose revenues are between 10 and 500 Mio euros per year.

I3FORUM – Questions 4 and 5

Are you familiar with the activities of the i3Forum in favor of the wholesale telecommunications industry?



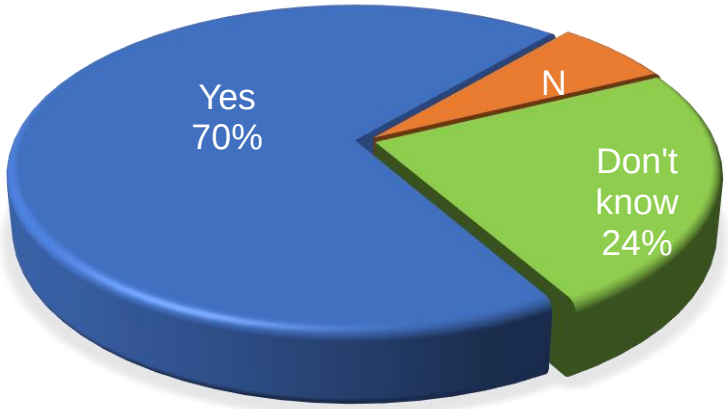
Is your company an i3Forum Fraud Fight group member?



I3FORUM – Question 6: Do you believe the i3Forum Fight against Fraud working group can make a difference in the telecom industry by raising awareness and creating guidelines on how telcos can reduce fraud?

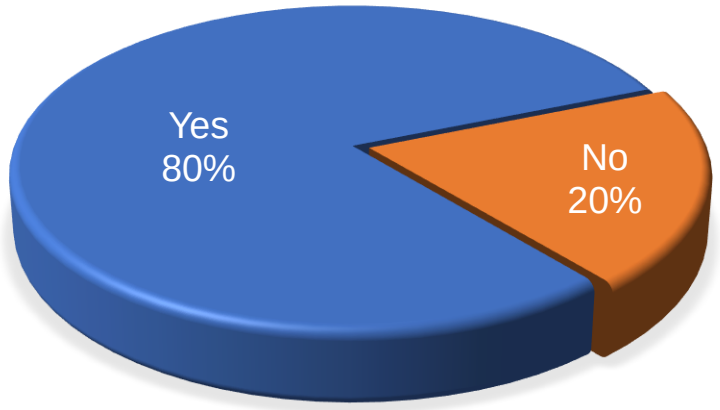
Apart from the i3Forum members (37% of the respondents), 33% of the respondents are familiar with the i3Forum activities in the international wholesale space.

The respondents familiar with the i3Forum activities (70% in total) also think the i3Forum does make a difference in the industry by creating recommendations, white papers, analysis and informational activity.

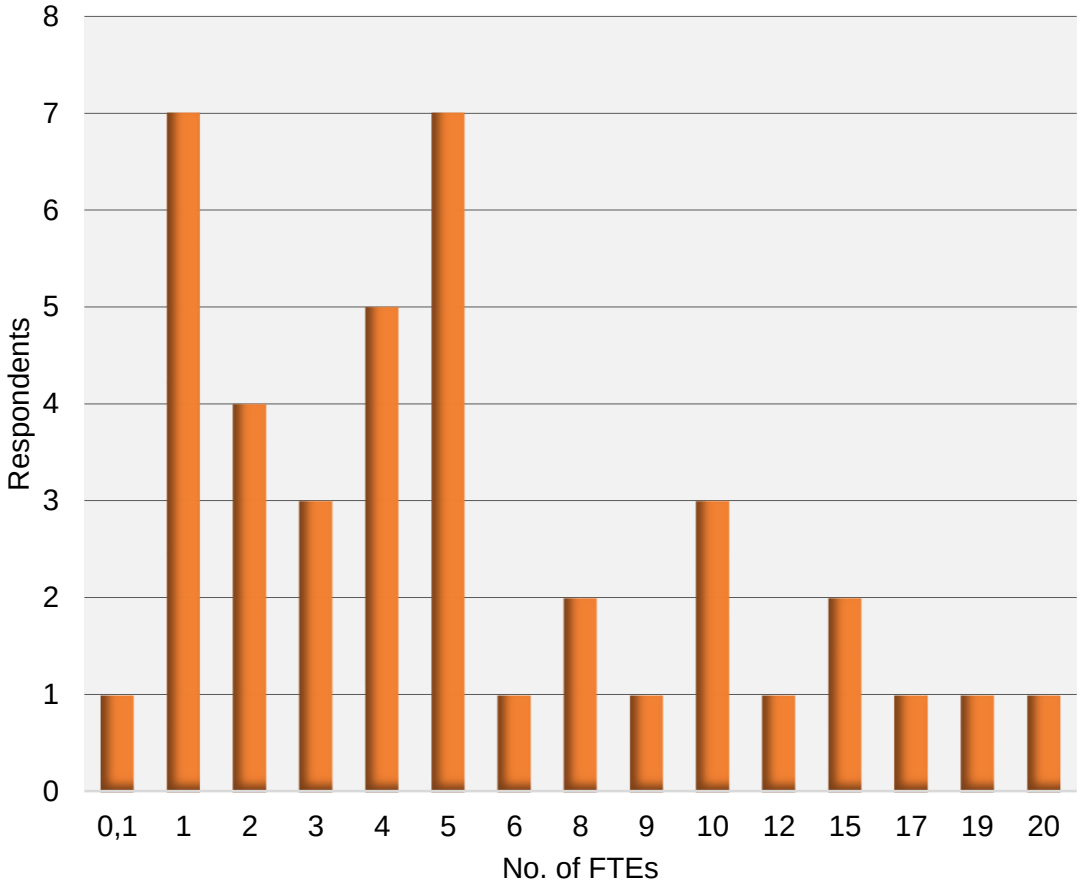


FRAUD GENERAL – Question 7

Does the wholesale division of your company have a dedicated anti-fraud team?



FRAUD GENERAL - Question 8: how many full-time-equivalents work on fraud-related activities in your company?

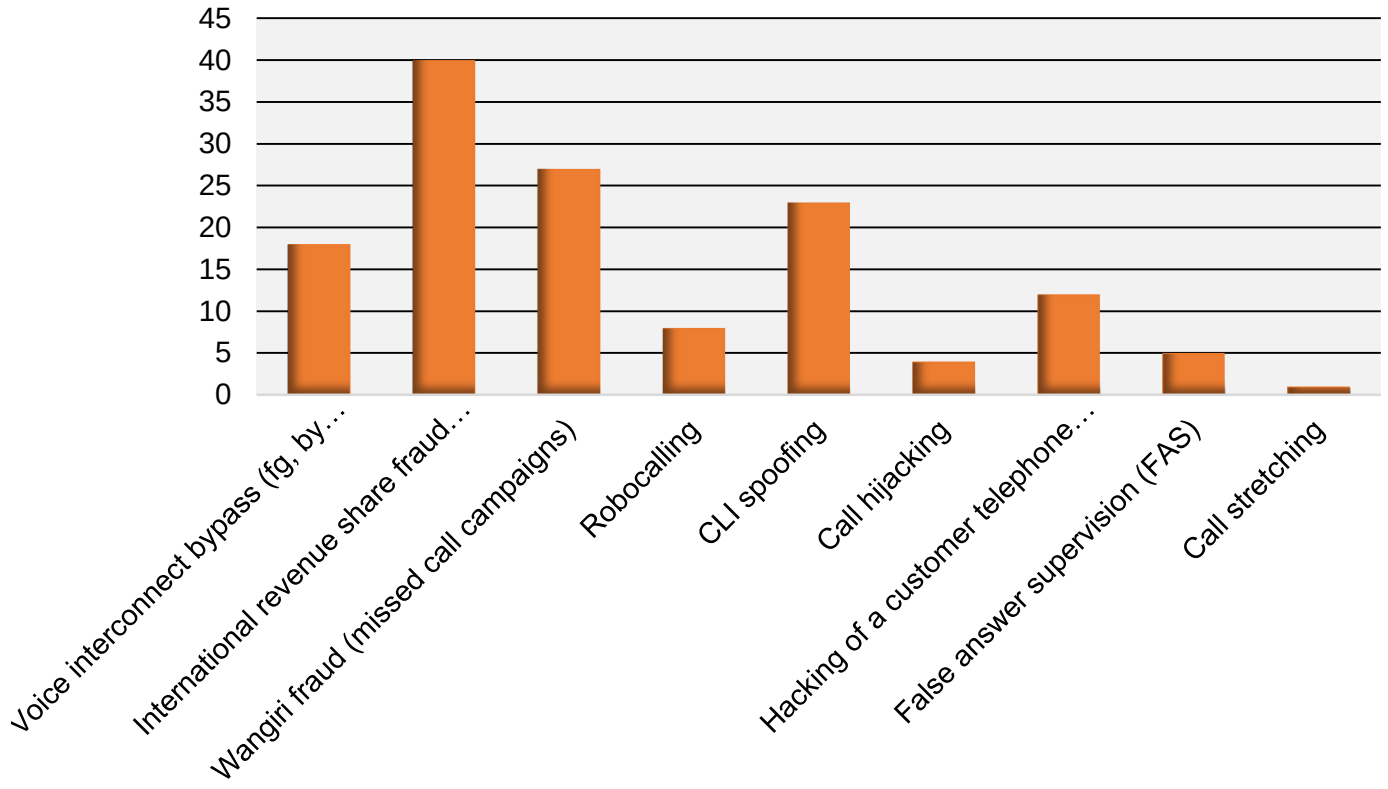


80% of the respondents have a dedicated anti-fraud team and dedicate 1 to 5 FTEs to support this fraud protection.

This shows the increased focus from carriers in active fraud protection and that the reactive approach to fraud prevention is no longer the preferred one.

This shows that the experience acquired over the past years is integrated and actively used by carriers in their fight against fraud activities

FRAUD GENERAL - Question 9 : which are the top 3 fraud scenarios impacting your company's international wholesale traffic?



As expected, the results shown join the results indicated by other similar surveys for other industry groups. The 3 scenarios that most severely impact the carriers are:

1. IRSF
2. Wangiri
3. CLI spoofing

FRAUD GENERAL – Question 9 : Which are the top 3 fraud scenarios impacting your company's international wholesale traffic?

International Revenue Share Fraud (IRSF) is still having the biggest impact on international wholesale carriers: **87%** of the respondents rated this fraud scenario as the biggest concern

Regulation still needs to improve to support the fight against IRSF, especially in small exotic islands, where unscrupulous businesses are still able to setup unethical activities using these islands numbering plan resources with the sole purpose of generating and accepting fraudulent traffic (both voice and SMS more recently)

Wangiri remains another of the main impcting fraud schemes for international wholesale carriers. Close to **60%** of the respondents indicated wangiri as a serious threat. The set-up and use of auto-diallers is accessible to virtually anyone, which eases the generation of high volumes of calls to the target destinations. The call back ratio is estimated to be 10%, which builds a very good return on investment for fraudsters.

The modus operandi of wangiri attacks remains borderline and although the spamming aspect of the missed calls can be considered as fraudulent, the call-back to these missed calls remains an active action by end-users that can hardly be considered as fraudulent according to some regulations/legislations.

CLI spoofing is tightly linked to the widespread use of Origin Based Charging (OBR) in some regions. Close to **50%** of the respondents thought this is a very serious issue with direct impact in their bottom lines.

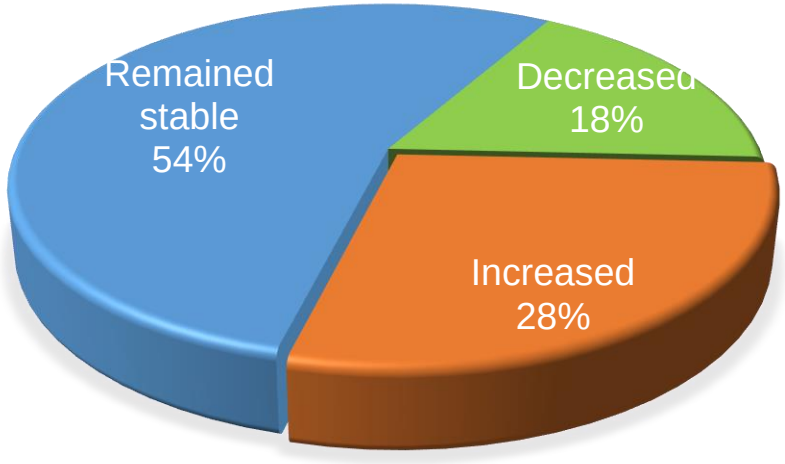
In this scenario, calls originated in countries with higher termination rate carry a spoofed CLI to show the call is rather originated in a country that allows for lower termination rates (10, 20 or even 100 times lower in some cases).

This very high difference in termination costs create a strong incentive for rogue players to manipulate the CLI to try and fake a cheaper origin.

FRAUD GENERAL – Question 10 : What is the trend for fraud losses over the last 12 months?

More than 80% of the respondents thought fraud either remained stable or increased.

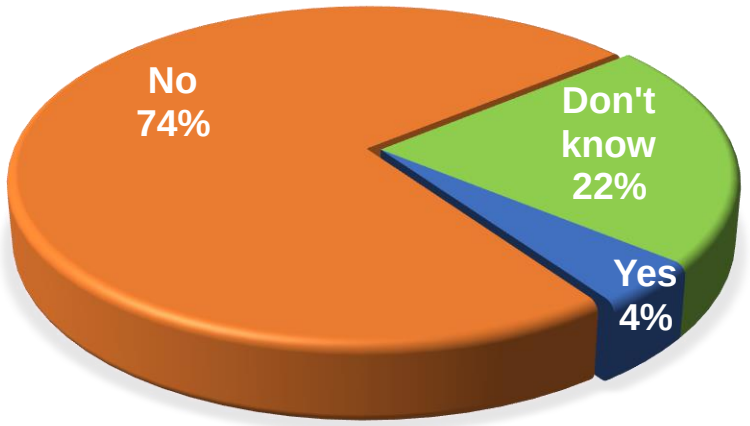
This could explain why most of the carriers feel the need to invest in fraud operations to mitigate the impact of fraud and protect customers.



FRAUD GENERAL - Question 11 : do you believe fraud is prevented or reduced by the work done by law enforcement (e.g. Regulators, Europol, ENISA, etc)

Most of the respondents feel that Law Enforcement Agencies (LEAs) would need to be more agile in creating the right framework and taking concrete actions to avoid telecommunication services misuse.

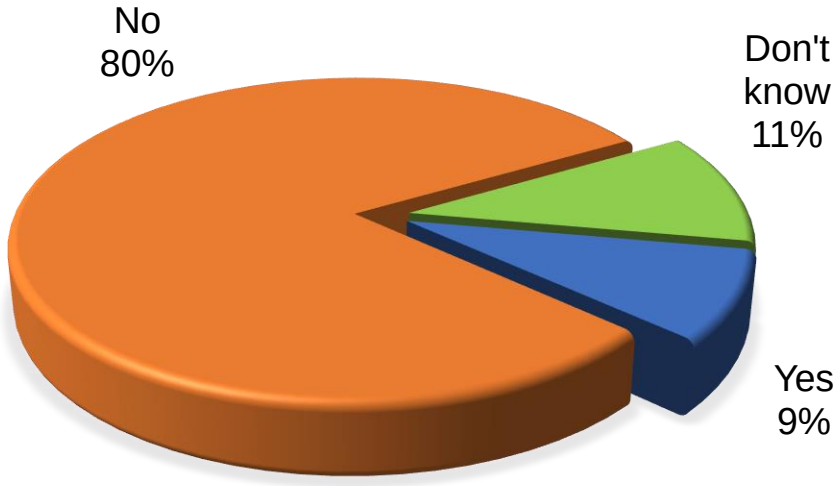
A tighter collaboration between the carrier community and the different LEAs may have a positive impact and improve collaboration and information exchange to foster a safer Telecommunication ecosystem,



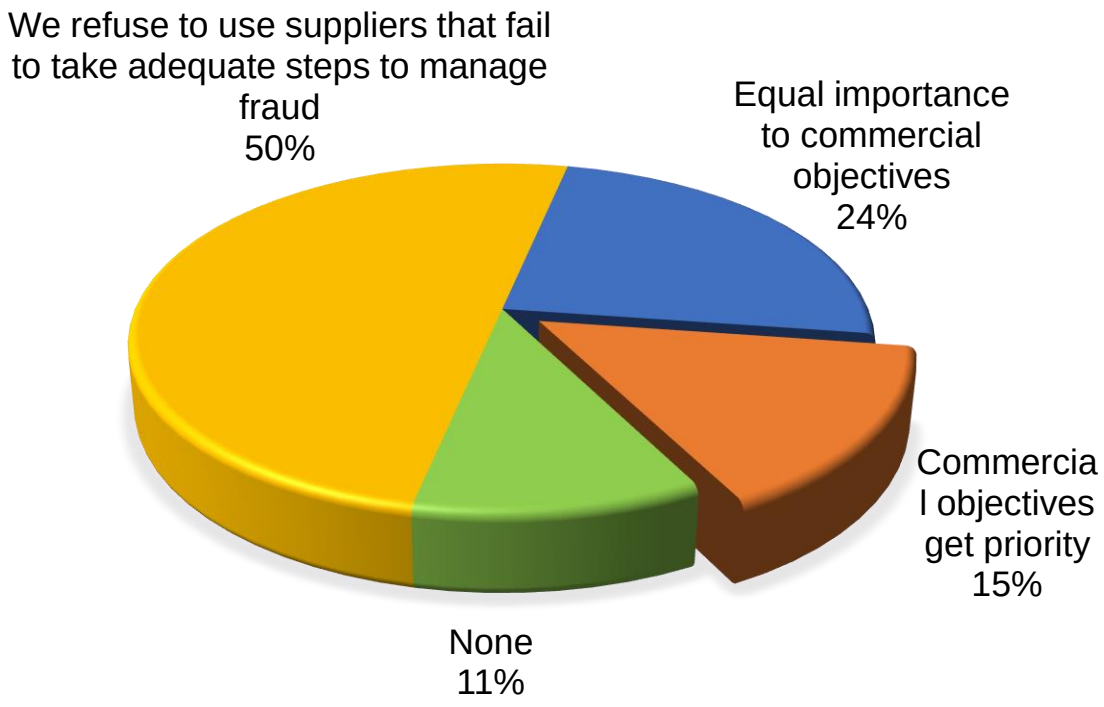
FRAUD GENERAL - Question 12: Are you satisfied with your country's regulatory framework with respect to fraud?

A majority of respondents agreed that the National Regulators should do more to help the carrier community in the fight against fraud and to mitigate misuse.

The right regulatory framework may provide the tools to help protect not only end-users but also the National operators and International carriers.



FRAUD GENERAL – Question 13: When your company makes routing decisions, what importance does your company attach to a supplier's approach to managing fraud?



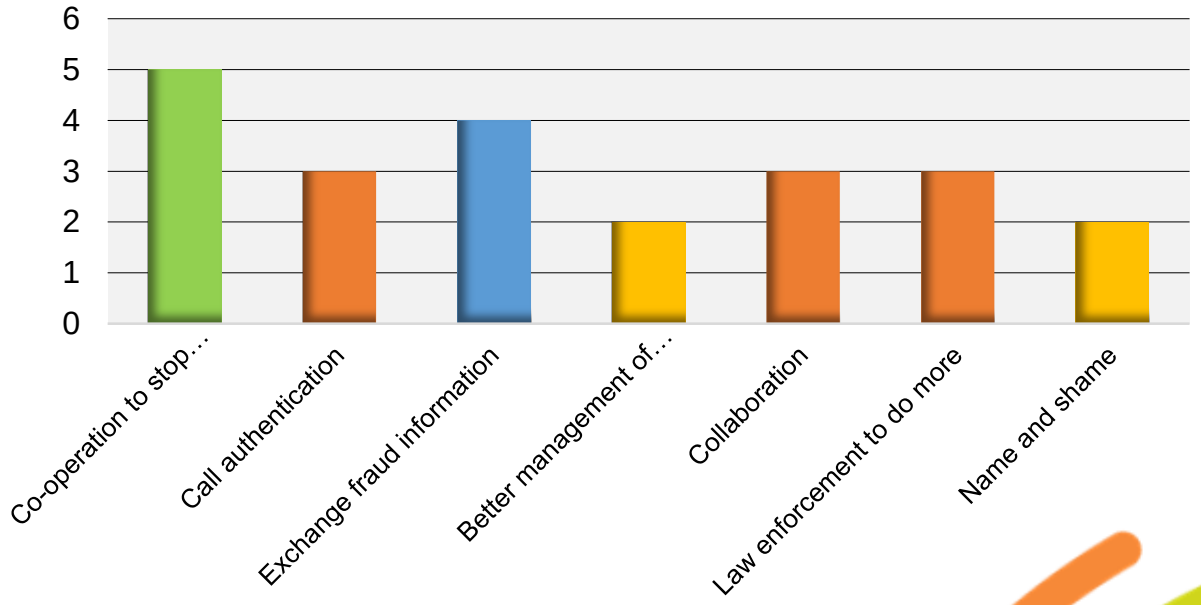
Only half of the respondents consider that using fraud protection conscious suppliers is the priority. Surprisingly, 7 respondents have the impression that, in their company, it doesn't matter if a supplier is not engaged in fraud protection .

Some parties remain attached to the principle that any traffic they receive should be passed on unaltered, no matter the nature of it.

FRAUD GENERAL – Question 14: What is the single most important objective that you would like the industry to adopt in order to reduce fraud? (I)

Most of the respondents agreed that **stopping the money flow** related to fraudulent transactions is the most important action available to fight fraud effectively and to deny revenues from fraudsters. Both the 'Co-operation to stop payment for fraud' and the 'Exchange fraud information' are key to denying revenues from fraudsters.

The second most popular answer relates to **sharing information timely** with peers, to improve the response to ongoing attacks and build a preventive strategy for future cases. The need for such information share has been acknowledged by the i3Forum community and an information share process has been running successfully for several years now.



FRAUD GENERAL – Question 14: What is the single most important objective that you would like the industry to adopt in order to reduce fraud? (II)

3 different objectives share the third place:

- **Call authentication** : the recent Regulatory initiatives in several countries that promote CLI authentication standards and procedures (e.g. STIR/SHAKEN in US and Canada, Ofcom requirements for UK phone providers to block spoofed calls, initiatives from Arcep in France, etc) require changes across the whole ecosystem. The results of these initiatives are not yet visible from the international carrier community perspective.
- **Collaboration** across the industry
- Improved **law enforcement** activities

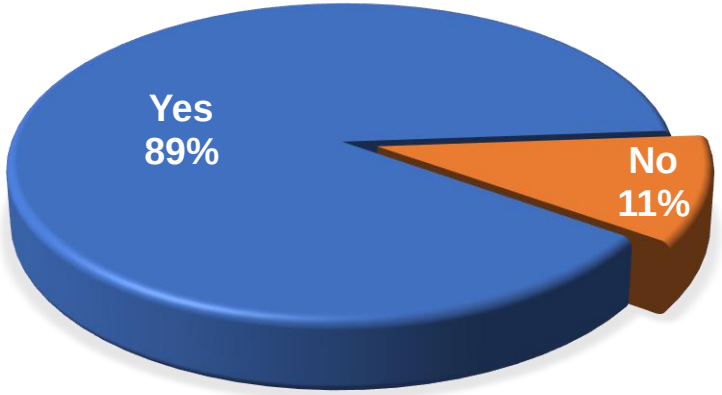
Finally, **better management of number ranges** by the carriers (including the detection and blocking of fraudulent number ranges) and ‘**name and shame**’ of the guilty parties could help improve the fight against fraud.

FMS/MONITORING/DETECTION – Question 15: Do you use a FMS to monitor international wholesale traffic?

Almost 90% of the respondents have invested and use a FMS to detect fraud.

The increased complexity of the fraud attacks and the increase in the volume of these across telecommunications services are driving the increased investments in automation.

In general fraud detection and protection of the telecommunications services to provide a better customer experience are getting fraud to become a strategic topic for international carriers,

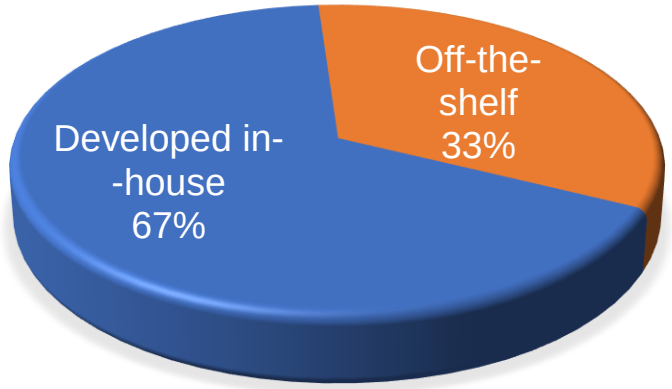


FMS/MONITORING/DETECTION – Question 16: if you use a FMS to monitor international wholesale traffic, was it purchased oof-the-shelf from an external supplier or was it developed in-house?

Most of the respondents (67%) dedicated efforts to create a FMS tailored to their own needs and environment.

Only 33% acquired an off-the-shelf platform and they tailored it to suit their own environment and architecture.

The international wholesale space has specificities versus a traditional operator's needs. These specificities are not often integrated in the standard FMS.



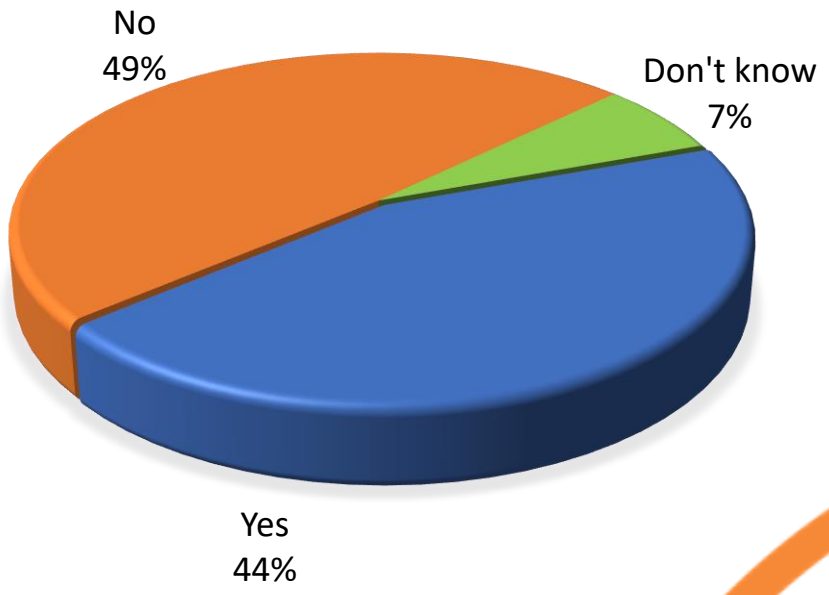
FMS/MONITORING/DETECTION – Question 17: Do you use artificial intelligence and machine learning to detect fraud?

Artificial intelligence (AI) and machine learning (ML) are gaining traction to detect fraudulent patterns affecting telecommunications transactions.

They provide very good results for some specific fraud scenarios such as CLI spoofing and spam detection and are very efficient as a complement to the traditional rule-based fraud detection.

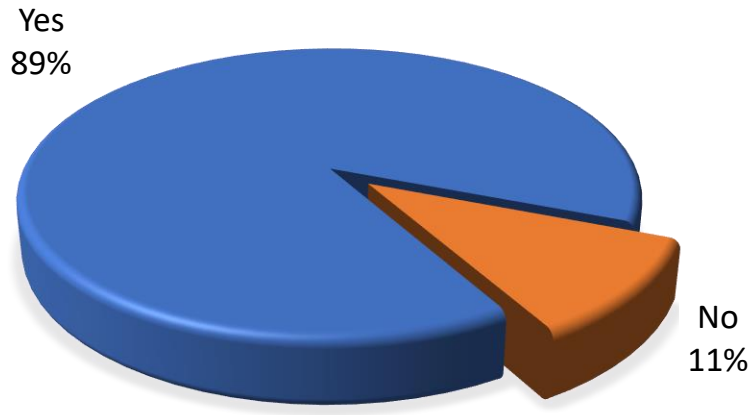
Almost 50% of the respondents do not use AI or ML in fraud detection and almost 45% do use it.

We expect the use of AI and ML to continue increasing in the coming years.

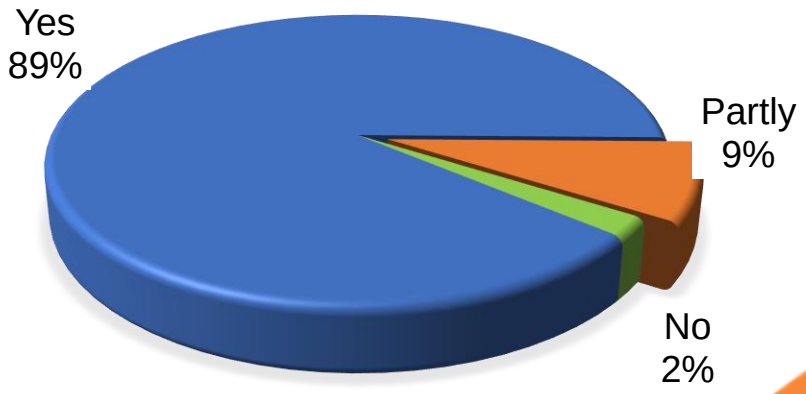


FMS/MONITORING/DETECTION – Questions 18 , 19

Do you actively block inbound wangiri calls before they reach the end user?



Do you actively block International wholesale traffic you find to be fraudulent?



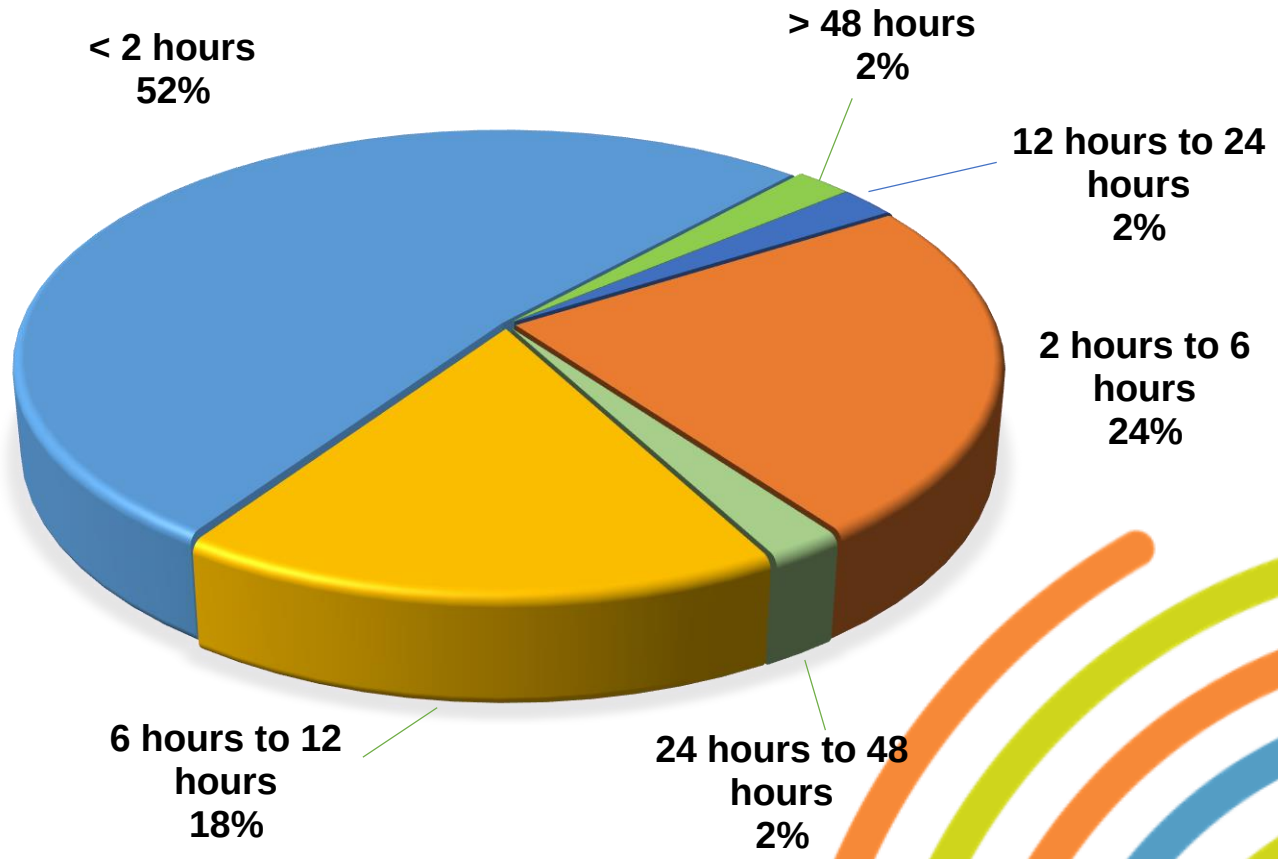
Close to 90% of the respondents block fraudulent traffic when it is detected, including wangiri attacks. This shows the high commitment from the wholesale carrier community to fight fraud and enhance the quality of the telecommunications services globally .

FMS/MONITORING/DETECTION – Question 20: How much time typically elapses between detecting fraud and blocking the fraudulent traffic?

The delay from detection from blocking may vary on different elements such as the fraud type, the complexity of the investigation, etc.

In any case the time lapse from detection to blocking varies significantly but it has improved considerably in the past years thanks to the experience gained by the wholesale carrier community and the increase in automation.

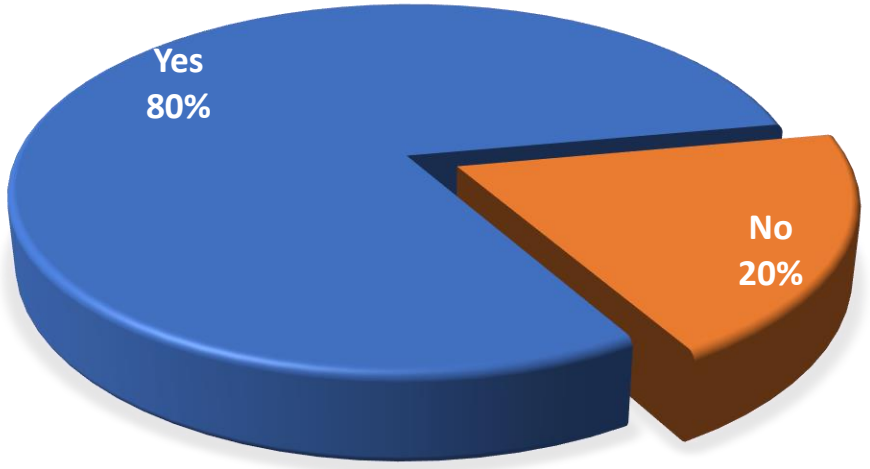
Altogether, over 90% of the respondents indicated a maximum of 12 hours elapses between detection and blocking.



REPORTING- Question 21: Do you have a system to report the traffic that was blocked because of fraud?

Most of the carriers responding to this survey 80% generate reports on the blocking of fraud incidents.

There are less respondents generating barring reports than the respondents that have FMS in place, which could be explained by the fact that, in most cases, the enforcement point is outside of the FMS, requiring separate reporting.

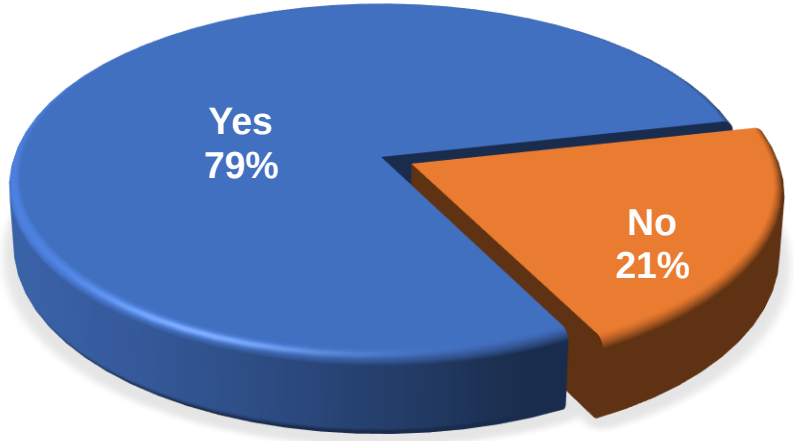


REPORTING- Question 22: If you have a system to report the traffic that was blocked because of fraud, do you believe that the reporting raises awareness of fraud amongst the senior managers in your company?

There seems to be no consensus on whether the barring reports can help raise awareness with regards to fraud to senior management:

- Most of the respondents (79%) thinks it makes sense
- 21% does not agree with this statement, out of which 1/3 completely disagrees, 1/3 has doubts and 1/3 did not reply to this question.

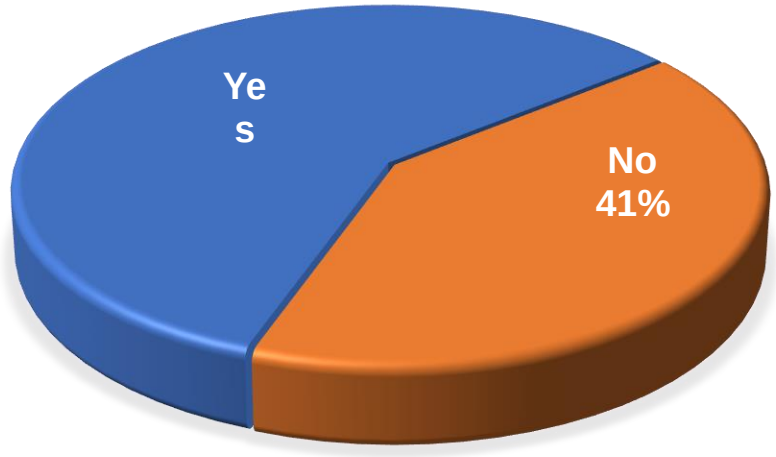
The experience shows that the commitment of senior management is decisive in fighting fraud.



REPORTING- Question 23: Do you offer a fraud reporting service to your wholesale customers?

Close to 60% of the respondents think it's important to invest not only in FMS and reporting tools, but also to inform customers duly on the fraud detection.

The international carriers have build different value-added services to improve the customer experience and the quality of their telecommunications services.



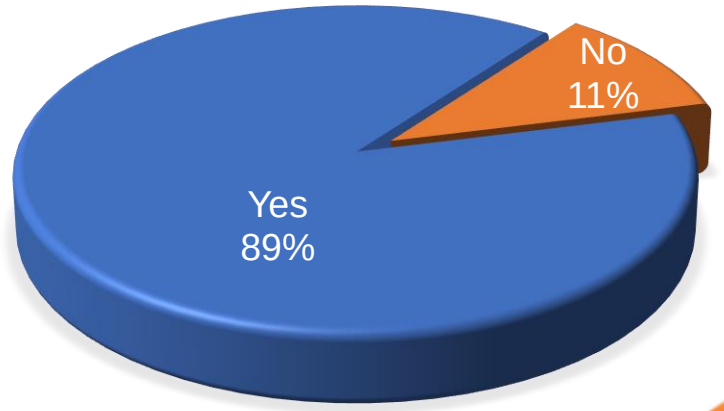
DISPUTES – Question 24: Do you have a dedicated fraud clause in contracts with other parties (wholesale carriers, operators, etc)

Previous questions in the survey show that payment withholding in case of fraud is a fundamental building block in fighting fraud.

Implementing payment withholding requires bypassing the traditional contractual obligations (traffic sent = traffic to be paid for). It is important to have the right back-to-back contractual clauses that will allow for payment withholding under well-agreed conditions.

The i3Forum provides guidance regarding the terms of fraud contractual clauses to allow for a homogeneous setup in the industry.

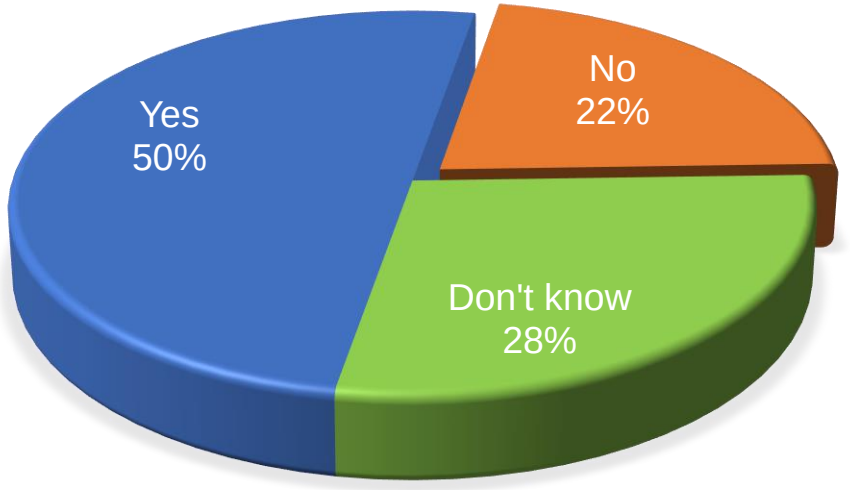
Most carriers do foresee such contract clauses, as recommended by i3Forum and GLF Code of Conduct.



DISPUTES – Question 25: Have your contacts incorporated the standard wording of the fraud clause recommended by the i3Forum?

The i3Forum proposed fraud contractual clauses are increasingly used in the industry by i3Forum members and non-members. 50% of the respondents utilise such clauses in the commercial contracts, allowing for a proper process to be defined within the companies and back-to-back support throughout the industry.

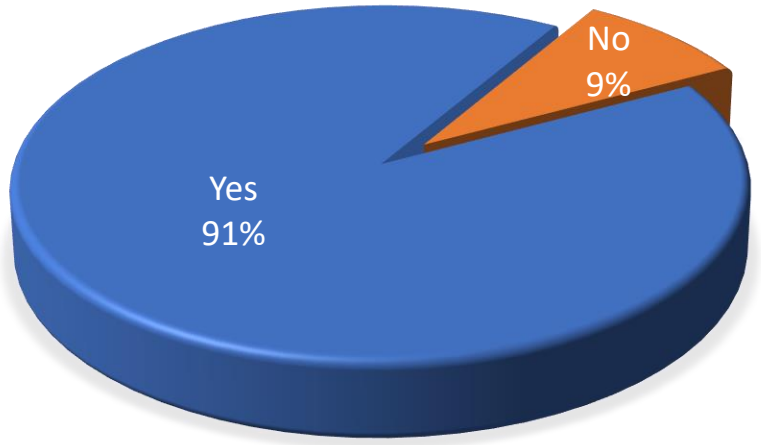
Updating all commercial agreements is a lengthy and complex activity that requires time.



DISPUTE- Question 26: Have you implemented a process to stop payments related to fraud?

Most carriers not only have proper fraud dispute clauses to stop payments for fraud traffic, but they also have built and implemented internal processes to support fraud payment withholding.

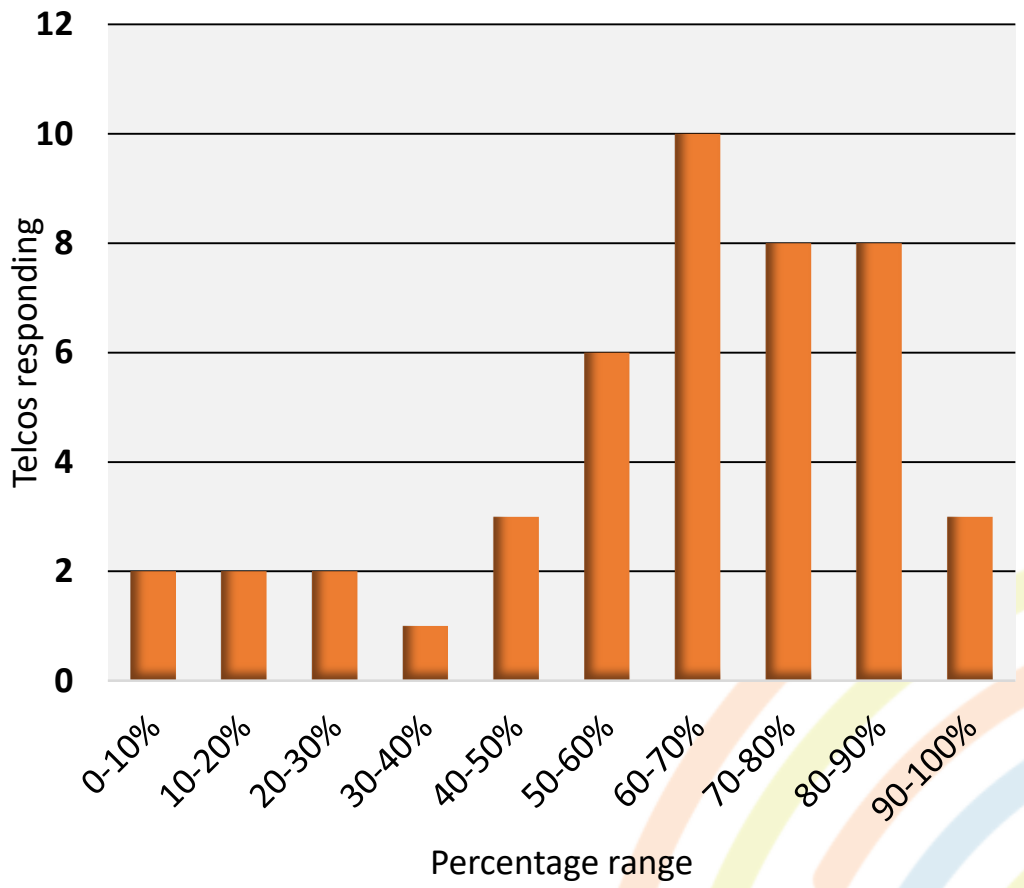
Such processes are key to implement fraud payment withholding efficiently and to provide timely response to fraud.



DISPUTE – Question 27: For the fraud disputes opened timely and supported with all required proofs, what percentage results in a full credit note for the disputing party?

Over 60% of the respondents reported they managed to get full credit notes for fraud disputes where all supporting material is provided timely. This means the elements indicated below were provided timely and cascaded to all relevant parties:

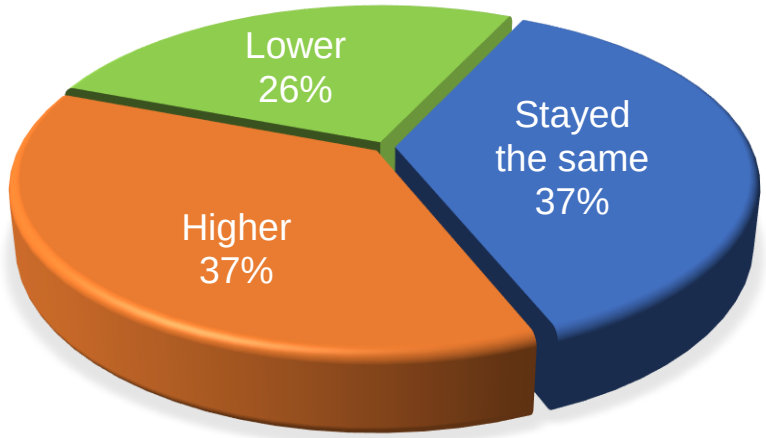
1. An early warning for payment withholding was sent to the supplier to avoid the supplier releases payments to the subsequent party in the chain
2. The relevant Call Data Records (CDRs) were provided to identify the portion of the traffic considered fraudulent
3. A police report (or from another law enforcement agency) issued by the traffic originating carrier was provided. This helps objectivise the fraud event, inform the authorities and possibly trigger an investigation.
4. A clear description of the fraud event is provided.



DISPUTE – Question 28: How did the number of fraud disputes evolve in 2021 compared to 2020?

70% of the respondents reported that the amount of fraud disputes either remained the same or increased.

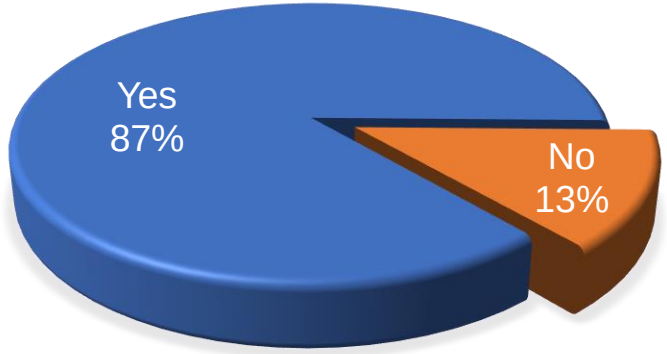
Fraud departments will keep an important role to safeguard telecommunications services in the future



DISPUTES – Question 29: Do you believe non-disclosure clauses are sometimes an obstacle to reducing fraud? Would you be willing to waive non-disclosure clauses for fraud incidents?

Most respondents recognize NDAs are an obstacle to identify the rogue actors generating or facilitating fraud. Secrecy in the industry has its historical roots in protecting the identity of the suppliers each party uses.

Regulatory support is required to bypass NDAs in case of fraud events (e.g. International Traceback Group process in US supported by FCC in the frame of the robocall mitigation efforts)



Thank you for your attention and collaboration!

Tamas Marothy
Senior Consultant,
i3 Forum

Katia Gonzalez
Chairperson of i3 Forum Fight Against Fraud working group

Eric Priezkalns
Chief Executive,
RAG