TAKING ACTION AGAINST FRAUD

Demonstrating the International Wholesale Industry's Leadership Against Telecoms Fraud

Oct 2018

in partnership with

DELTA PARTNERS

This report has been commissioned by:

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 Jussi Makela at:

jmakela@capacitymedia.com

DELTA PARTNERS

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

FOREWORD

Daniel Kurgan
CEO, BICS and Chair of GLF Fraud Working Group

Since its inception the GLF has brought together leaders of the international carrier industry to share insights and collaborate on strategic topics that are critical to the future of the industry. We work on areas where working together across carriers is critical for the betterment of the industry and not an area of service differentiation. Acting against fraudulent traffic is clearly a case in point. Seeking an operating environment that is free from fraudulent traffic is not an area of differentiation between my company and our peers. It is an issue where we should all work together both to improve the efficiency of our businesses but also to contribute to society – fraudulent telecoms traffic is often used by organized crime to raise and distribute funds. As such, by working to reduce fraud we are creating benefit beyond our businesses.

In March this year, the GLF launched its Code of Conduct to guide international carriers on how to work internally to manage fraudulent traffic. As of writing, there are 24 signees including many of the worlds' largest carriers. This report marks the launch of what I hope will become an annual milestone in our industry to assess our progress in reducing the impact and volume of fraudulent traffic and serve as a catalyst for future action. I thank my colleagues from around the world for their engagement and support in addressing fraudulent traffic. Together, I believe, we can strive towards a fraud free future.

Jussi Makela
Director, GLF

In an era of such intense inter-network operator competition, it is excellent to see how strongly the international carriers' leadership at the GLF have aligned behind a common goal of reducing fraudulent traffic. This is not a trivial topic – with an estimated annual cost of $17 billion and potential to reach all carriers, addressing fraudulent traffic should garner management attention. Our research in this report highlights the nature and range of focus this issue is receiving within carriers, the on-going 'battle' between fraudster and carrier, and the opportunity for technology innovation to address fraudulent traffic. We also present a framework for how international carriers may wish to take further action by moving beyond purely signing the Code of Conduct.

In producing this report, we have engaged with more than 20 leading international carriers as well as the CFCA and i3 Forum. We would like to thank all contributors for providing the information and insights that are shared in this report. We hope this report will serve to strengthen the dialogue within individual carriers for how they can reduce the volume and impact of fraudulent traffic as well as, importantly, encourage carriers as a community to take further collaborative actions.

Report contributors

CONTENTS

EXECUTIVE SUMMARY

1. Fraudulent traffic is estimated to cost the international wholesale carrier industry $17 billion annually, but the sources of fraud continue to change. In the last 12 months carriers highlight missed call campaigns and private branch exchange (PBX) hacking as having increased most significantly

2. 85% of carriers cite fraud as a priority for their organisation with 74% saying that it's growing in importance. Enhanced technology helps support an increased number of fraudulent traffic incidents but, from a carrier's perspective, a greater ability to quickly respond

3. Having dedicated fraud management full time employees (FTE) who are not linked to commercial performance is critical to ensuring that they have clear incentives to reduce fraudulent traffic

4. The use of fraudulent traffic by organized crime to raise and distribute funds highlights how important it is that international carriers work to reduce fraud as the impact goes beyond the carriers' profit and loss

5. While most carriers can identify and remove fraudulent traffic from their networks within six hours, contractual service agreements and a fear of mistakenly blocking legitimate traffic can make removing fraudulent traffic complex

6. Proactive customer management and allocating additional FTE are the two primary internal carrier requirements to reduce fraudulent traffic - only 5% carriers see technical innovation, such as AI, as a reason to reduce FTE focused on fraud management

7. Nearly all carriers track some metrics to manage fraudulent traffic. However, there is a lack of consistency in metrics tracked and less than 70% of carriers report these to the CEO's level

8. There is a disconnect between carriers prioritisation of fraudulent traffic as a strategic priority and the recognition of its financial impact – only 21% of carriers are able to identify an OCF of over 3%

9. Several carriers are working together informally to share information and pool resources, subject to competition law requirements, to address fraudulent traffic and there is an appetite for greater collaboration

10. The GLF Code of Conduct is being adopted by many leading international carriers with 25 signing up in its first seven months, but carriers want more action beyond this commitment

11. Through commitment, compliance, and collaboration the carriers will collectively act to move their organisations and the international wholesale industry towards a fraud-free future

12. All carriers are encouraged to adopt the Code of Conduct as well as seeking support from their customers and suppliers

13. Carriers are encouraged to self-attest adherence to the Code of Conduct and measure a common set of metrics communicated to CEO / Business Head level

14. Formalising information sharing and communication networks across the carrier community will improve the ability to collaborate in the shared aspiration of reducing fraudulent traffic

LIST OF EXHIBITS

PART 1

EVOLUTION OF FRAUDULENT TRAFFIC

1

Fraudulent traffic is estimated to cost the international wholesale carrier industry $17 billion annually, but the sources of fraud continue to change. In the last 12 months carriers highlight missed call campaigns and private branch exchange (PBX) hacking as having increased most significantly

2

85% of carriers cite fraud as a priority for their organisation with 74% saying that it's growing in importance. Enhanced technology helps support an increased number of fraudulent traffic incidents but, from a carrier's perspective, a greater ability to quickly respond

3

Having dedicated fraud management full time employees (FTE) who are not linked to commercial performance is critical to ensuring that they have clear incentives to reduce fraudulent traffic

4

The use of fraudulent traffic by organized crime to raise and distribute funds highlights how important it is that international carriers work to reduce fraud as the impact goes beyond the carriers' profit and loss

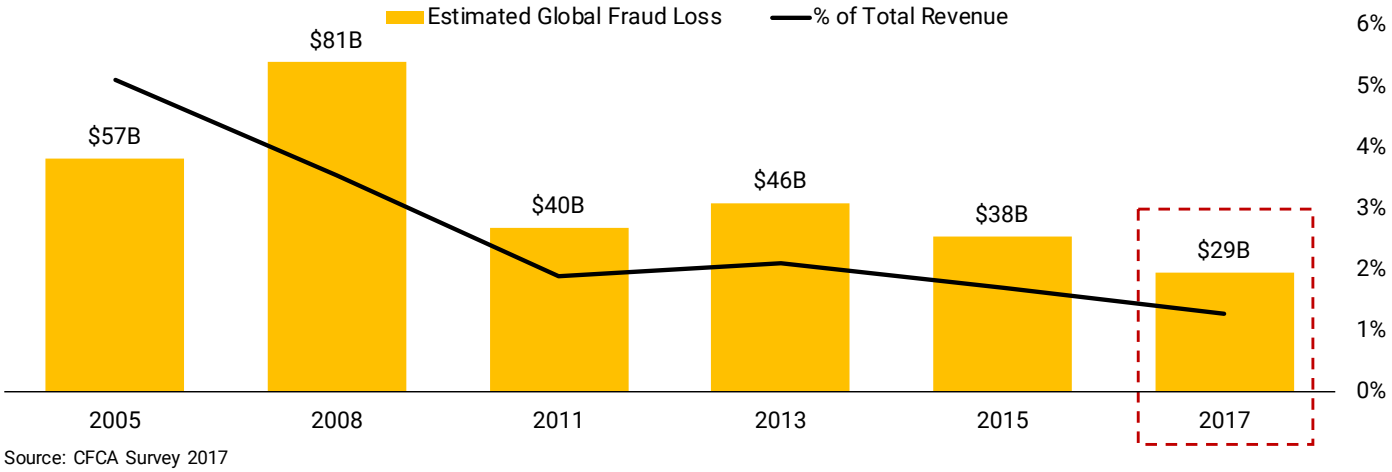
1. THE STATUS OF FRAUDULENT TRAFFIC AND ITS USE-CASES

The status of fraudulent traffic and its use-cases

Fraudulent traffic is a significant issue facing the international wholesale carrier industry. Analysis by CFCA measures the impact of fraudulent activity as $29 billion in revenue.

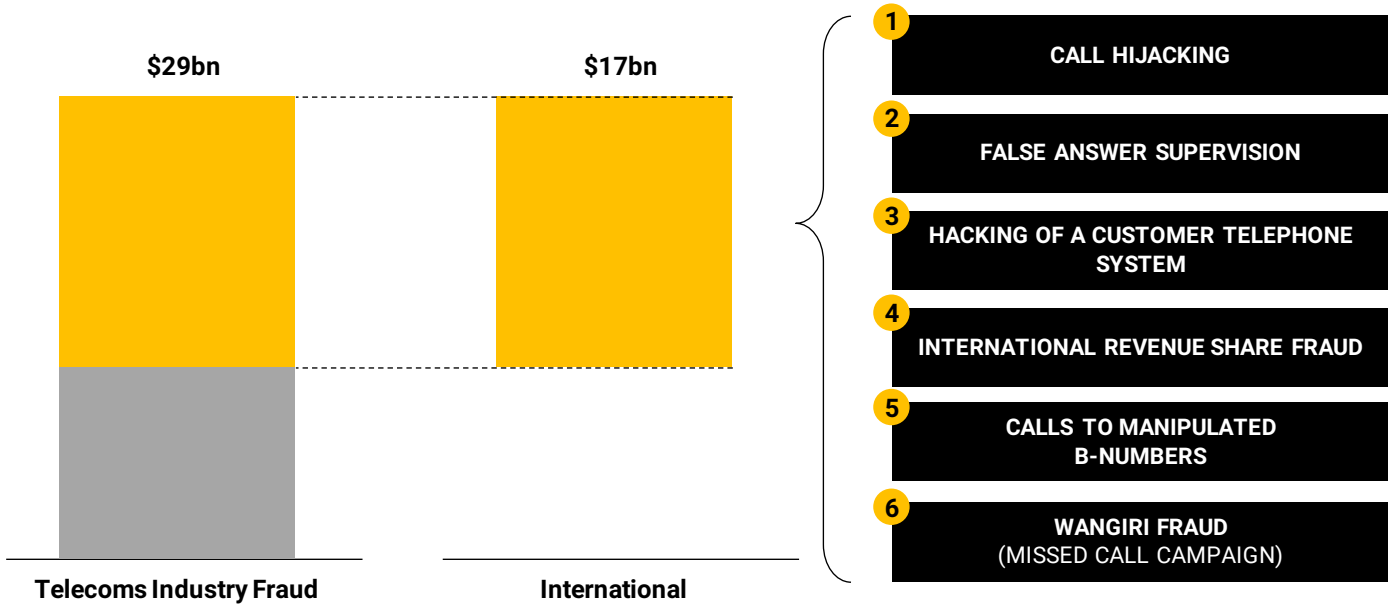
As a percentage of revenue, all telecom fraud has declined from around 5% in 2005 to little more than 1% in 2017. However, this still represents a multi-billion-dollar issue for the telecoms industry. Through CFCA analysis, approximately $17 billion worth of revenue is lost to fraud solely within international traffic.

EXHIBIT 1: CFCA ESTIMATE OF GLOBAL TELECOMS FRAUD ($BN, % OF REVENUE)



Source: CFCA Survey 2017

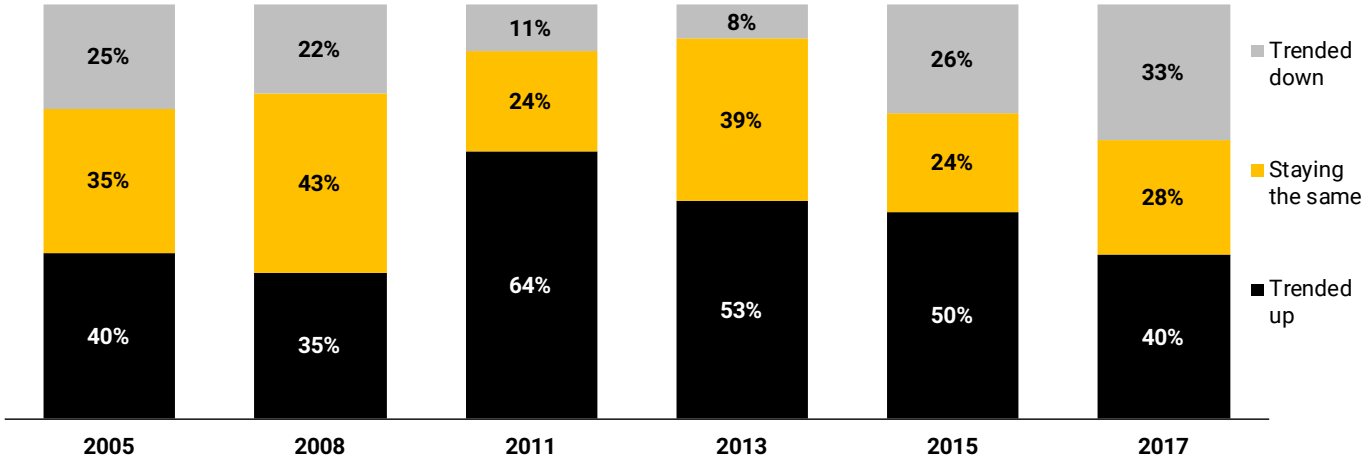
EXHIBIT 2: INTERNATIONAL AS A SHARE OF TOTAL TELECOMS FRAUD



Note: Examples of Fraud based on i3 Forum definitions; Source: CFCA Survey 2017

EXHIBIT 3: CFCA SURVEY PARTICIPANT VIEW OF FRAUD EVOLUTION

Over the past 12 months, has fraud in your company, trended up, trended down or stayed the same?
(% responses)



Source: CFCA Survey 2017

Overall, fraud has generally declined. In 2017, around 61% of respondents in 2017 reported a downward or stable trend in fraud in the previous 12 months compared with just 35% of CFCA survey respondents in 2011.

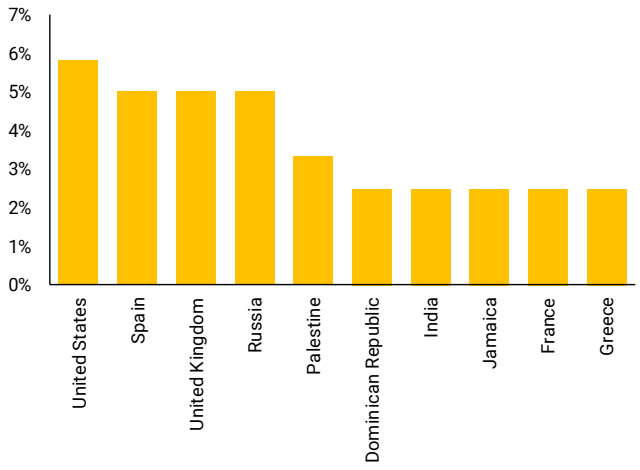
At the beginning of 2018 the ITW Global Leaders Forum ("GLF") agreed that it should take a leadership position on fraud. By March, it launched a Code of Conduct for carriers to demonstrate their commitment to a set of practices to monitor and reduce the volume and impact of fraudulent traffic in their organisations. This report has been commissioned by the GLF as the first in an annual series that will monitor the progress being made by the international carrier industry to address telecoms fraud.

Fraud cannot be isolated to any particular type or origin and its impact extends from the top line through carriers accounts to profit margin through lost opportunity cost, damaged customer experience and increased overhead to detect, eliminate, and prevent fraudulent traffic. Exhibit 4 shows the top 10 most cited countries for the origination and destination of fraud. However, when it came to ranking the top 3, numerous respondents featured countries that weren't in the top 10 most commonly cited. For example, respondents mentioned an additional 75 countries for originating fraud in their top 3 and a further 94 additional countries for fraud to be terminated in in their top 3.

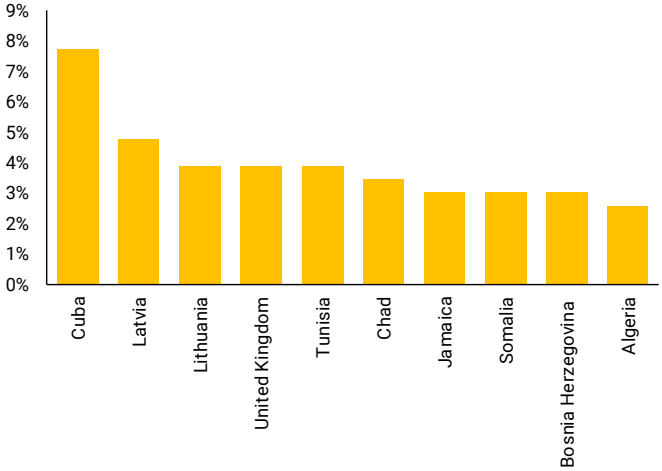
At the core of international telecoms fraud is an intent to manipulate either the origin, destination or content of a

EXHIBIT 4: TOP 10 MARKETS FOR ORIGINATION AND TERMINATION OF FRAUDULENT TRAFFIC

Top 10 Countries That Originate Fraudulent Traffic
(% responses)



Top 10 Countries That Terminate Fraudulent Traffic
(% responses)

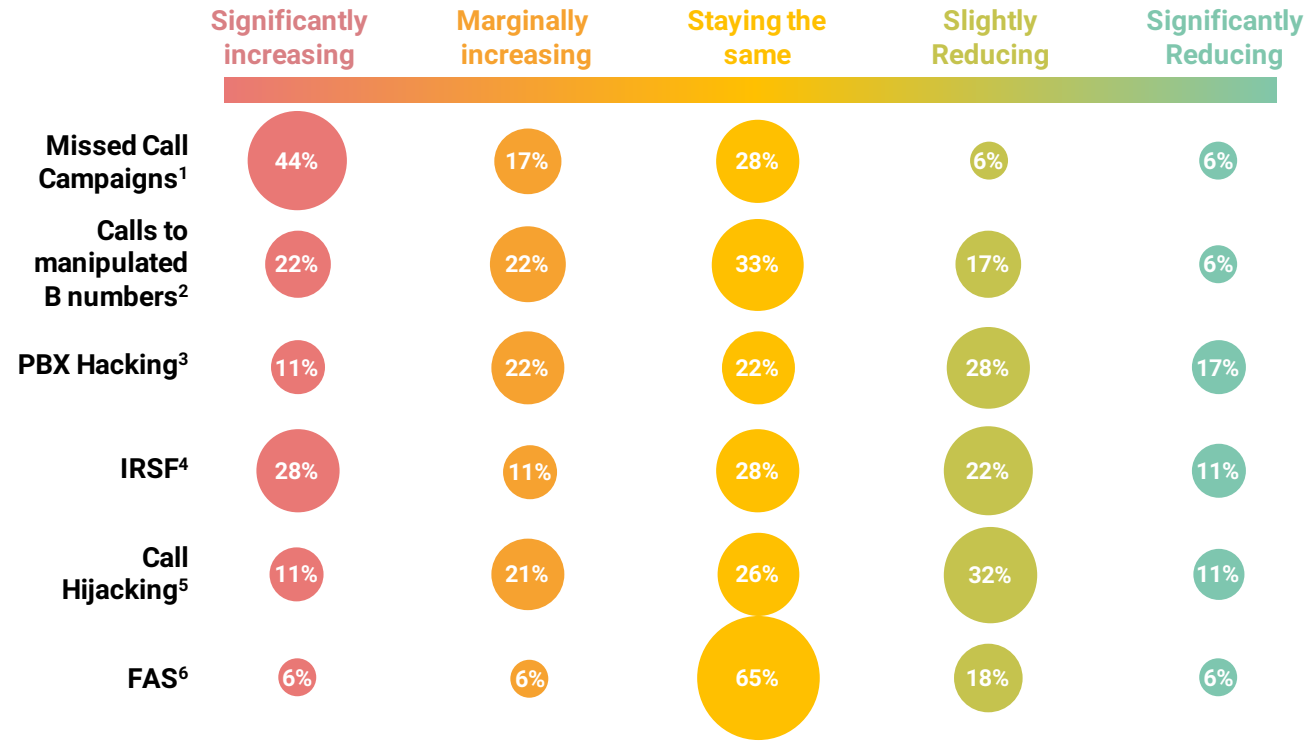


Source: CFCA Survey 2017

call by intending to extract payment before the fraudulent traffic can be disputed. This ultimately ends up placing a financial burden on carriers with some or all paid out to the party behind the fraud in the first place. This fraud takes many shapes that fall under one of the following use-case definitions, as defined by i3 Forum in its Fraud Classification Release in May 2014. From the GLF survey we see that fraud activity is also inconsistent – there is significant variance of volume and impact across use-cases.

EXHIBIT 5: CHANGING PREVALENCE OF FRAUDULENT TRAFFIC BY USE-CASE

With respect to different fraudulent traffic use-cases how has their volume and impact changed over the past 12 months?[1]
(% responses)



Notes: [1] n=18, [2] n=18, [3] n=18, [4] n=18, [5] n=19, [6] n=17, respondents without a response were not counted; Source: GLF Survey 2018, Delta Partners Analysis

Use-case 1: Call Hijacking

Call hijacking is the redirection of traffic to compromised networks or from compromised devices with the intention of maximizing call duration to maximize billing. There are two predominant scenarios:

1. Redirection of normal customer traffic to a network using a recorded message with the intention to keep the customer online for maximum time;
2. Artificial inflation of traffic from a compromised PBX or mobile phone(s)

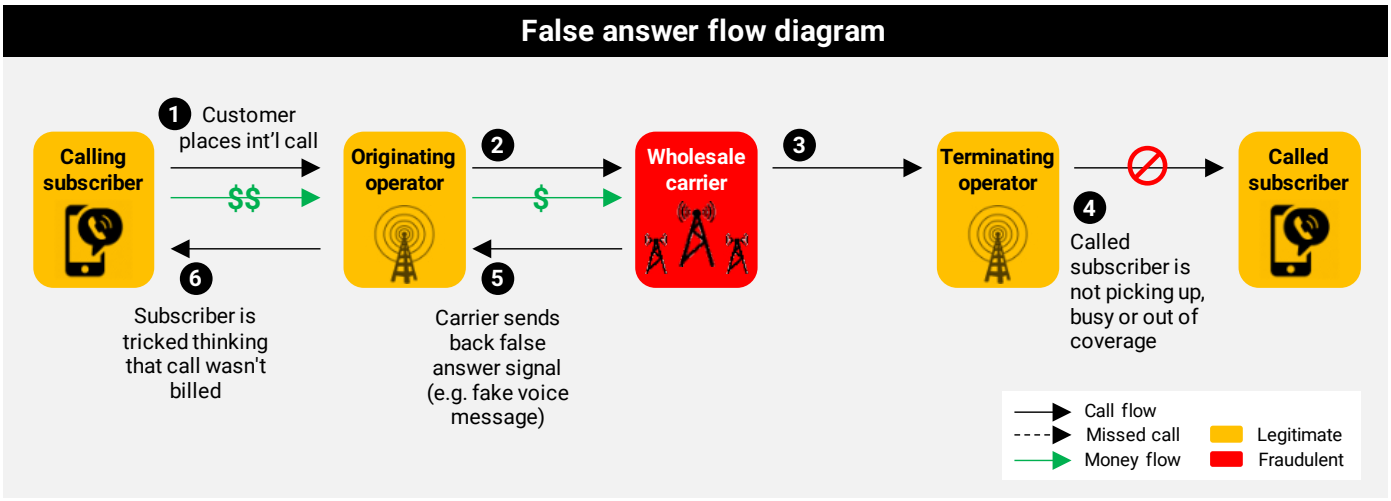
With call hijacking, the fraudulent party will ensure, through low pricing, that they are in route for a destination and will select unallocated numbers in the destination network. Their partner generates high volumes of calls to these unallocated numbers and all answered with long durations. Other carriers receiving these calls will either fail them as "number unallocated" or return a route advance signal which simply redirects traffic to the fraudulent supplier.

Just over 30% of respondents to the GLF survey said that over the past year, the volume of call hijacking has increased, while just under 45% saw a decline. A concerted effort to drop problematic customers was cited as a key reason for some carriers identifying a decrease

Use-case 2: False Answer Supervision

False Answer Supervision (FAS) involves a party in the traffic flow chain returning a false answer signal to the carriers earlier in the chain, which initiates billing for all parties. There are two variants of FAS:

EXHIBIT 6: OVERVIEW OF FALSE ANSWER SUPERVISION



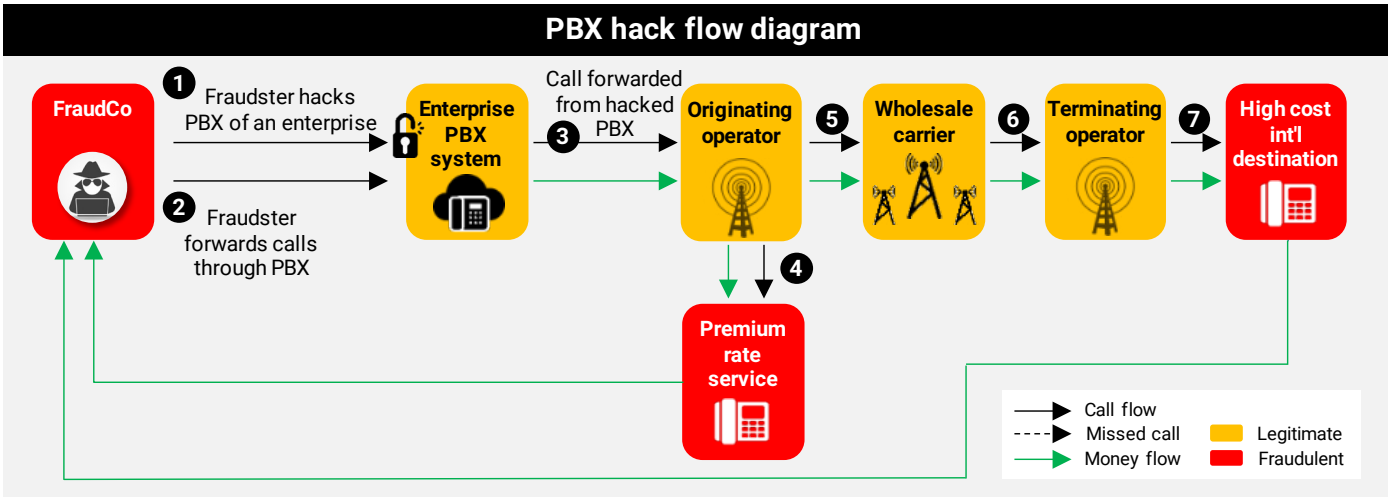
Source: i3 Forum

1. The fraudulent party continues to try to establish the call, in which case, the caller pays for ringing regardless of whether the distant customer answers or not;
2. The fraudulent party routes the call to a recorded message that first plays a ringing tone and then plays a recording that mimics an answer and conversation. This is known as call diversion

The recording that mimics a conversation is created with the intent of keeping the calling customer on the line and paying for the call for as long as possible.

Only 12% of respondents reported a significant or slight increase over the past 12 months while 65% indicated that the amount of FAS has stayed the same. For carriers that reported a stable or increasing volume of FAS, the issue of limited recourse of performing tests or limited ability to test vendors was identified. One carrier noted: "FAS is always an issue because it can happen anywhere on any route, and the only thing we can do it to test and use tested vendors."

EXHIBIT 7: OVERVIEW OF PBX HACK



Source: i3 Forum

Use-case 3: Hacking a customer Telephone System / Software Manipulation

Hacking a customer Telephone System / Software Manipulation, also known as PBX hacking, consists of attackers infiltrating retail customer telephone systems by accessing admin passwords.

After gaining access to mobile smart phone equipment or a retail customer telephone system, the fraudulent party establishes a call-forwarding or a dial-thru to a high price destination. Then the attacker originates many calls as possible to the infiltrated telephone system, usually from an IP-based source to avoid detection and the system forwards the calls to the high price destination. In other cases the attacker programs software which initiates calls automatically, avoiding the need to generate incoming calls.

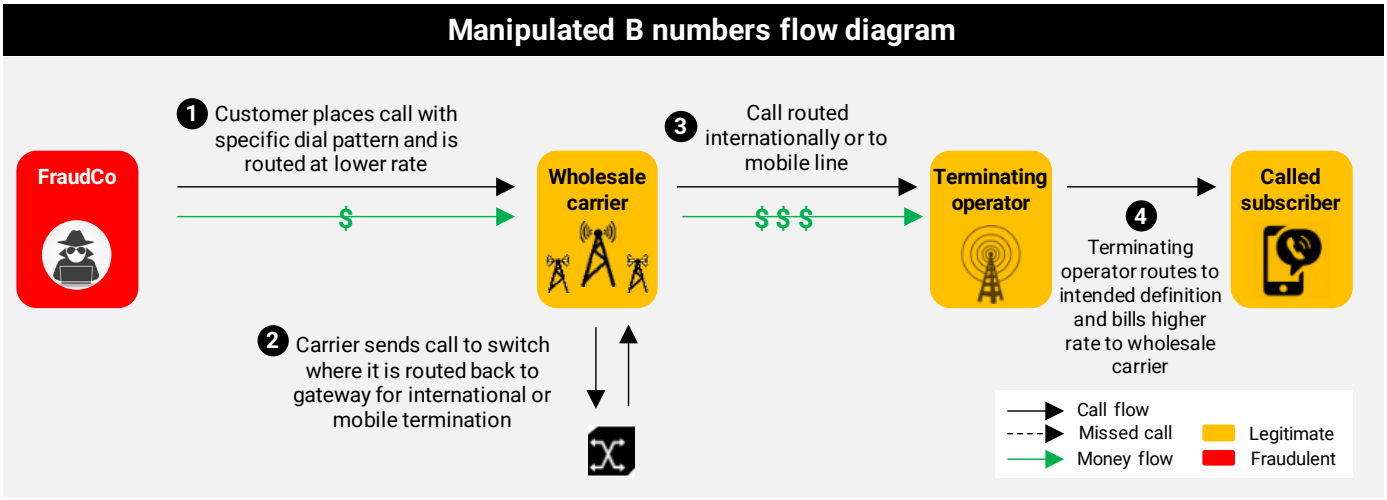
Carriers were split in reporting decreases and increases in this type of hacking with little more than 30% reporting an increase and around 45% reporting a decrease over the past year.

Use-case 4: Calls to manipulated B-numbers

Calls to manipulated B-numbers are defined as calls containing two country codes and the fraudulent party takes advantage of the difference in cost between the destinations

1. In routing schemes with two country codes (either by design or inadvertently left open), end customers or originating operators will deliberately manipulate numbers to take advantage of cases where the terminating carrier will inadvertently route traffic to a higher cost destination (e.g., to a mobile phone or international destination) while billing at a lower, in-country rate.
2. Fraudulent parties will add the home country code of the terminating carrier at the front of the number string to get charged a lower rate. The principle here - for the fraudulent parties - is to select such carriers where actual destination is significantly more expensive than the terminating carrier's normal rate.

EXHIBIT 8: OVERVIEW OF MANIPULATED B NUMBERS



Source: i3 Forum

Therefore, the originating operator will receive an invoice from the carrier after a call termination in the carrier's home country, but at the same time the carrier will receive an invoice from the real termination country's operator. The difference between the two invoices causes a financial loss for the carrier.

Just under 45% of carriers reported an increase or significant increase in manipulated calls to B numbers over the last twelve months while almost 35% of respondents said the volume of calls to manipulated B numbers remained stable. "We have seen some marginal increases for manipulated B numbers, and we are taking efforts to correctly route and bill traffic. For B numbers, we see it originate internally and externally to the EU; fraudsters see the higher billing outside the EU as more potent target," said one surveyed.

Use-case 5: Wangiri Fraud (Missed call campaign)

Wangiri Fraud entails fraudulent parties initiating texts or calls that immediately hang up or drop. The intention is to deceive the customer into calling the number back and keeping them on the line to maximize billing.

The fraudulent party originates, via machine, calls to mobile customers in a specific country or operator. Their approach is to generate calls to thousands/millions of those customers and immediately hanging up/dropping the call after one or two rings. The fraud can also be generated by massive SMS spamming campaigns. Manipulation is also performed on the A-number field, where the fraudster incorporates the same number for all calls, usually a hijacked number or a premium/high rated destination number on an International Premium Rate Service.

The deception occurs as the unsuspecting customer notices the missed call or short SMS message and a proportion decide to return the call or dial the number from the SMS message. When calling back, the target subscriber will usually hear a recording that intends to keep the caller on the line for as long as possible.

Respondents reported the largest increase in Wangiri Fraud of all the use cases surveyed with just under 45% reporting a significant increase and almost 20% reporting a slight increase in the last 12 months. Around 10% reported a decrease in Wangiri Fraud. "Wangiri attacks are just constant and all over. They don't pose much of an issue due to low value risk, but they are very visible due to customer interaction," according to one of the respondents.

Use-case 6: International Revenue Share Fraud

International Revenue Share Fraud ("IRSF") occurs by failing to provide a promised service, deliberately extending the length of a call, or generating non-legitimate or artificially inflated traffic in a high revenue regular destination or an International Premium Rate Services (IPRS) destination.

IRSF is one of the more common ways a fraudulent party extracts value from a compromised system. Due to relatively higher rates attributed with to high revenue regular destinations (e.g. Cuba) and IPRS destinations, these route destinations remain extremely sensitive to fraud given the significant revenue that can be generated in a relatively short period of time. Routing any fraudulent traffic to either of these destination types is the most minutes of use (MOU) efficient way of extracting value from fraudulent traffic.

There was variance across the base of respondents regarding IRSF, with just under 30% reporting a significant increase and just under 30% reporting IRSF staying the same in the last 12 months. The smallest percentage responses were significant reduction and marginal increase with just over 10% of respondents reporting these to be the case over the last 12 months. Carriers reported that "IRSF is a fraud that is particularly difficult to combat; the number goes directly to end customer, and normally wouldn't be completed. However, when you are going to terminate through a carrier that negligently or willfully participates in the fraud, they will complete the call. It takes a lot of manipulation of the middle man, but it's like buying a fake Rolex directly from Rolex store," noted one responder.

2. TRENDS IMPACTING FRAUDULENT TRAFFIC

Overview: Changes in Prevalence and Types of Fraud

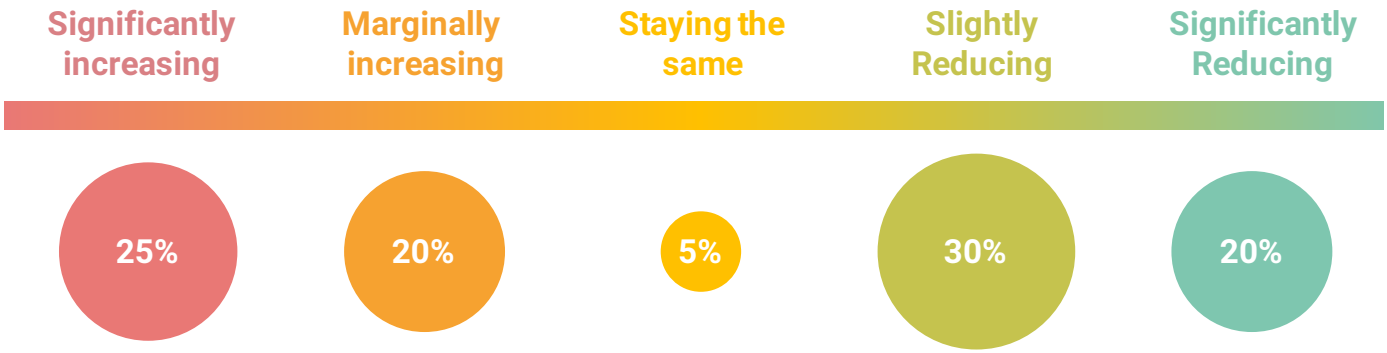
At an industry level two primary macro trends have been identified: technology enables a greater frequency of attempted attacks, while the average value loss of each attack has declined. Technology is a double-edged sword as it provides the enablement of better data creation, collection, consumption, and speed of response, but also allows new fraud types and gives fraudsters greater accessibility, scale, and sophistication.

Individual carriers have experienced diverging trends in fraud. While 45% of carriers believe fraud is decreasing, 50% believe it is increasing. One carrier said: "There is always a back and forth with the fraudster. It is a continuous battle that doesn't stop. If we aren't detecting fraud, then it is a time to worry." Respondents attributed this variance in the trend in fraud to multiple factors including difference geographic footprint, customer segments covered, an effectiveness of internal efforts to combat fraud. As International Long-Distance traffic adjusts to the emergence of VOIP, carriers experience different trends due to the multiple factors listed previously as well as those some factors play a role in customers' and partners' networks as well.

Carriers report that, globally, fraud has been increasing in frequency with mixed net effects depending on customer types and footprints with an observation from one carrier that: "We are seeing countries where the whole country

EXHIBIT 9: CARRIER VIEW OF CHANGE IN FRAUDULENT TRAFFIC OVER PAST 12 MONTHS

How has the volume and impact of fraudulent traffic hitting your organization changed in the past 12 months?
(% responses)



Source: GLF Survey 2018, Delta Partners Analysis

is spammed." In this specific case, simple technology has allowed relatively unsophisticated fraudsters to systematically attack every number available in a country code. However, successful attacks are reportedly becoming less severe as carriers improve detection and removal capabilities.

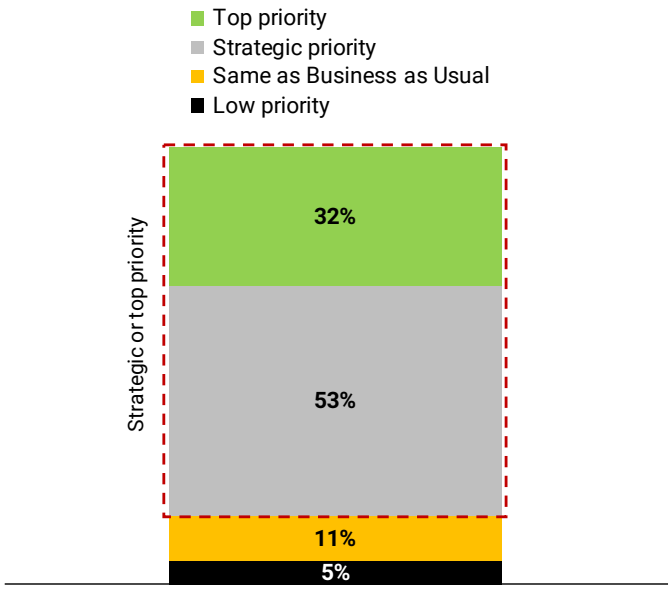
The type of fraud observed varies also. Carriers generally report an increase in missed call campaigns and PBX hacking. The prevalence of call hijacking, however, has decreased. Carriers are seeing evolving techniques and more sophisticated methods of fraud. New technologies, such as cloud-based offerings, provide easy prey for fraudsters as the amount of publicly facing ports and connections are dramatically increased. While new tools, such as automation, serve to expand the breadth and reach of fraudsters with the proliferation of automated actions like robo-dialing to facilitate a Wangiri hack being utilized by relatively unsophisticated fraudsters.

Carriers have not sat idle while this evolution of fraud has happened. They are increasingly prioritizing fraud and ways to mitigate it. Nearly all survey respondents said that fraudulent traffic was an important topic for their organization, and all respondents said that its importance has persisted or increased over the past 12 months. For example, one carrier explained: "We had a very manual process before, and then fraud managment became a core strategy for us. We brought in data analysis, developed algorithms, and got close to real time."

Carriers in the GLF survey have taken steps both through

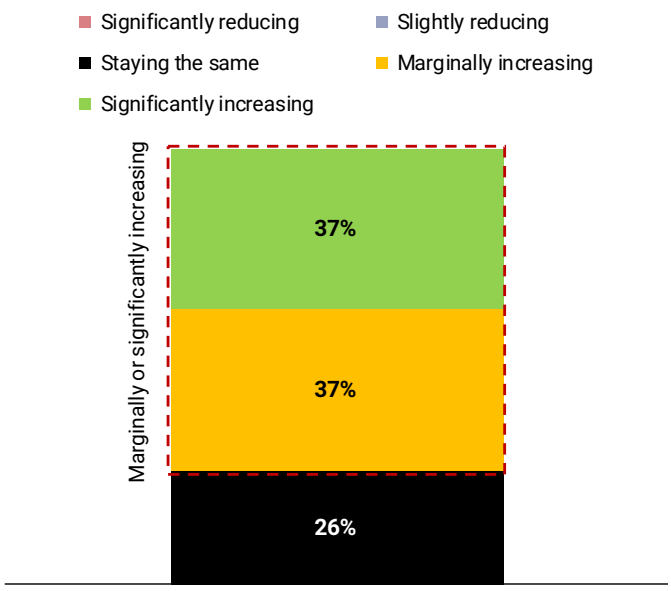
EXHIBIT 10: CARRIER VIEW OF PRIORITY OF FRAUDULENT TRAFFIC MANAGEMENT WITHIN THEIR ORGANISATION

Where would you rank the importance of fraudulent traffic as a topic in your organisation?
(% responses)



Where would you rank the importance of fraudulent traffic as a topic in your organisation?

How has the importance of fraudulent traffic management in your organization changed over the past 12 months?
(% responses)



How has the importance of fraudulent traffic management in your organisation changed over the past 12 months?

Source: GLF Survey 2018, Delta Partners Analysis

organizational changes, process improvement and the proliferation of tools used to expand and improve fraud management capabilities. There are three primary areas:

1. **Organizational Changes:** one participant integrated fraud management teams with routing teams to improve collaboration and decision-making efficiency;
2. **Process Improvement:** historically, fraud alerts would be sent to customers to gain approval to act, but, recently, carriers are seeking to get pre-approval so that action can be taken much sooner;
3. **Proliferation of Tools:** machine learning and use of blockchain-based solutions are seen by many carriers as the focus of investment in the near future

Many carriers are at the beginning of the learning curve with new technology and tools and expect to progress as they become more sophisticated in detecting fraud. Carriers can learn from the fraud they detect as it makes them more efficient in the face of future attacks.

While the proportion of smaller attacks has risen, the number of larger attacks has declined. Participants said recently implemented tools have led to the detection of more attacks but because of improved tools and infrastructure the response time is much lower. Thus, the value per attack is reportedly dropping or being eliminated entirely. One carrier, which represented a common view, said: "We recently implementing a next gen tool and are detecting more attacks, but, because we are a lot faster, the value per attack is dropping or being eliminated entirely. So, we are experiencing and detecting more cases, but the overall fraud value is dropping."

There will always be a back and forth battle against fraud; as one weakness is resolved, another will likely appear. Carriers current goal is simply to stop the most potent attacks and systemically make it more difficult to perpetuate attacks in the future. Two of the more important use-cases, PBX hacking and Wangiri, have become a focus of many carriers for differing reasons as discussed below:

Deep Dive 1: Focus on PBX hacking

Due to the large potential impact of a single attack, PBX hacking is a top focus for most carriers. Mitigating efforts are to find the attack early and minimize the damage as much as possible. Efforts are made to encourage better behavior from customers thought improved network security at the customer. Participants also report attempts to offload some of the risk onto the customer through prepaid services or insurance, especially in the case of repeat offenders. This was an area of significant debate with the carriers:

- "A significant amount of our fraud has been eliminated by cutting ties with problematic customers";
- "Three years ago, this was a huge topic within our organization, and then we developed our internal system, integrated new tools, and ended relationships with problematic customers. Now, fraud is important but not nearly so relative to back then." ;
- "Most of our effort has been looking for common denominators whether that might be destination, suppliers, or customers. As a result, we have ended a number of commercial relationships."

PBX hacking vulnerability is distributed among end customers. A carrier's network is only as secure as weakest customer's security. To combat this issue in extreme examples, service will be discontinued from customers to avoid risk that has been deemed unacceptable after several failed opportunities to mitigate customer risk. The frequency of successful, large-scale PBX hacking attacks has been fallen according to several participants in this study. However, specific policies, like the European origin-based 4G pricing increased the severity of a PBX hacking attack. In this specific case, it was historically unnecessary to investigate the Calling Line Identification (CLI) as no one had to question that validity of the CLI, but with the introduction of the origin-based rating concept has been taken advantage of by fraudsters who manipulate the policy to ensure the highest billing rates possible.

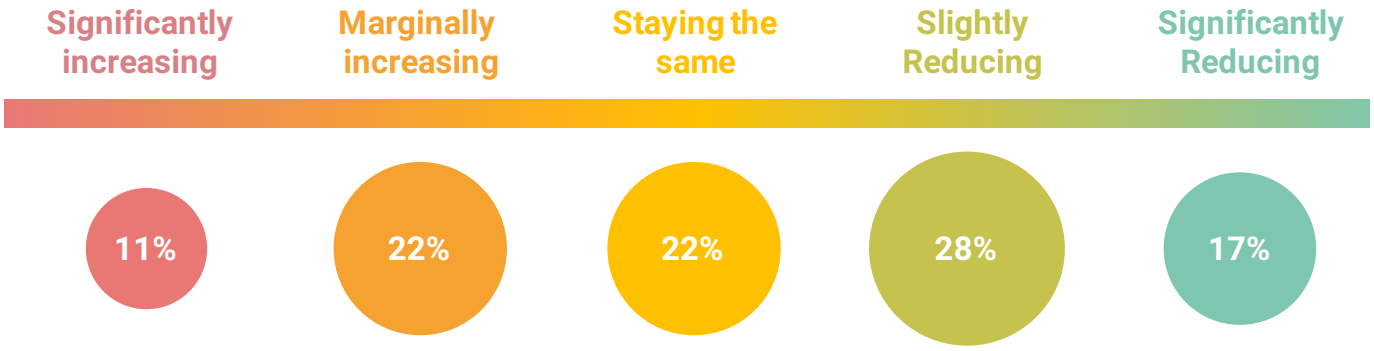
11% of survey respondents report that PBX hacking has significantly increased over the past 12 months. Carriers suggest this type of fraud has been particularly difficult to combat due to risk originating from the end users and constantly-changing destinations between countries from one month to another.

Ultimately, PBX hacking does result in large material attacks but, thanks to high prioritization and improved fraud management, it is "nowhere near as frequent; PBX hacking attacks used to be as high 60-80 per year in recent past, but now we are down to one or two significant attacks a year."

EXHIBIT 11: CARRIERS' VIEW OF THE EVOLUTION OF PBX HACKING

With respect to PBX Hacking, how the volume and impact changed over the past 12 months?[1]

(% responses)

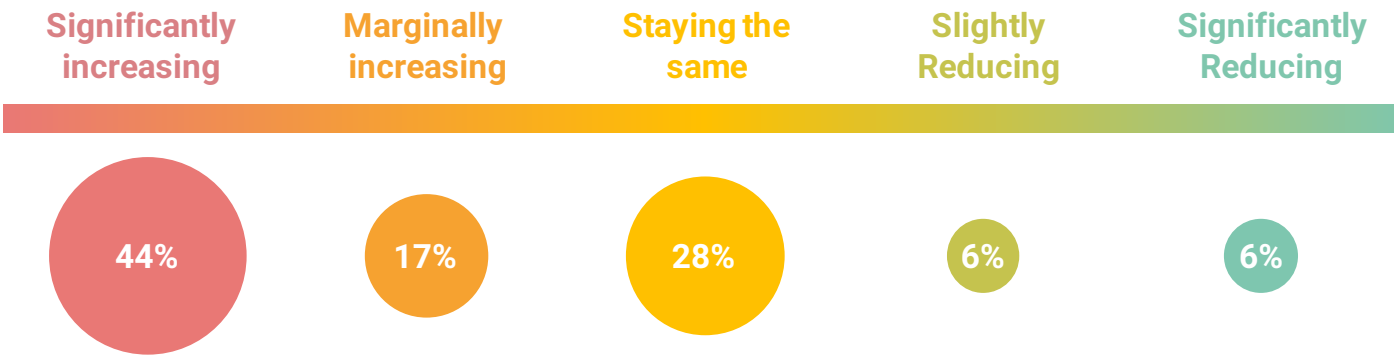


Notes: 1 n=18, respondents without a response were not counted
Source: GLF Survey 2018, Delta Partners Analysis

EXHIBIT 12: CARRIERS' VIEW OF THE EVOLUTION OF WANGIRI FRAUD

With respect to wangiri, how the volume and impact changed over the past 12 months?[1]

(% responses)



Notes: 1 n=18, respondents without a response were not counted
Source: GLF Survey 2018, Delta Partners Analysis

Deep Dive 2: Assessment on the increase in FAS/Wangiri attacks as well as the lack of severity

While not as serious as PBX hacking due the inherently low value of an attack that relies on unwitting customer behavior, Wangiri presents an issue because of the nuisance it creates in the form of spam calls and SMS messaging. This fraud use-case has lower barriers to entry, relative to a use-case like PBX hacking, given that there is no requirement to gain access to a system and is constantly changing origins and destinations, which makes it both common and hard to eradicate. Wangiri rarely reaches a massive scale due to its reliance on the actions of customers which also can make it difficult to identify among normal traffic.

Carriers in high-cost markets are reporting more Wangiri attacks, but even outside of those markets Wangiri attacks have been especially prevalent relative to other fraud types. Over half of all respondents said they have experienced an increase in missed call campaigns over the past year. Though Wangiri attacks are common, they are considered less severe — and therefore less significant — than other types of fraud. One carrier noted: "Wangiri attacks are just constant and all over. They don't pose much of an issue due to low value risk, but they are very visible to the end customers."

Deep Dive 3: Customer management efforts made to reduce volume/impact of fraudulent traffic

It is evident that there is an arms race between carriers and fraudsters when it comes to fraudulent traffic. Fraudsters improve their tools and sophistication as quickly while carriers develop new ways to counter them. The volume and impact of fraudulent traffic has grown with the increasing number of customers and usage of carrier networks. At the same time, carriers need to balance resources while keeping pace with fraudsters. Carriers may reach a point where there are diminishing returns to adding resources to fraud mitigation. Therefore, there comes a point where higher certainty in fraud mitigation may be not be worth the effort required.

Carriers are dealing with missed call campaigns by removing customers or limiting customer's international access. For example, if a carrier detects fraud coming repeatedly from a single customer, they may remove that customer. It was noted that "Wangiri in particular, but also other fraud use-cases, have been declining because we removed problematic customers or limited international access of other customer. Much of our overall success is due to active customer management. We have simply been ending relationships with 'bad customers'. A big part of our historical fraud was due to a bad customer base."

Carriers can also reduce risk of fraud by vetting new customers. To support this, the i3 Forum has developed a pre-screening questionnaire that can be used to get a better understanding of a vendor's traffic. Carriers report managing customers by gathering a better understanding beforehand to reduce fraudulent traffic.

3. ORGANISATIONAL IMPORTANCE OF REDUCING FRAUDULENT TRAFFIC

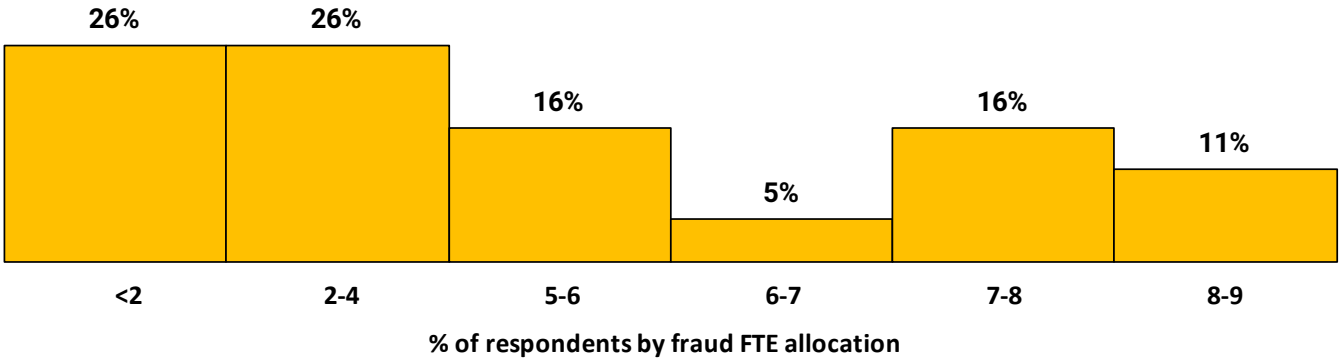
Factors Determining Number of FTEs Allocated to Fraud Management

A company's size and use of technology creates a large variation among FTEs dedicated to fraud management among carriers. The carriers that state higher prioritization of fraud management tend to have larger teams overall, encompassing both dedicated employees and those with partial focus on fraud management. From respondents to the GLF survey, the size of fraud team ranges from 1 to 12 with a mean size of 4.5.

Carriers report that team placement within the organization can also have influence on effectiveness with the most successful teams are incorporated in the commercial decision-making process while maintaining independence from revenue and profit goals. There is also a correlation between the size of fraud team and the prioritization towards fraud within the organisation. Respondents who prioritize fraud management but have relatively small FTE allocation, supplement their small teams with informal coordination with related teams, investments in technology to leverage their small teams, or are in the process of expanding their smaller team.

EXHIBIT 13: DISTRIBUTION OF SURVEY RESPONDENTS FTE FOCUSED ON FRAUDULENT TRAFFIC

Distribution of Employee Allocation[1]
(Number of FTEs)



Notes: [1] n=19, respondents without a response were not counted
Source: GLF Survey 2018, Delta Partners Analysis

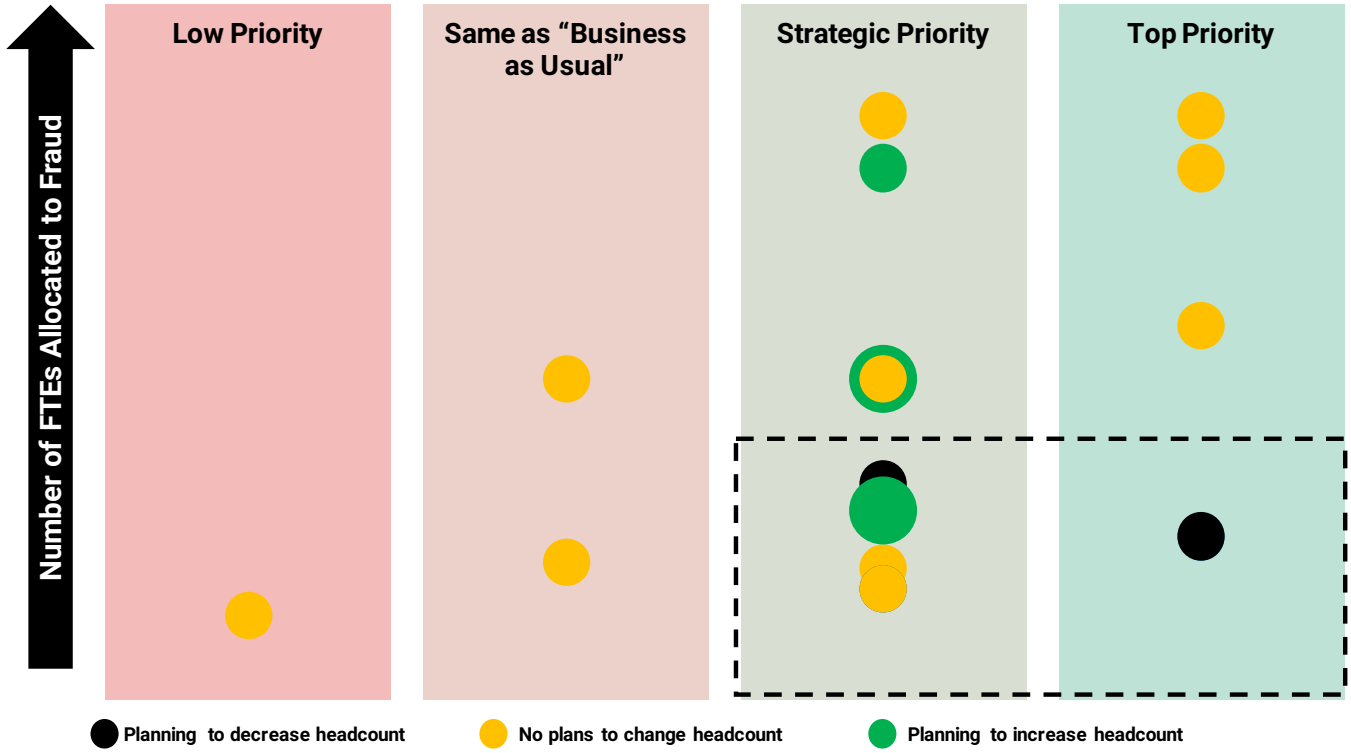
The structure and size of fraud management teams within carriers varies based upon several factors. Based on customer profile, carriers may not feel the need to dedicate a significant number of employees to fraud management. One such carrier stated: "As most of our customers are retail, we focus more on payment fraud". Other carriers handle fraud management by structuring the team with a limited number of dedicated employees and a variety of employees from other teams focusing a portion of time on fraud management. Carriers report that the most successful teams consisted of only dedicated employees, rather than larger teams with multiple partially dedicated employees.

Placement of fraud teams

The placement of the fraud management team within the carrier organization also plays an important role in the effectiveness of the team. The fraud management team is responsible for identifying and eliminating fraudulent traffic sources. The routing team, which is responsible for originally choosing the traffic sources, often is not incentivized to reject potentially fraudulent suppliers as they are focused on revenue maximization and cost reduction – as such, there can be opposing incentives. A system whereby the fraud management team is directly incentivized by the maximization of revenue and profit risks hesitation from the fraud management team in shutting down a fraudulent revenue source based on mixed incentives. Aligning the incentives of the fraud management team

EXHIBIT 14: COMPARING PRIORITIZATION OF FRAUD WITH THE NUMBER OF FTE ALLOCATED TO FRAUDULENT TRAFFIC

Comparison of prioritization and number of FTEs allocated to managing fraud
(Number of FTEs, bubble size denotes number of respondents, color denotes plans to change headcount)



Source: GLF Survey 2018, Delta Partners Analysis

with maximization of profit and revenue creates the risk of mixed incentives but removing the fraud management team from the commercial decision-making process can cause an organization to lose sight of fraud elimination altogether. As one carrier stated, organizations "need to get people willing to pay more for less fraud. Stated bill rates that are 10% under market rate will end up costing more as calls are artificially extended 15-25%".

Interviews with carriers highlights the importance of multiple factors outside of the sheer size of a fraud management team. Significant factors in determining effectiveness of fraud management identified in interviews centered around the following themes:

1. Positioning of the team within the organization: teams may be placed in-line with product teams, revenue assurance teams, sales, the NOC, and several other options
2. Focus of fraud management teams: depending on customer dynamics and geographic footprint, a fraud management might be focused more on payment fraud, SIM box detection or on documentation and proper reporting to law enforcement as appropriate
3. Ability of the team to leverage technology: recent tools have become a potent ingredient in building efficient, effective fraud management teams. Due to the amount of data created by a network, aggregation and analysis of large data sets can greatly leverage the time and energy of fraud management teams
4. 24/7 coverage: the average time lag between an attack, detection, and action can be exacerbated when a fraud team lacks 24/7 coverage. Respondents note that fraudsters leverage this fact as many attacks are initiated during evenings and weekends

4. IMPACT OF FRAUD: EXTENDING BEYOND THE CARRIER BUSINESS MODEL

Fraudulent traffic as a tool for international crime and terrorism

Fraudulent traffic has impacts far beyond a carrier's commercial performance. A normal customer doesn't accidently launch a Wangiri attack. As such, fraudulent traffic use-cases are being intentionally exploited and in cases this can be by criminal organizations which extends all the way to financing terrorist activities.

Fraudulent traffic is one of the ways that criminal and terrorist organizations can monetize fraudulent traffic through the theft of sim cards and cellphones, employee theft and identity theft. Multiple carriers in discussions to produce this report noted this connection, stating that "these shady organizations perpetuating fraud on our networks are linked to organized crime or even terrorist organizations." One of the reasons for the prevalence of fraudulent traffic is the fact that it can be used as a means to obscure or anonymize the movement of illicit funds—especially in cases where money is crossing international borders. Most of this activity is given little thought, however. As one respondent suggested, "There needs to be big case to make this a focus."

But the potential for criminal organizations goes beyond theory. Carriers noted specific cases where fraudulent traffic was used for illicit purposes. One survey respondent noted that, "We had an American agency that tracked funds derived from fraudulent traffic to a source to Al Qaeda and linked to a specific bombing. I always tell people that it's not 'just fraud' and there are huge implications." Carriers know best how cases of fraud can have far reaching repercussions. Another carrier noted that "at a conference in Barcelona, the head of Spanish cybercrime discussed an Interpol investigation. In the investigation it became clear that organized crime in Pakistan, which was responsible for fraudulent traffic, was using that income to finance terrorism." A case in Italy was reported where coding premium numbers were used for money laundering by the mafia. This case resulted in senior officials within Telecom Italia being removed.

Identifying culprits and coordinating with law enforcement can have powerful repercussions by opening investigations on actions that would otherwise go unnoticed. Focusing on mitigating fraudulent traffic would have positive consequences that go beyond the carrier itself.

PART 2

MANAGING CARRIERS' RESPONSE

1

While most carriers can identify and remove fraudulent traffic from their networks within six hours, contractual service agreements and a fear of mistakenly blocking legitimate traffic can make removing fraudulent traffic complex.

2

Proactive customer management and allocating additional FTE are the two primary internal carrier requirements to reduce fraudulent traffic - only 5% carriers see technical innovation, such as AI, as a reason to reduce FTE focused on fraud management

1. ENSURING AN EFFECTIVE RESPONSE

Speed of detection and removal

Fraudulent actors pursue opportunities to perpetuate fraud for the maximum amount of time while carriers continuously search for entry points to prevent further abuse. The speed at which carriers can detect and react to fraudulent traffic can make a significant difference in reclaimed revenue as attacks accumulate.

Carriers interviewed place high importance on quickly identifying and removing fraudulent traffic from their network with just under 75% identifying the fraudulent traffic within three hours and almost 90% able to remove it three hours after identifying the fraudulent traffic.

Carrier interviews explain the barriers in place and the steps taken to improve response and action time against fraudulent attacks. According to experts interviewed from leading carriers, reduction in response time can be difficult for several reasons related to the reluctance to act quickly due to the fear of stopping legitimate traffic, including the need to establish a pattern from a large amount of data, the limited ability of the network in generating real-time data and the confirmation with the client to determine whether the fraudulent traffic was legitimate. Additionally, carriers have stringent contractual obligations that do not allow customers' traffic to be blocked unless there are specific agreements in place. As the carrier can be a mere conduit of the traffic with service level agreements in place it cannot make a unilateral decision to block traffic that it expects to be fraudulent without agreement of their customer. This puts the carrier in a complicated situation when it detects fraudulent traffic, and as of today there is no standard framework in place across carriers for how this should be managed.

Carriers emphasized automation and infrastructural upgrades as the priorities to reduce the time between occurrence of a fraudulent event and an action taken by the carrier.

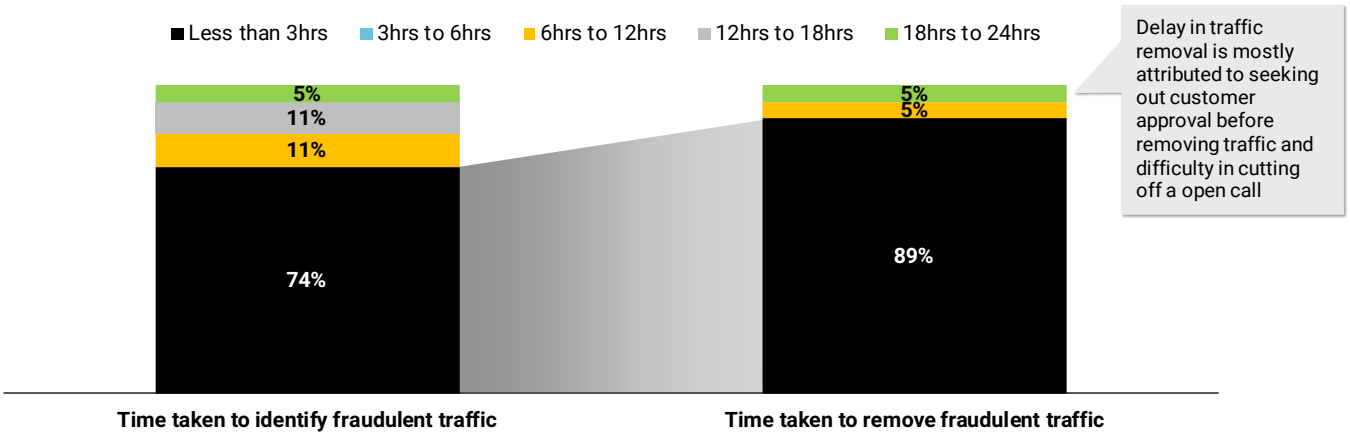
2. INVESTING IN FRAUDULENT TRAFFIC REDUCTION

Carriers continue to advance fraud management capabilities through personnel and technology advancement. Interviews confirm that carriers have been investing in assets to simplify and improve the fraud detection process. Nearly 70% of respondents stated they would increase investment in fraud management infrastructure over the next year and 20% of respondents planned to increase FTE including several experts who stated that they would add FTE to provide 24/7 coverage.

Carriers identified two types of investments that provided the greatest return on investment, namely the active

EXHIBIT 15: CARRIERS' VIEW ON ABILITY TO IDENTIFY AND REMOVE FRAUDULENT TRAFFIC FROM THEIR NETWORKS

How long does it take for you to identify and remove fraudulent traffic on your network?
(% responses)



Source: GLF Survey 2018, Delta Partners Analysis

EXHIBIT 16: EXAMPLES OF INVESTMENT TO REDUCE LAG-TIME TO IDENTIFICATION AND REMOVAL OF FRAUDULENT TRAFFIC

Degree of sophistication

Legacy networks that were built incrementally can present a problem. There is even a large carrier still operating off Nortel DMS switches. Even if it isn't to that extreme, it can take time to generate a CDR. As everything is moved to IP this is solved, but much of the delay is on the switch side.

Time to response depends on what services the customer is enrolled in. If not enrolled in any, we just send an alarm. Many customers enroll in features and it takes less than 20 minutes to remove traffic when it exceeds the acceptable level and when triggered.

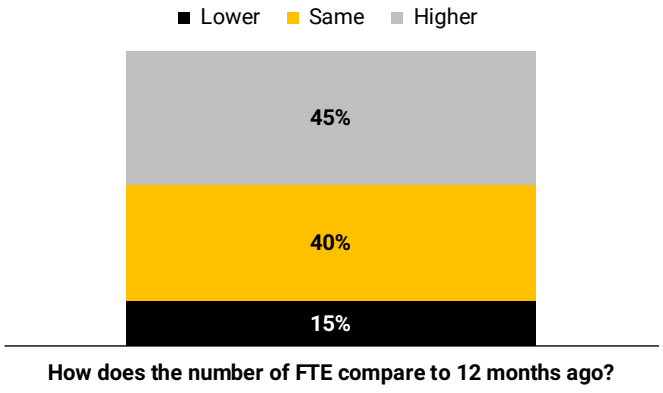
Not long ago, we had a manual process. Then fraud management became a core strategy, and we brought in tools for data analysis and algorithms. We brought in some new systems and machines that can consume that much data and now we have gotten close to real time

A home-grown system that can ID and block a call in 15 min, but the call will go until done. We have a two-prong approach between us and the fraud department. Used to be very manual, but now our efforts are on fraud dept to automate.

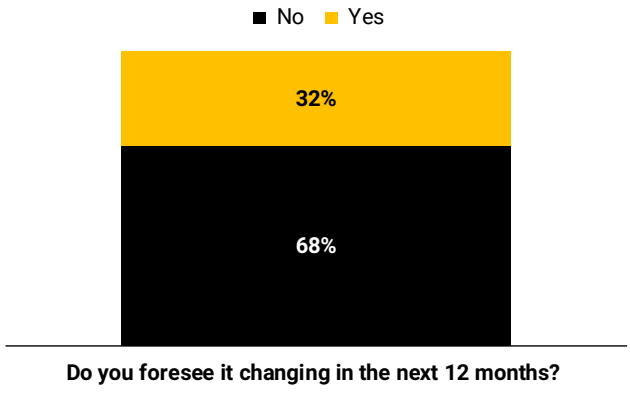
Source: GLF Fraud Survey 2018

EXHIBIT 17: CARRIERS' VIEW OF CHANGES TO THEIR FTE ADDRESSING FRAUDULENT TRAFFIC

How does the number of FTE focused on fraudulent traffic compare to 12 months ago?
(% responses)



Do you foresee it changing in the next 12 months?[1]
(% responses)



Source: GLF Fraud Survey 2018; note: [1] n=19, respondents not providing an answer were not counted

management of customers by dropping known bad customers and reallocating the coverage of FTE by scheduling employees to ensure a 24/7 operation.

Carriers perceive technological innovation as a measure to support fraudulent traffic prevention. However, only 5% of respondents specifically cite machine learning and automation as causes for reducing FTE. Collectively carriers report some on the most impactful investments happening within the addition and expansion of tools and technology, but these tools act to expand the capabilities of FTE instead of replacing them. Many tools enable the conversion of what were, historically, manual processes into automated processes; this conversion, reciprocally, creates more data sources enabling more analysis and automation. This cycle further leverages FTE' time by focusing their work and increasing the efficiency and impact of their investigations and analysis. While still in the initial stages of implementation, utilization of blockchain technology has been reported to have some initial successful uses in simplifying and speeding up the dispute process between carriers.

PART 3

MEASURING THE IMPACT

1

Nearly all carriers track some metrics to manage fraudulent traffic. However, there is a lack of consistency in metrics tracked and less than 70% of carriers report these to the CEO's level

2

There is a disconnect between carriers prioritisation of fraudulent traffic as a strategic priority and the recognition of its financial impact – only 21% of carriers are able to identify an OCF of over 3%

1. YOU CANNOT MANAGE WHAT YOU DO NOT MEASURE

The trade off in fraudulent traffic analysis

International wholesale carrier networks generate massive amounts of data as every call is routed, a trail and record of the call route is compiled, billing is generated, and accounts receivable are collected. Filtering out the noise to detect fraud, resolve disputes, limit and reduce losses, and measure the response efficacy are all the ultimate goals of fraud management.

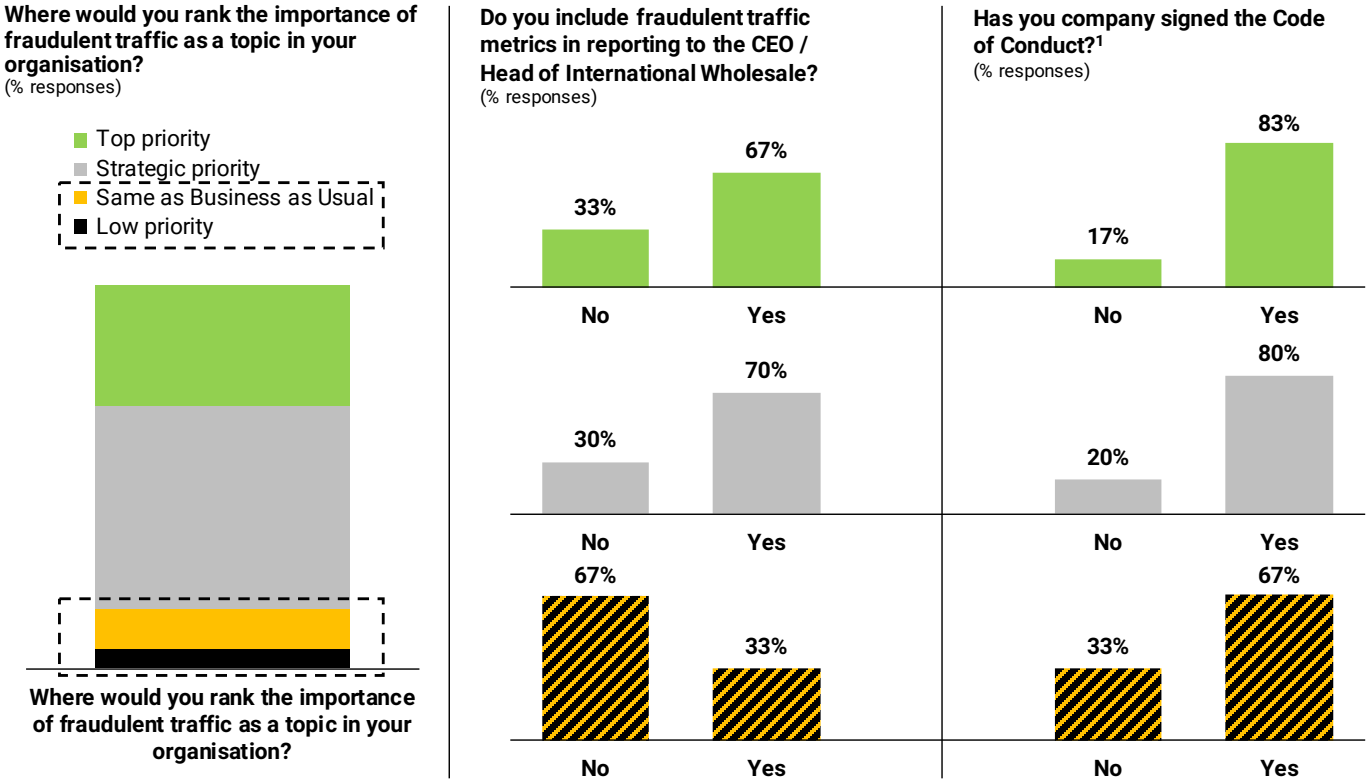
Data analysis within fraud management comes down to looking at live call detail records and graphical patterns. Statistical analysis built on those patterns is utilized to construct live alerts either to the fraud management team, or, when appropriate, the customer. The alert to the team would lead to deeper analysis, and the alert to the customer would seek approval to block the specific event. Ideally, this confirmation step would be automated or given by default.

Carriers report two prominent approaches to data analysis:

1. **Investigations launched at the "DNA-level detail"** at a per call record where the characteristics of the call are analyzed and compared to the historical patterns of that specific route, origin, or destination;
2. **Investigations launched at the aggregated level** view comparing the traffic type and volume of a specific country destination or origin over a day are compared to historical benchmarks

One respondent warned: "When you investigate at a per call level, you risk getting into too much detail. You may end up chasing your tail and risk missing a whopper that you should have seen coming a long way away." In an aggregate view, respondents focus on "catch big and medium fish" at the cost of allowing "little fish" to go undetected. The rationale being that limiting large fraud

EXHIBIT 18: CARRIERS' CORRELATION OF IMPORTANCE OF FRAUDULENT TRAFFIC AND ORGANIZATIONAL BEHAVIOUR



Notes: [1] n=19, respondents without a response were not counted; Source: GLF Fraud Survey 2018

attacks is more economical accepting smaller attacks as the cost of doing business. The time and effort required for an aggregate CDR view at a daily level for each customer investigating when results stray from the norm is much lower than the per-call-level alternative. After an issue is identified at a daily level, then further investigation can be initiated on an hour-by-hour level or lower until the analysis is concluded.

Approaches to measurement

Nearly all respondents reported tracking the amount of fraudulent traffic though some combination of the following metrics:

1. Value: attributing a monetary value of the fraud within a given timeline (i.e., how much revenue was lost due to fraudulent traffic); this can be used as a direct input into commercial decision as well as a barometer of how effective fraud management efforts have been
2. MOU: attributing the total MOU that was composed of fraudulent traffic; this can be used to measure the proportion of traffic created as a result of fraud at various levels (e.g., entire network, origin, destination, route, customer)
3. Total number of attacks: capturing the number of attacks regardless of size; the metric can be used to assess detection process decisions as well as commercial decisions should total number of attacks significant increase or decrease because of change
4. Number of alerts: capturing the total number of times that FTE or customers were required to act in the process; this can be a measure of fraudulent traffic, FTE workload, and accuracy of detection

All of metrics have their merit especially in relation to those that are already being tracked and measured within a given organization. However, the lack of some degree of standardization can lead to complications during collaboration.

While many respondents reported tracking volume, the number of respondents who report fraud management metrics to head-of-business or higher management was lower. Furthermore, very few respondents reported giving a regular report to management either as a stand-alone brief or as a part of a larger network brief. The degree of prioritization was observed to correlate with the proportion of survey respondents who included fraud metrics in regular reporting. However, even within the respondents who stated top prioritization of fraud management, 35% reported they did not include fraudulent traffic metrics in management reports. This inconsistency in reporting fraud management metrics is certainly an issue when carriers then make commercial decisions and either bring in fraud management figures or leave out fraud risk considerations entirely. Neither of these are good options especially when exacerbated by a lack of standard metrics that fraud is reported through.

As a measure of effectiveness and accuracy, false positive tracking provides potent feedback on fraud management processes. However, only 20% of respondents reported that they actively used false positives as part of their normal KPIs. This underutilized metric provides a useful measure of improvement in fraud detection processes, analytics, and FTEs performance. Given enough data to develop thresholds, false positive tracking may help guide fraud management decisions and lead to improvements in the efficiencies and effectiveness in fraud management.

The benefits of implementing these three practices (standardized and consistent metrics, consistent reporting to the head or business, and a false positive/type I error) are to build a foundation of data collection and flow that: systemically increases the effectiveness of fraud management efforts; decreases the friction and barriers to collaboration; highlights the operational repercussions of fraud risk; facilitates meaningful integration of fraud risk assessments into commercial decisions; and iteratively improve the accuracy of fraud detection.

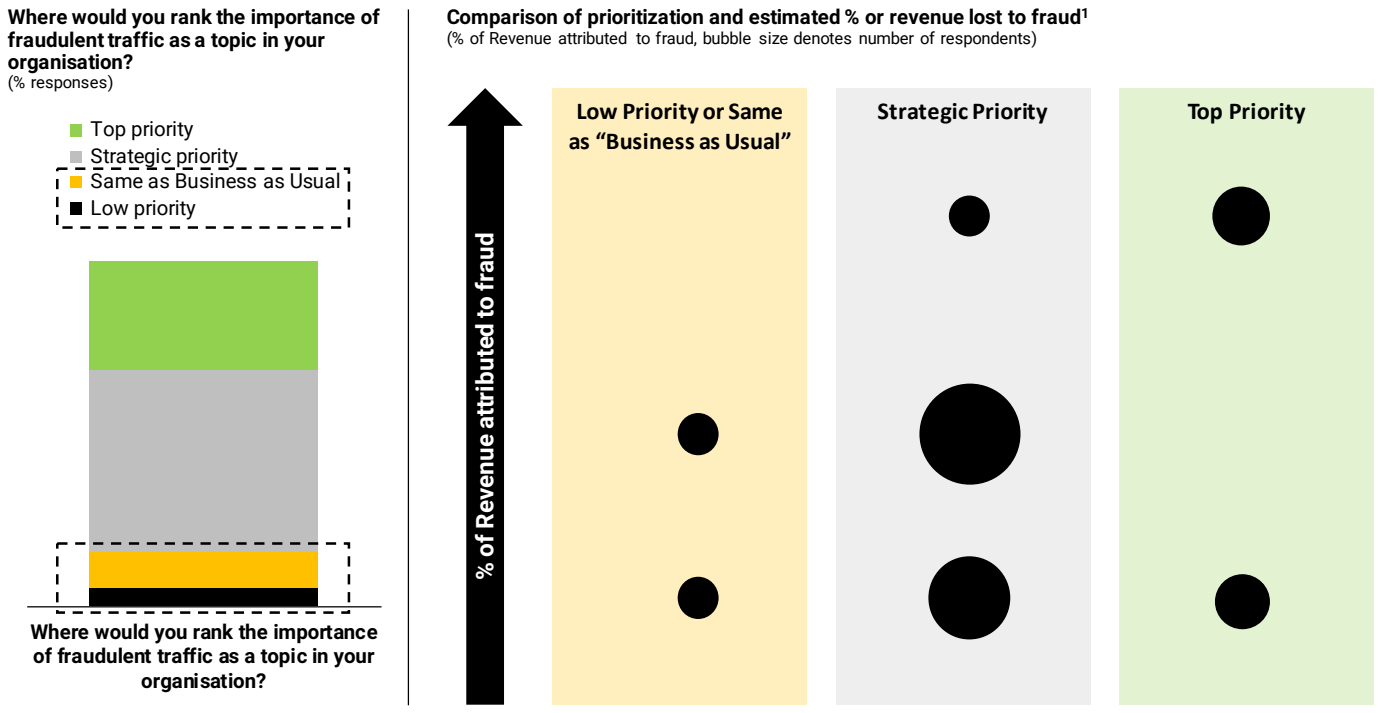
2. THE DISCONNECT BETWEEN STRATEGIC PRIORITY AND FINANCIAL IMPACT

As seen in Exhibit 19, respondents generally showed a correlation between the value placed on fraud and the prioritization of fraud management within their organization. While the data relies on small a sample, interview participants collaborated this sentiment. Multiple participants described the difficulty of placing a measurable estimate of fraud on a given commercial decision without the benefit of hindsight. The most reliable measure of value comes from disputed claims which, obviously, does little to inform a decision preemptively. Even those that cited the value within the industry at 3% suggested that this might have been collectively pulled from CFCA estimates in the place of real measured estimation.

Fraud management should be an integral part of commercial decisions, balancing the cost of routing with the costs of managing the amount of fraud that sometimes arises with low cost routing partners. One respondent gave the following illustrative example: "We have seen the cost of a route being advertised to a country, let's just say hypothetically that its cost is 8 cents/min, when we know from experience that it should cost about 10 cents/min. our routing team, driven heavily to reduce cost choses the lowest cost option. We then have something happen where we are forced to move that traffic and, all of the sudden, the MOU drops by 20% with a new routing partner who just so happens to charge 10 cents/min. you know that the low-cost, original routing partner was using extended call fraud and the like to make up for artificially low rates."

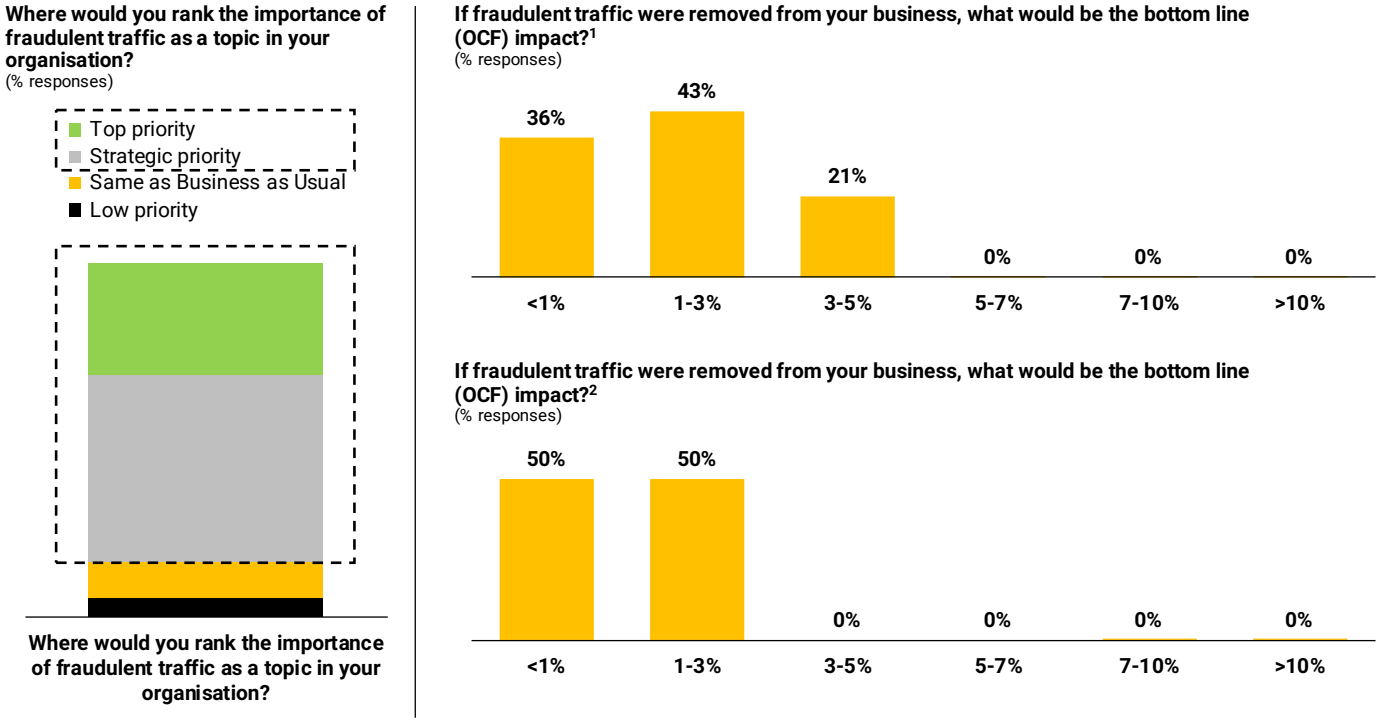
Perfect information is unobtainable, so carriers are forced to make decisions with imperfect information. Finding such a clear-cut, quantifiable amount of fraud to be able to attribute a relatively accurate value on the amount of expected fraud associated with a given commercial decision is rare. Respondents note that some carriers and geographies have been hit harder than other with a decline in traffic as a result of VOIP alternatives giving fraud teams a rough sense of what routing decisions might come with increased fraud risks. However, even well-known, good wholesalers have been recently shown to be serious offenders. "This is not a shock. Margin pressure is tight, and fraud is a way to meet revenue and margin targets". Fraud is not isolated to one carriers' network. When carriers expose themselves to fraud, either by choice or on purpose, the affects impact other carriers and carry with it a presumed guilt-by-association regardless if warranted or not. The mixture of imperfect information and intergroup

EXHIBIT 19: CARRIERS' CORRELATION PRIORITISATION OF FRAUD AND PERCEPTION OF IMPACT



Notes: [1] n=14, respondents without a response were not counted; Source: GLF Fraud Survey 2018

EXHIBIT 20: CARRIERS' PERCEPTION OF THE FINANCIAL IMPACT OF FRAUDULENT TRAFFIC

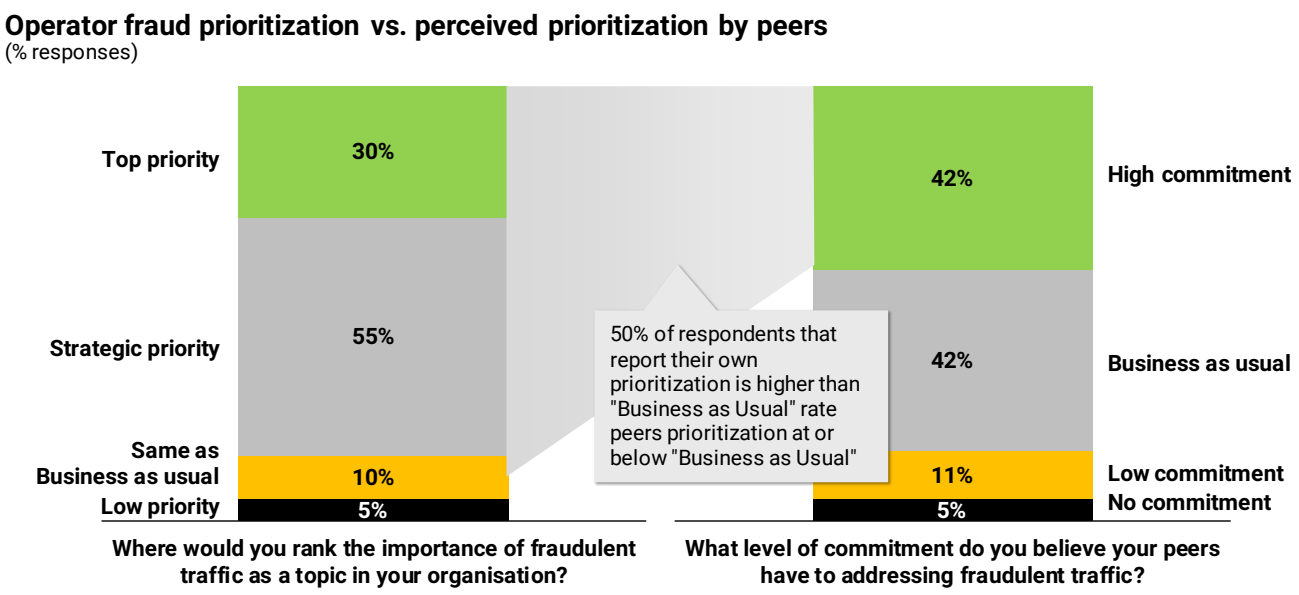


Notes: [1] n=14, respondents without a response were not counted; [2] n=8, respondents without a response or answered not measurable were not counted
Source: GLF Survey 2018, Delta Partners Analysis

bias leads to a perception that internal efforts are, on average, more prioritized and effective than efforts made by other carriers. This difference in perception was found in the GLF survey data where 50% of respondents report their own prioritization is higher than "Business as Usual" rate peers' prioritization at or below "Business as Usual".

This same perception difference was also observed in the results of the CFCA survey data where respondents' responses implied that their own efforts were over twice as effective than other carriers at reducing fraud as a percentage of revenue.

EXHIBIT 21: OPERATOR FRAUD PRIORITIZATION VS. PERCEIVED PRIORITIZATION BY PEERS



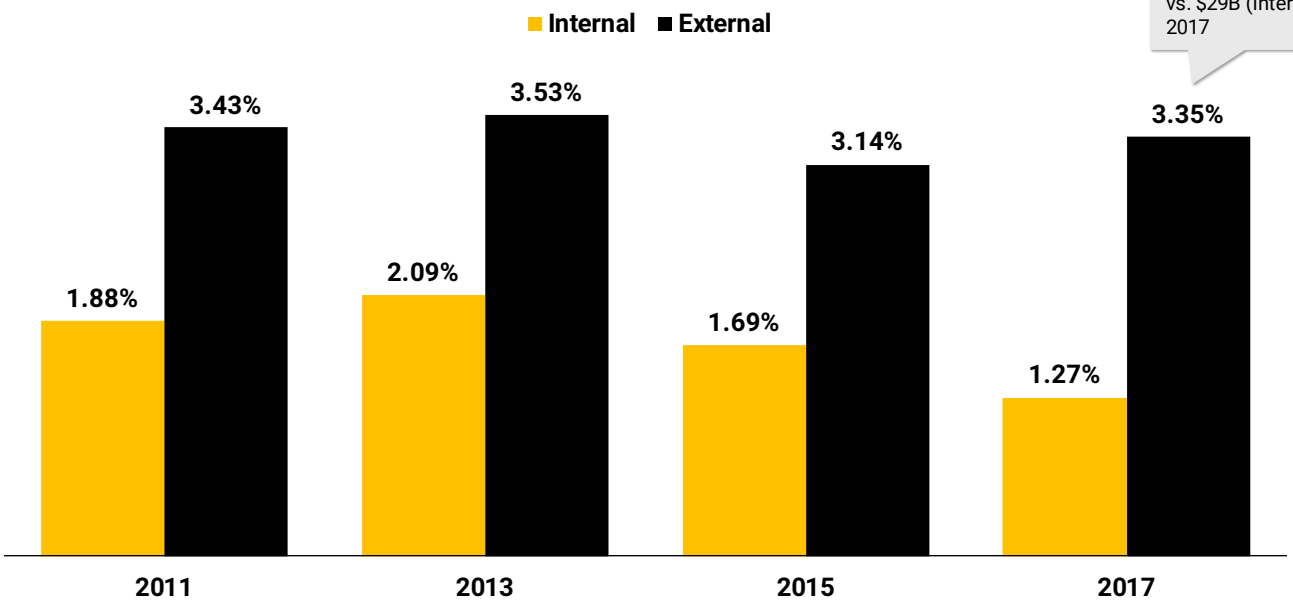
Notes: n=18, respondents without a response were not counted; Source: GLF Survey 2018, Delta Partners Analysis

EXHIBIT 22: INTERNAL VS. EXTERNAL FRAUD VALUE PERCEPTION

Respondents were asked to estimate the amount of revenue lost to fraud as a % of revenue in two different ways

Internally: what percentage of your **OWN** company's revenue is lost due to fraudulent traffic?	**Externally:** what percentage of **OTHER** companies' revenue is lost due to fraudulent traffic?

Estimated percentage of all telecom revenue lost to fraud internal vs external comparison
(weighted average %)



Percentage estimates imply $77B (external) vs. $29B (internal) in 2017

Source: CFCA 2017

PART 4

THE IMPORTANCE OF COLLABORATION

1

Several carriers are working together informally to share information and pool resources, subject to competition law requirements, to address fraudulent traffic and there is an appetite for greater collaboration

2

The GLF Code of Conduct is being adopted by many leading international carriers with 24 signing up in its first seven months, but carriers want more action beyond this commitment

1. SHARING KNOWLEDGE AND INFORMATION

Opportunity to pool resources

There are several opportunities to pool data from vendors serving the international wholesale carrier market, usually in conjunction with a service or analytic tool tied to fraud management. All pooled resources are limited by the participation of additional carriers. Ideally, an independently run data lake with full, or as close to full as possible, participation with anonymous, standardized data is shared would serve to develop a pooled blacklist/whitelist, use-case patterns and data from which to build norms and thresholds.

Pooled resources will have to overcome several barriers; not least among them are competitive barriers. Numerous respondents to the GLF survey said a major barrier to collaboration is that some players have invested significant resources developing internal databases. Because of this sunk cost, respondents reported that carriers will be hesitant to pool resources with other carriers. This hesitation has been noted already.

Fraud, like safety in the airline industry, should not be a component of competition between individual players. Earlier in the section "Extending beyond telecoms," we noted that fraudulent traffic is not "just fraud" and that international wholesale carriers have an imperative to collaborate and ensure that every effort is made to prevent and limit fraud as much as possible. Additional barriers include current NDAs and privacy laws which will take concerted effort to work around, but, as respondents note, they are not insurmountable. In the airline industry the IATA Operational Safety Audit serves to assess the operational management and control systems of an airline assess the operational management and control systems of an airline and ultimately ensures that safety advancements do not become a competitive advantage.

Sharing data

Within the GLF survey numerous respondents stated that, initially, sharing contact information of the fraud management teams at participating carriers and data on the customers that are repeatedly responsible as originators of fraud would be the most valuable. This would provide more information for commercial decisions particularly around the risk associated with a given customer. Additional shared data could be blacklists, whitelists, and unallocated lists. This data lake would need be structured with safeguards in place to comply with privacy and anti-trust regulations. Additionally, the data lake needs to be kept up to date as some data will be time sensitive. Other data sets would have great value over time; sharing the amount of baseline traffic to any given country destination can help facilitate the creation of accurate thresholds. Fraud use-cases should align with the i3 forum guidance. Creating a positive feedback loop, where greater participation among carrier's leader to additional carriers participating, is crucial. Similar to the code of conduct, participating in the data lake would be a clear external signal of taking fraud management seriously.

The benefits of a data lake are varied from holding customers and carriers accountable for fraud management negligence to highlighting attacks encountered by numerous carriers and can lead to the discovery of attacks that are currently unnoticed on numerous additional carriers. Ensuring the short-term benefits received by carriers from fraud would lead to reputational harm would create an incentive for carriers to take appropriate actions on managing fraud.

Examples of successful collaboration efforts:

- "Industry forums like the i3 Forum help to get everyone talking the same language; in disputes with people within these forums we have the same definitions with which to talk about fraud and have a specific fraud clause in our contracts. Ultimately, we are working to stop the money flow."
- "We initiated a pilot program testing a new technology, we started with one partner and are now transitioning to include 3 additional carriers. Ideally, we will progress to all collaborating on a separate, neutral entity to manage the implementation amongst industry members"

2. INTENT AND IMPACT OF THE CODE OF CONDUCT

GLF Code of Conduct – a first step towards industry leadership

Addressing fraud is challenging for international carriers as instances or contributors of fraudulent traffic cannot be irrefutably verified, with anti-trust implications from carriers making false accusations. As such, for fraud to be addressed, its symptoms, like irregular traffic patterns, should be an initial focus, which due to its cross-network impact requires collaboration between carriers.

> **"It is hard enough just trying to figure out who my counterparts are at other carriers, let alone start sharing information"**

The GLF developed a Code of Conduct for international carriers to demonstrate their commitment to reducing fraudulent traffic and work only with parties who can demonstrate their active commitment to preventing fraudulent traffic. As of October 2018, 25 carriers have signed up to the Code of Conduct, which is driven by six principles.

Respondents note that the Code of Conduct is a public statement without an accountability mechanism, but all are hopeful that this will be developed as more parties sign. As one respondent noted: "Right now, it is just paper, need to see action and share knowledge. We signed it, but I hope it goes further than that." Respondents noted that the participation rate of the code has been encouraging. "[We] hope it will be positive and current large participation rate is encouraging." Initial benefits of the Code of Conduct are already being seen however as participants noted that they perceive other carriers that are active in fraud management also participate in the Code of Conduct. The code was cited as a factor for one company to select one partner over another player who had not signed the code. "The Code of Conduct signals that other carriers are aware and are taking action to combat fraud." While initial participation is encouraging, respondents want larger behavioral changes to accompany signing the document "We haven't seen massive changes yet, but I think they will come once the sentiment starts to trickle into commercial decisions."

> **"We would like to share the latest, but everyone is very protective or share generic cases"**

Future hopes for Code of Conduct signees include that all signees have a network of direct connections to avoid any tier 2 or 3 carriers leading to the elimination of players with a vested interest in keeping known-bad players viable. Participants suggested management compensation tied to performance in fraud management as a potential future inclusion to act as an accountability mechanism. All carriers agreed that the Code can be an initiation of increased collaboration across the industry.

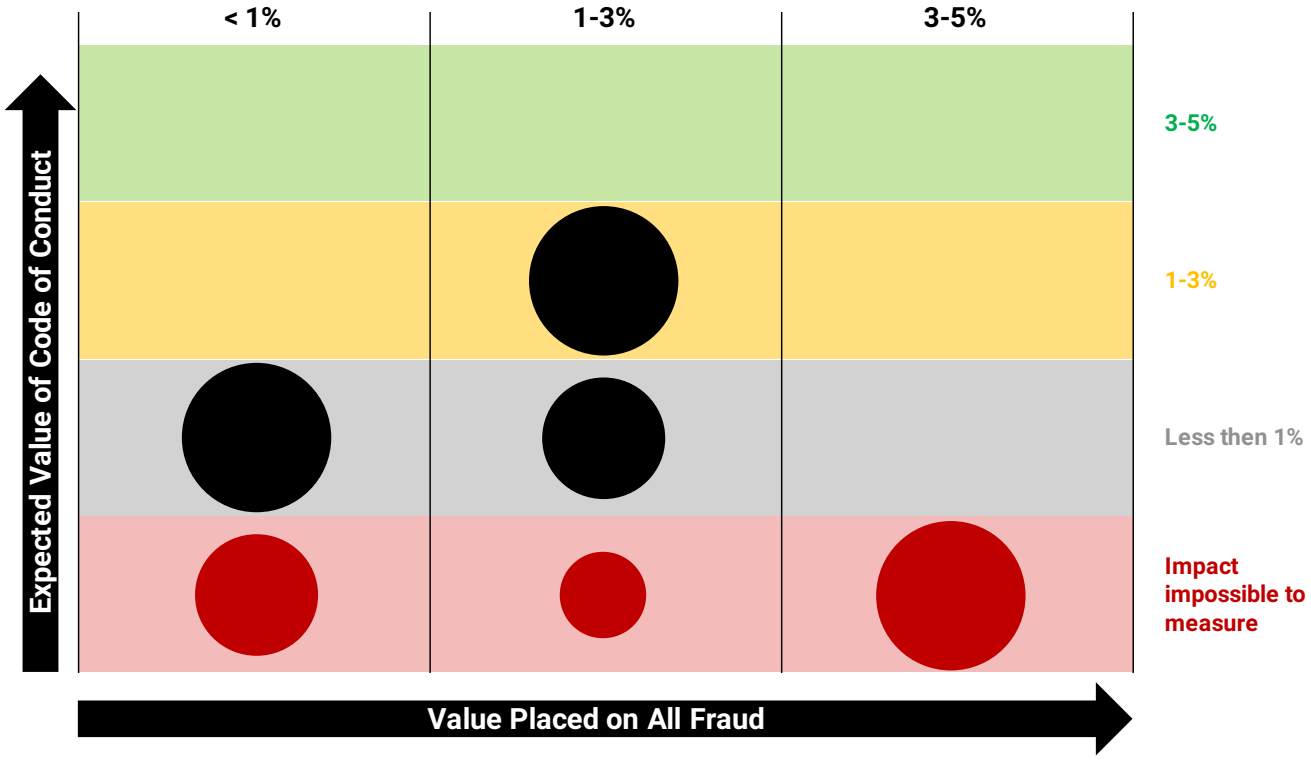
EXHIBIT 23: GLF CODE OF CONDUCT SIX PRINCIPLES

	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

EXHIBIT 24: GLF MEMBER VIEW OF IMPACT OF CODE OF CONDUCT ADHERENCE

Comparison of value placed on revenue loss to fraud vs. OCF impact of the code of conduct
(% of revenue, size of bubble indicates number of respondents)



Notes: n=17, respondents without a response were not counted; Source: GLF Survey 2018, Delta Partners analysis

PART 5

STRIVING FOR A FRAUD FREE FUTURE

1 Through commitment, compliance and collaboration the carriers will collectively act to move their organisations and the international wholesale industry towards a fraud-free future

2 All carriers are encouraged to sign-up to the Code of Conduct as well as seeking support from their customers and suppliers

3 Carriers are encouraged to self-attest adherence to the Code of Conduct and measure a common set of metrics communicated to CEO / Business Head level

4 Formalising information sharing and communication networks across the carrier community will improve the ability to collaborate in the shared aspiration of reducing fraudulent traffic

1. A THREE-TIER APPROACH: THE THREE 'Cs'

The previous section highlighted some of the barriers to collaboration as well as the benefits found in increased collaboration. In this section, we lay out a framework in overcoming those hurdles to realize the benefits of collaboration. There are three themes that will guide the industry away from the decentralized, isolated fight against fraud towards an industry united in the effort and progress of systematically reducing the volume and impact of fraudulent traffic within international wholesale networks: commitment, compliance, and collaboration. Through this framework, the industry will build from a foundation of establishing trust to taking internal action before collectively working to manage fraud.

2. SECURING COMMITMENT

Recommended action

The first step in building an industry that removes fraud prevention as a topic of competition is to establish a baseline of trust. The intent of the Code of Conduct is to signal a desire to reduce fraud work with likeminded partners and is achieved through the following actions:

1. **Signing GLF Code of Conduct** – all international carriers to sign the GLF Code of Conduct;
2. **Requesting all suppliers and customers sign Code of Conduct** – having signed, all carriers require likewise from their customers and suppliers as a pre-requisite to do business;
3. **Announcing organization aspiration for fraud reduction** – communicate to own organisation and the industry a commitment to fraud reduction through a CEO-shared aspiration

EXHIBIT 25: FRAUD PREVENTION 'THREE Cs' FRAMEWORK

	Actions	Impact
1 **Commit**	• Sign GLF Code of Conduct • Request all suppliers and customers sign Code of Conduct • Announce organisation aspiration for fraud reduction	• Establish trust between carriers and alignment of goals • GLF members seek accountability from suppliers / customers • Communicate clear message to wider industry
2 **Comply**	• Publicly attest adherence to all Code of Conduct principles • Internally track, to CEO level, industry-standard KPIs • Set internal targets for fraudulent traffic reduction • Provide data for industry 'black-box' benchmarking	• Externally signal actions being taken within the carrier • Ensure that there is common measurement of fraud impact • Encourage internal accountability to reduce fraud • Allow consistent industry-level measurement
3 **Collaborate**	• Agree to share data alerting carrier peers to fraud • Participate in fraud communications networks across carriers • Database of white-/black-listed number ranges • Formalization of industry information sharing platform	• Improve data-set on which carriers undertake fraud analysis • Allow increased carrier-to-carrier communication • Enable data-driven identification of fraudulent traffic • Enable systematic improvement in fraud response

Importance of carriers' commitment

Setting a clear commitment will align competitors on a common ground and promote the kind of forums and platforms on which ideas can be shared, best practices can be established and advancement of technology can occur. The actions serve as a public signal of intent to partners encouraging partners to also consider signing as well creating a virtuous cycle of more partners aligning on the Code of Conduct further encouraging others to join. Through these simple gains – common ground, positive feedback loop, and promoted settings for communication – further action can be taken starting with signees internally first.

3. ENSURING COMPLIANCE

Recommended action

After establishing a common ground, action is required for advance of fraud management. Carriers need to change behaviour, and they need to demonstrate those changes to convince other partners to base commercial decisions off a new value source. Carriers also need to measure their efforts and progress towards fraud management and have an honest perspective of their progress while constantly striving for further improvement. Through the following actions carriers can internally pursue a fraud-free network:

- **Publicly attest adherence to all Code of Conduct principles** – communicate to the industry not only commitment by adherence to the Code of Conduct as a signal to parties involved in fraudulent traffic;
- **Internally track, to CEO level, industry-standard KPIs** – carriers to adopt a common set of metrics (see i3 Forum proposal, below) to track internally to ensure consistent measurement across the industry;
- **Set internal targets for fraudulent traffic reduction** – set targets within organisations along with internal incentives to ensure active efforts are being taken to reduce fraudulent traffic;
- **Provide data for industry 'black-box' benchmarking** – create an industry-level anonymized database of performance of managing fraudulent traffic as a tool for carriers to benchmark their own performance and set targets.

Compliance as a signal to the industry

Measurement and active management of the performance of a carrier's fraud team provides the feedback to guide internal decisions as well as commercial decisions. Benchmarking provides a perspective on the relative performance of fraud management efforts as well as a standard to judge performance of partners after establishing commercial relationships. In measuring and reporting fraud management metrics, better decisions can be made as the effects of commercial decisions can be more accurately observed. To this end the i3 Forum has proposed the following KPIs:

1. Value of detected fraud

Definition: No estimation on future losses – actual fraud only; Period = 1 month

Measurement: Two approaches:

i) Actual fraud amount – mandatory to be anonymized: wholesale cost

ii) % of fraud traffic (volume minutes) vs of total traffic of the carrier in the period

2. Fraud disputes

Definition: Dispute = dispute/claim opened by a sending party; Successful dispute = CNs accepted; Partial successful disputes are considered as successful; Currency = EUR; In the value calculation we only consider the wholesale cost relative to the amounts credited back

Measurement: Three approaches:

i) Sum of total value (wholesale cost) of disputes – mandatory to be anonymized

ii) Sum of total value (wholesale cost) on successful disputes – mandatory to be anonymized (i.e., how much money we prevented from reaching criminals?)

iii) Ratio on successful value of disputes vs total value of disputes

3. Capability to react on fraud

Definition: Traffic confirmed as non-fraud by the sending party is not considered as fraud; Start time = switch time of 1st call of the carrier detecting the event; End time =

time of action triggered by fraud department (traffic stop / inform sending party / etc)

Measurement: average time from start time of the fraudulent traffic to end time of traffic end or removal

4. **Fraud potential losses reduction**

Definition: determine the value of fraud prevented

Measurement: the suggested measure is to look at the length of time it takes a company to detect a fraud through other processes if the fraud team were not in place

4. PRIORITISING COLLABORATION

Recommended action

Technology has unlocked the ability to discern and learn from vast quantities of data. The best way to combat fraudsters around the world is learn from each one of them and apply that knowledge collectively towards reducing the value and impact of fraud. Creating and sharing fraud data through the following actions will drive collective progress towards a fraud-free industry. Initially, to gain momentum, the focus of collaboration should be at an inter-carrier level, but in time collaboration should cover wholesale carriers, retail operators, OTT communications providers and even regulatory bodies. Each stakeholder group will have a role to play, and aligned incentive, to work together to reduce fraudulent traffic. Four initial ideas for collaboration action to reduce fraudulent traffic that could be considered are:

- Agree to share data alerting carrier peers to fraud – where permissible under competition law share data between carriers that can support in the reduction of fraudulent traffic volume and impact;
- Participate in fraud communications networks across carriers – formalize the relationships between carrier personnel addressing fraudulent traffic;
- Database of white-/black-listed number ranges – produce an industry-centralized reference database to allow carriers to have consistent view of number ranges;
- Formalization of industry information sharing platform – as has been pioneered by the GLF with regards to network security, create a platform for information sharing and communication between all carriers to work collaboratively to reduce fraudulent traffic

Accelerating industry collaboration

Internal efforts are not adequate in an industry where risk is decentralized and where networks are only as secure as the weakest connection. Elevating the lowest common denominator is in the interests of all parties involved. As a collective, carriers will all benefit from the reduction and elimination of the $17 billion of revenue that is currently lost annually. This effort is not only a benefit financially to carriers but also an ethical imperative to deny the financing of the worst of humanity.

DELTA PARTNERS

DELTA PARTNERS