CFCA 2021 Fraud Loss Survey

A message from the President of the CFCA
Stacy Graham
It is always a significant milestone in CFCA history when the hard work of reviewing, assessing, and consolidating the results of a Fraud Loss Survey are completed, and we can present and discuss the results in detail to our members.

We wish to thank all the CSP’s who have spent time to respond to this survey as well as our sponsors and partners who have assisted in contributing to the intelligence and insights we can share in this report. This year sees a continuation is this survey of being more global, with North American responses for the second time being exceeded this time by African CSP’s.

We hope this trend continues and we can provide a truly global fraud loss survey for the telecommunications industry. This also truly demonstrates how when associations work together with their members, we can achieve great things and provide value to the industry.

A message from the Survey Chairman
Jacob Howell
I have undertaken the Fraud Loss Survey for a number of years, and I am always excited to see the changes and adaptations in the industry. This year is somewhat different as we have weathered a pandemic. In this report we asked respondents for feedback on how Covid-19 has impacted fraud.

Thank you to all those who have taken the time to contribute, it is appreciated, and this collaborative approach allows the telecommunications industry to determine the losses and measure the impact fraud has upon our industry.

We have updated the questions in the report to ensure we are reflecting the current industry position as well as the wider aspects of business and consumer behaviour that impact fraud. The questions were defined in a collaborative approach with CSP’s, vendors, sponsors and individuals keen to support the CFCA initiative to share insights on fraud.

Collaborating across industry groups, collaboration amongst CSP’s, collaboration amongst consultants, vendors, and technology partners and amongst your peers has allowed the CFCA to be able to undertake this survey once again. This year it is a truly global fraud survey with respondents from all around the world contributing.

We hope you enjoy reading the comprehensive content, the figures, graphs, and tables speak for themselves, but we have included our own insights and understanding of the data from our in-depth analysis and ability to analyse some of the results at a greater level of detail.
Contents

2021 Fraud Loss Survey

CFCA 2021 Fraud Loss Survey ........................................................................................................................................... 2

Contents ............................................................................................................................................................................. 3

2021 Fraud Loss Survey .................................................................................................................................................... 3

Introduction ....................................................................................................................................................................... 6

Report Reflection ................................................................................................................................................................. 9

Survey Type & Methodology ........................................................................................................................................... 10

In which region are you located? ................................................................................................................................... 11

Responding on behalf of your company or group of companies? .................................................................................... 11

Number of employees in your company? .......................................................................................................................... 12

What is your annual revenue? ......................................................................................................................................... 12

Where is your fraud department situated? ....................................................................................................................... 13

How many levels of management exist between you and your Chief-Executive or Board? ........................................... 14

What percent of YOUR COMPANY’s revenues are monitored by your organization? ...................................................... 14

What percentage of overall revenues requires your organization’s intervention or action to mitigate against fraud? ...... 15

How long has the fraud management department / team existed? .................................................................................. 15

What functions apply to your current role and responsibilities? ..................................................................................... 16

How many are in your fraud department? ..................................................................................................................... 16

When is your fraud department staffed? ........................................................................................................................ 17

Have you created any new positions or new job functions within your organization? If so, what? ............................. 18

Law Enforcement Trends ............................................................................................................................................. 19

How many cases does your department refer to law enforcement per YEAR? ............................................................. 19

Of the cases reported to law enforcement, how many result in a law enforcement action per YEAR? ............................ 19

Of the cases reported to law enforcement, how many were related to internal fraud ............................................... 20

Why are cases not reported to law enforcement? ............................................................................................................. 21

Covid-19 Impacts ................................................................................................................................................................. 22

How has the Covid-19 pandemic affected fraud within your company? ..................................................................... 22

Covid-19 Impacts ................................................................................................................................................................. 22

USA Only – Regulatory Questions .................................................................................................................................. 23

Industry Benchmarks ......................................................................................................................................................... 24

Which anti-fraud controls are in place within your company? (Mark all that apply) ..................................................... 24

What tools do you use to detect fraud? .............................................................................................................................. 24

Do you use automation tools such as Robotic Process Automation (RPA) in your operations? ................................. 27

What percentage of your company receives anti-fraud training? ................................................................................. 28

Does your hiring policy include the following (where permitted by law)? ................................................................. 28

Does your company have an effective fraud reporting mechanism in place? (For example, a fraud hotline)? ....... 29

© Copyright 2021 CFCA  Fraud Loss Survey Report 2021
Are surprise fraud audits performed in addition to regularly scheduled audits? ................................................................. 29
Do managers actively review the controls, processes, accounts, or transactions for adherence to company policies and expectations? .................................................................................................................. 30
Does your internal audit department have adequate resources and authority to operate effectively and without undue influence from senior management? .................................................................................. 30
Are data analytics techniques used to proactively search for fraud and has the use of such techniques been made known throughout the organization? .......................................................................................... 31

FMS Benchmarks ................................................................................................................................................................. 32
Which tools do you use to detect fraud? ................................................................................................................................ 32
How frequently are Existing Fraud Management control rules and thresholds reviewed and adjusted? .............................. 32
How frequently are New Fraud Management control rules and thresholds reviewed and adjusted? .................................. 33
How many false positives does your fraud management system generate? ........................................................................... 33
How much time does your department spend researching false-positive cases? ................................................................. 34
On average, how much time does your department spend re-tuning or fine-tuning the rules and thresholds of your FMS? .... 35
Do you maintain a database or list of suspicious or fraudulent numbers? .......................................................................... 35
How willing are you to share intelligence (incident reports, fraudulent numbers, IMEs, fraud alerts, etc.) with industry forums? .................................................................................................................................. 36
Do you subscribe to any third-party data sources for your fraud management system? .......................................................... 37

Fraud Trends ........................................................................................................................................................................... 38
What percent of YOUR COMPANY’s revenues are monitored by your organization? ......................................................... 38
What percentage of fraud costs are paid by your customers? ...................................................................................................... 39
What percentage of your voice traffic is fraudulent or low value calling utilizing techniques such as spoofing, spamming or robocalling? .................................................................................................................................. 40
Over the past 12 months, have fraud alerts, trended up, trended down or stayed? .............................................................. 40
Over the past 12 months, have fraud losses trended up, trended down, or stayed the same? ........................................... 41
Top 10 Countries That ORIGINATE Fraudulent Calls: ........................................................................................................ 41
Top 10 Countries Where Fraud TERMINATES: ................................................................................................................... 42
What do you view as the top 5 fraud methods GLOBALLY? ........................................................................................................ 42
What do you view as the top 5 fraud methods at YOUR COMPANY? ...................................................................................... 43
What do you view as the top fraud types at in YOUR COMPANY? ............................................................................................. 43
What do you view as the top fraud types at in YOUR COMPANY? ............................................................................................. 44
What do you view as the top fraud types at in YOUR COMPANY? ............................................................................................. 44
What do you view as the top 5 EMERGING fraud methods at YOUR COMPANY? ................................................................. 45
What do you view as the top 5 EMERGING fraud types at YOUR COMPANY? ................................................................. 45

IOT & 5G Fraud ..................................................................................................................................................................... 46
Does your organization monitor IOT traffic for fraud and abuse? ......................................................................................... 46
How do you think fraud will impact 5G services? ................................................................................................................... 47
Which department monitors signaling security? ....................................................................................................................... 48

Fraud Loss Estimates ............................................................................................................................................................. 49
What percentage of bad debt is a result of fraud in YOUR COMPANY? ................................................................................. 49
Does your organization distinguish between bad debt and synthetic identity fraud? ............................................................... 49

If you measure synthetic identity fraud within your business, what percentage of bad debt is related to synthetic identity fraud within YOUR COMPANY? ........................................................................................................... 50

What percentage of the total GLOBAL telecom revenue base, do you think is fraud? ............................................................. 50

What percentage of YOUR COMPANY’S service revenue base do you think is fraud? ............................................................... 51

What percentage of YOUR COMPANY’S revenue base do you think is fraud? ............................................................................. 51

Of the global telecom revenue base, what percentage do you think is fraud?* ........................................................................... 52

2021 Global Fraud Loss Estimate ........................................................................................................................................... 53

2021 Survey Highlights ............................................................................................................................................................... 54

Summary - Comparison to Previous Surveys ................................................................................................................................. 55

Summary – Top Fraud Methods ....................................................................................................................................................... 55

Summary – Top Fraud Types ............................................................................................................................................................ 56

APPENDIX ....................................................................................................................................................................................... 57

Fraud Methods in YOUR COMPANY ........................................................................................................................................ 57

Emerging Fraud Methods GLOBALLY .................................................................................................................................... 58

Definitions ........................................................................................................................................................................................ 61

Fraud Method Definitions ................................................................................................................................................................. 61

Fraud Type Definitions .................................................................................................................................................................... 63

This report is dedicated to Mark Zmigrodski .................................................................................................................................. 64
Introduction

During World War II, Winston Churchill famously quipped

“You never let a good crisis go to waste.”

Fast forward to 2020 when the Covid-19 virus caused a global economic shut down. For a time, the amount of fraud impacting our industry decreased significantly. But, as workers shifted to a “new normal” of working from home and as the global economy has reopened, so has the amount of fraud and abuse affecting our industry.

In 2021, total global telecom revenues\(^1\) are estimated to be approximately $1.8 Trillion USD. The total amount of telecom revenue loss due to fraud is estimated to be 2.22% of revenues or $39.89 Billion USD.

Compared to 2019, fraud losses increased 28%, or approximately $11.6 Billion USD. To put that increase into perspective, it is the market value\(^2\) of US companies such as: TD Ameritrade Holding, Hartford Financial Services, O’Reilly Automotive and ADT.

There are many factors that are contributing to this increase in fraud. The primary reasons are due to:

- Increase in cross-industry targeted social engineering schemes (Wangiri, SMS Phishing/Pharming, Social Engineering, Robocalls)
- Increase in financial services impersonation frauds using stolen credentials from data breaches
- Use of faceless transaction portals to commit Subscription Fraud and Account Take-overs
- Increase in theft of stolen equipment and services
- Compromise of network, device or configuration weaknesses associated with voice-over-IP technologies
- Abuse of Voice & Data Service Terms & Conditions

The increase is also associated with an increase in demand and consumption of telecommunications services. The shift to working from home has fueled an insatiable demand for network connectivity and infrastructure. Similarly, the temporary shutdown of entertainment complexes and outdoor entertainment venues due to social distancing requirements has greatly increased the usage of various digital platforms, including social media, gaming, video conferencing, and OTT applications. Mobile voice traffic has also increased, with many prominent communications service providers reporting an enormous escalation in voice traffic since the outbreak of the pandemic. The increase in usage is also driving the increase in the amount of reported fraud loss.

Fraudsters are also using the Covid-19 pandemic crisis to take advantage of potential unsuspecting victims through targeted social engineering methods such as CLI/ANI Spoofing, Wangiri call back schemes, SMS Phishing/Pharming, Email Phishing/Pharming and Robocalling. They are also harvesting personal identifying information to commit subscription fraud and take over victims’ accounts.

Rahm Emanuel recently echoed Winston Churchill when he said: “You never want a serious crisis to go to waste. And what I mean by that is an opportunity to do things that you think you could not do before.” I agree with this sentiment. As an industry, I believe we can take the recent changes within the telecom industry to better secure and protect our business from fraud and abuse. We have an opportunity to re-frame what good fraud


management and security looks like for our industry. By working together, we can make a difference in protecting our customers and our businesses.

**Highlights from the 2021 CFCA Fraud Loss Survey**

**Top Fraud Methods Reported in 2021**

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>Description</th>
<th>$USD (Billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing (IP or CLI/ANI)</td>
<td>Manipulation of the IP address/CLI/ANI to hide someone's true origination or identity.</td>
<td>$2.63</td>
</tr>
<tr>
<td>Wangiri (Call Back Schemes)</td>
<td>Call back fraud schemes</td>
<td>$2.23</td>
</tr>
<tr>
<td>SMS Phishing/Pharming</td>
<td>Theft of personal info or credentials via SMS hacking, phishing, vishing, etc.</td>
<td>$2.03</td>
</tr>
<tr>
<td>Subscription Fraud (Application)</td>
<td>Creation of false details to gain access to goods and services with no intention to pay</td>
<td>$2.03</td>
</tr>
<tr>
<td>IP PBX Hacking</td>
<td>Compromised IP PBX used to make fraudulent calls</td>
<td>$1.82</td>
</tr>
<tr>
<td>Abuse of network, device, or configuration weakness</td>
<td>Exploitation of a configuration weakness to gain access to a network or device; Includes VoIP equipment such as a modem or router</td>
<td>$1.62</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>Manipulation and utilization of existing customer’s account to gain access to a device or service</td>
<td>$1.62</td>
</tr>
<tr>
<td>SIM Swapping / SIM Jacking</td>
<td>Replacing a new SIM card to gain access to the device or service</td>
<td>$1.62</td>
</tr>
<tr>
<td>Phishing / Pharming</td>
<td>Theft of personal info or credentials via email hacking, phishing, vishing, etc...</td>
<td>$1.62</td>
</tr>
<tr>
<td>Robocalling</td>
<td>Use of computerized auto-dialers to deliver pre-recorded messages to perpetrate fraud</td>
<td>$1.62</td>
</tr>
</tbody>
</table>
## Top Fraud Types Reported in 2021

<table>
<thead>
<tr>
<th>Fraud Type</th>
<th>Description</th>
<th>$USD (Billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Revenue Share Fraud (IRSF)</td>
<td>Artificial inflation of traffic terminating to international revenue share providers</td>
<td>$6.69</td>
</tr>
<tr>
<td>Traffic Pumping (includes: Domestic Revenue Share, Toll Free Traffic Pumping and International Toll Free Traffic Pumping)</td>
<td>Abuse of Communication service provider Interconnect agreements through such things as Traffic Pumping, Switch Access Stimulation, 8yy Dip Pumping and CNAM Revenue pumping schemes</td>
<td>$4.54</td>
</tr>
<tr>
<td>Arbitrage</td>
<td>Exploitation of the differences in rates between different countries</td>
<td>$3.82</td>
</tr>
<tr>
<td>Voice Interconnect Bypass (e.g. SIM box)</td>
<td>Unauthorized insertion of traffic onto another communication service provider’s network. This includes Interconnect Fraud and GSM Gateway Fraud or SIM Boxing</td>
<td>$3.11</td>
</tr>
<tr>
<td>Theft / Stolen Goods</td>
<td>Equipment theft</td>
<td>$3.11</td>
</tr>
<tr>
<td>Domestic Premium Rate Service (In Country)</td>
<td>Artificial inflation of traffic terminating to domestic premium service providers</td>
<td>$2.39</td>
</tr>
<tr>
<td>Commissions Fraud</td>
<td>Schemes used by dealers to collect additional commissions and spiffs</td>
<td>$2.15</td>
</tr>
<tr>
<td>Data Charging Bypass</td>
<td>Exploitation of network and protocol misconfigurations to bypass charging. For example, interjecting voice traffic onto Viber, Skype or WhatsApp</td>
<td>$1.91</td>
</tr>
<tr>
<td>Voice Service Reselling (e.g.: Call Selling)</td>
<td>Resale of voice services.</td>
<td>$1.91</td>
</tr>
<tr>
<td>Device / Hardware Reselling</td>
<td>Resale of equipment such as handsets, tablets, IPTV devices, routers, etc.</td>
<td>$1.67</td>
</tr>
</tbody>
</table>

**Jacob Howell**  
CFCA Board Secretary & CFCA Survey Chair  
Subex, AVP Business Consulting - Americas
Report Reflection

Fraud is not just measured by telecom operator loss...

Since the pandemic, the telecom landscape, in fact every business landscape has changed. Individuals and businesses have had to manage the impacts of remote working, prolonged sickness/staff shortages, hybrid teams, disparate teams, new digital operationist or transformation acceleration, digital self-service and much more.

Fraudsters have utilized the confusion within these changes to expedite their fraudulent activities. The new attack profile has started to shift to not target the corporate entity for their financial gain, but utilise the opportunity within these environmental impacts to target the end consumer via manipulation of the complex infrastructure of our daily lives. Criminal operations are targeting not only goods and services but the data around the consumer. This data is then utilized within extremely targeted and sophisticated social engineering to manipulate individuals in larger, more complex financial frauds and scams. From a telecoms perspective these attacks are not overtly causing revenue impacts for the service provider, the end goal of these operations are targeting the consumer and financial services and schemes to facilitate financial gain.

Fraud in 2021 now a multi-industry fraud – attacks in the telco industry impact the consumer, financial services and other industries, not simply the telecom service provider. So, we can no longer consider ourselves in an individual silo of operations, we must understand the global, multi-industry context of fraud.

As such, the losses in this report are measuring the impact of fraud to the telecom service provider in its own right, but does not measure the impact of security breaches, revenue and cost leakages, consumer losses or the impact/loss in financial services which would show significantly higher levels based on other industry reports undertaken in 2021. So, it is important to understand the losses within this report in this context.

Countries are now seeing initiatives and collaborations and multi-regulatory involvement with banks, financial services, telecom service providers as well as consumer groups in looking to communicate, share and work together to tackle the increase in frauds and scams.

Federal Trade Commission
https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic

https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports

UK Finance
Survey Type & Methodology

Panel of Experts Survey:
The survey report was a collaboration of individuals involved in fraud management in telecoms, including employees of CSP’s, risk management vendors and industry organizations.

Respondents
Surveys were taken from fraud and security experts working within the industry who are directly involved in identifying and stopping communications fraud and work for a telecommunication serviced provider.

Responses were received from:
Communications Service Providers (CSPs) located throughout the industry and around the globe
Both Small (<1K employees) and Large (100K+) CSPs
Wireless, wireline, broadband, and narrowband CSPs
Voice, data, financial services, content distribution and Internet of Things (IoT) service providers

This document was consolidated from two presentations by Jacob Howell undertaken with CFCA members on October 21st and 28th 2021.
In which region are you located?

The Communications Fraud Control Association (CFCA) tries and encourages many different telecommunications operators from different geographic regions to complete the survey, but of course we are dependent on respondents taking the time to answer the survey fully. This year’s report sees a wider distribution of responses, with Africa, North America, Asia, South America and Europe providing over 80% of the responses. This is the second survey where North America has been trumped by another region in responses. In 2021, the CFCA also distributed its survey in Spanish and Portuguese.

Responding on behalf of your company or group of companies?

Nearly 75% of the responses were on behalf of their own company with just over 20% responding as a group operation. This split of respondent types allows for a more granular response when it comes to fraud loss and the insights shared.
Number of employees in your company?

The Survey also represents different types and sizes of operations, this spread of company size ensures the report get a full view of fraud issues across the spectrum of different telecom operations. It is important to note that the report is focused on telecom service providers and consultants, risk vendors did not respond to this survey.

What is your annual revenue?

As with the employee numbers, the size of operations based on revenues is also a representative cross-section of different tiers of telecom operations.
Where is your fraud department situated?

The 2021 Fraud Loss Survey shows fraud departments are more commonly now residing under Security. Historically Finance had been the most common place for the fraud department to reside. This change is likely reflecting the steady progression of security being a requirement in fraud issues and scams as well as the protection of the operations from hacking and denial of service attempts.

Other areas mentioned in this survey include:
- Technology
- Revenue Assurance
- Wholesale
- Credit & Collections
- Product Management

In the 2019 Fraud Loss Survey, 36% of FMOs were located under Finance, 28.87% under security and 2% were under Customer Care. Operations & IT grew by 3% and 1%, respectively.
How many levels of management exist between you and your Chief-Executive or Board?

58% of Fraud departments are located within 2 levels of management to their Senior leadership. The number of departments located within 1 level doubled to 38%. This positive sign demonstrates the importance of fraud within the telecommunication service providers business and operations.

<table>
<thead>
<tr>
<th>Answer Choices</th>
<th>Cumulative Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Level</td>
<td>38%</td>
</tr>
<tr>
<td>2 Levels</td>
<td>58%</td>
</tr>
<tr>
<td>3 Levels</td>
<td>74%</td>
</tr>
<tr>
<td>4 Levels</td>
<td>90%</td>
</tr>
<tr>
<td>5+ Levels</td>
<td>100%</td>
</tr>
</tbody>
</table>

What percent of YOUR COMPANY’s revenues are monitored by your organization?

In 2019, 50% of Fraud Departments were monitoring >50% of their company’s revenues, this means that when we analyze the losses to the industry and figure produced later in the report, we must be aware of this fact. As
in their reporting to us, this may only highlight a fraction of the true fraud impact, as many fraud losses may not be included in the monitoring remit of the fraud team.

A real concern in the response to this question, is the fact that 20% responded that less than 10% of the company’s revenue was monitored by the fraud operations, creating a huge potential revenue risk. This is an area where businesses need to look seriously at their fraud and risk strategy and how they can protect revenues and reputation.

What percentage of overall revenues requires your organization’s intervention or action to mitigate against fraud?

![Bar chart showing the percentage of overall revenues required for intervention or action to mitigate against fraud.](chart)

The results here reflect those operations either are very focused on specific revenue flows (that may be combined with what they monitor closely as the previous question), or fraud operations are required to cover a higher range of revenue producing services.

How long has the fraud management department / team existed?

![Bar chart showing the duration of existence of the fraud management department / team.](chart)
New fraud departments grew by 8% since our last report with 60% of fraud departments reported they are less than 10 years old. Fraud departments are increasingly becoming an established standard function and accepted within a telecoms organization. This is a positive sign, but as demonstrated above the coverage of these fraud departments needs to be constantly reviewed to mitigate possible risk from fraud threats and areas of the business not monitored.

What functions apply to your current role and responsibilities?

New responsibilities seem a direct relationship with the increase and awareness in digital frauds and scams being perpetrated on digital mediums. The increase in consumers being impacted by fraud correlates with the increase in customer service activities.

How many are in your fraud department?

Compared to 2019 Fraud Loss Survey, fraud departments have increased in size by approximately 40%. The increase was the result of an increase in outsourcing lead by the larger communication service providers.

This is a significant increase compared to 2019 which showed only a marginal staffing increase of 2%, with outsourcing decreasing by 5%. As digital frauds and more complex fraud scenarios appear, increased resource will be required to adequately manage the changes in fraud.
The new frauds now impacting consumers and third parties such as financial services are likely seeing a direct impact in resource and workload.

If you outsource any fraud management job function(s), where do you outsource those functions?

Compared to the 2019 Fraud Loss Survey, more communication service providers have started outsourcing some of their fraud operations to other, internal resources such as NOCs or call centers. Also, 1% fewer communication service providers are outsourcing to vendors. This will need to be monitored to see if moving fraud management to an outsourced function is successful and allows adequate management and oversight of fraud controls.

When is your fraud department staffed?

Compared to 2019 holiday coverage remained the same, 24x7 coverage on weekdays was replaced with an increase in coverage during business hours, and 24x7 coverage on weekends increased by 23%.
Have you created any new positions or new job functions within your organization? If so, what?

**New Fraud Department Positions**
- Fraud Service Operations Center (SOC)
- Cyber Emergency Response Team (CERT)
- Staff Augmentation
- Fraud System Creation/Evolution
- Digital Usage Management
- New Product Development

The creation of these new positions demonstrates that organizations are realizing that the next generation of services and risks are going to be digital, complex and require skillsets previously not contained in traditional fraud departments. It is likely the early adopters in recognizing and recruiting new skillsets will benefit operations and revenues.

Do you plan to upskill your fraud department staff to adopt Machine Learning or other advanced fraud detection techniques?

Respondents showed there was a clear drive to upskill resources to meet the needs of the business and new technologies and techniques that were being introduced. It is interesting to see that organizations are recognizing the need for advanced technologies over more traditional rule based and manual processes.
Law Enforcement Trends

How many cases does your department refer to law enforcement per YEAR?

16% of communication service providers did not report any cases to law enforcement. This is a further of 5% decrease compared to 2019 which saw 7% fewer cases were reported to law enforcement in 2017. 75% of communication service providers report less than 100 cases to law enforcement each year.

Of the cases reported to law enforcement, how many result in a law enforcement action per YEAR?

Compared to the 2019 Fraud Loss Survey, 3% more fraud investigations were initiated, and 11% more cases were prosecuted. This is a positive increase to see successful prosecution.
How do victim organizations punish external (non-employee) fraud perpetrators?

Other Reasons:
- Dependent on Value - action Fraud in UK
- Report to blacklists
- Termination of partner contracts
- Prevention of recurrence listing, credit history marks
- Blocked Payments
- Individual cases basis
- Police Reports
- Law enforcement based on country proclamation

Note: Some incidents may go unreported or unpunished

Of the cases reported to law enforcement, how many were related to **internal fraud**

Compared to the 2019 Fraud Loss Survey, 35% more internal fraud investigations were initiated, and 33% more cases were prosecuted. With the pandemic enforcing remote working for many, the risks from internal fraud increased based on the lack of physical oversight of individuals and teams, with possible opportunities to perpetrate internal fraud increasing with likely changes to security, processes and procedures as remote and disparate working teams were instigated by organizations.
How do victim organizations punish internal (employee) fraud perpetrators?

8% of internal fraud incidents not reported is a noticeable threat to any organization and impacts security of the business, reputation and employee motivation. The high percentage could be due to the environment employees found themselves in during the pandemic and remote working and reduced communication and interaction with colleagues and management.

Why are cases not reported to law enforcement?

Compared to the 2019 Fraud Loss Survey, perceived lack of interest or understanding by law enforcement to take the case decreased by 38% to 13%. Lack of evidence, expertise and resources also decreased 10%. However, no faith in the judicial system to administer the right punishment to deter others increased by ~20% to 26%. This seems to reflect the need for awareness of the frauds with law enforcement to ensure that cases reported can be confidently progressed through the correct channels to a successful outcome.
Covid-19 Impacts

How has the Covid-19 pandemic affected fraud within your company?

**Negative**
- Increase in Covid-related scams
- Increase in social engineering and account take over
- Shifted from retail stores to online (increase in digital based frauds)
- Increase in malicious SMS attacks
- VOIP attacks on WFH (work from home) networks
- Increase in illegal robocalls

**Positive**
- Slightly reduction in retail fraud
- Decreased as a result of local store access
- Fraud supply chains were impacted by Covid-19, but fraud infrastructure appears to be coming back to pre-covid status

It is clear through responses to this survey and other surveys and reports undertaken along with global news coverage, that Covid-19 was a new opportunity for fraudsters to perpetrate frauds and scams. Initially it was also likely an opportune time to attempt fraud whilst businesses responded to the impact of the pandemic on their working and operational environment. National lockdowns had a direct impact in availability of frauds to be perpetrated in store/retail outlets, but gave an opportunity to focus on call centers, online commerce, etc.

Covid-19 Impacts

- **Have work-from-home requirements impacted fraud management operations?**
  - Yes: 29%
  - No: 69%
  - Not sure: 2%

- **Have you seen a change in cases of robocalling?**
  - Up: 50%
  - Down: 15%
  - Stayed the same: 35%

- **Have you seen a change in cases of PBX Hacking?**
  - Up: 27%
  - Down: 35%
  - Stayed the same: 38%

- **Have you seen a change in cases of International Revenue Share Fraud?**
  - Up: 42%
  - Down: 29%
  - Stayed the same: 29%

- **Have you seen a change in cases of Subscription Fraud?**
  - Up: 33%
  - Down: 35%
  - Stayed the same: 32%

- **Have you seen a change in cases of Payment Fraud?**
  - Up: 27%
  - Down: 15%
  - Stayed the same: 58%
USA Only – Regulatory Questions

As expected, all of the North American respondents, all of the telecom service providers in this region met the regulators deadline of implementing STIR/SHAKEN technology.
## Industry Benchmarks

Which anti-fraud controls are in place within your company? (Mark all that apply)

![Graph showing various anti-fraud controls with percentages]

- Suspension of Account
- Terminating Number Blocking
- Manual Alerts
- Originating Number Blocking
- Management Reviews
- Industry Fraud Alerts
- Text Calls
- Fraud detection and prevention training for employees
- Account Blacklisting
- Fraud detection and prevention training for managers and executives
- Code of Conduct
- Corporate Anti-fraud policy
- Fraud Management System
- Hotline Numbers
- Automated Call Blocking
- Internal Audit Department
- Customer or Employee Reporting Hotline
- Individual Customer Notifications
- Formal fraud risk assessments
- Independent audit committee
- Proactive data monitoring/analysis
- Dedicated fraud department, function, or team
- Dynamic Call Re-routing (redirecting to an Operator or IVR)
- Surprise audits
- Incentivizing/reporting incentives
- Rewards for whistleblowers
- Review of Partners
- Acceptable Use Policies (AUPs)
- End users License Agreements (EULAs)
- Other (please specify)

### What tools do you use to detect fraud?

![Graph showing various fraud detection tools with percentages]

- Manual Processes: 30%
- Rules Based FMS: 28%
- Decision Engines: 15%
- Machine Learning / Artificial Intelligence Based FMS: 13%
- External review by experts: 12%
- Other (please specify): 2%

Other: Reporting (Intraday, Daily, & Week over Week)

Interesting to note that the adoption of AI/ML, Decision Engines, and external reviews remain low. Manual processes still significant and with a shift to remote working/teams and digital environment this remains a weak point in fraud management departments. With frauds migrating to digital environments, the need to be quick,
agile and responsive means that manual processes and rule-based systems will be seriously challenged to successfully manage and mitigate such risks to the organization.

Does your fraud management system analyze data in real-time or near real-time using CDR based analysis?

5% of respondents said they did not analyze data in real-time and 7% did not know, even though a small percentage, the need to analyze data quickly as possible is now becoming more and more important and prevalent with the frauds being perpetrated to be able to successfully identify them in real-time.

Does your fraud management system monitor signal records for real-time threat detection? (SIP, Diameter, or SS7)?

Communication service providers can increase their fraud coverage and reduce their time to detection by monitoring their signaling records. Monitoring CDR’s alone is not enough to identify the frauds now being the
most prevalent. As IP based networks become a majority the importance of analyzing these records will be become more important.

**Does your department use automation tools within any of the following areas? (e.g.: to create tickets, to contact customers, to review suspicious orders…)**

It is clear that the legacy techniques of rule-based analysis, reporting and manual processes are still the foundations of a fraud management departments’ tools to identify fraud. Decision engines, MLS, AI is starting to show more prominence and we will have to investigate in the future if this is vendor initiated or driven by the end users.
Adoption of AI/ML & Decision Engines although widely promoted and discussed by risk management vendors, the take up and adoption is relatively low within the CSP’s.

Do you use automation tools such as Robotic Process Automation (RPA) in your operations?

15% of communication service providers are planning to implement RPA into their business Operations. 45% are not using RPA. Approximately 20% are considering it.

The positive response to RPA means that organizations are seeing the need for automation in operations but somewhat contradicts other areas of improvement around improving systems with automation and machine learning.
What percentage of your company receives anti-fraud training?

Every company reported they provide anti-fraud training. Nearly 30% reported all their employees are trained.

There were several other communication service providers that reported few of their employees have been trained.

<table>
<thead>
<tr>
<th>Answer Choices</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 10%</td>
<td>22.86%</td>
</tr>
<tr>
<td>10-20%</td>
<td>8.57%</td>
</tr>
<tr>
<td>20-30%</td>
<td>14.29%</td>
</tr>
<tr>
<td>30-40%</td>
<td>5.71%</td>
</tr>
<tr>
<td>40-50%</td>
<td>2.86%</td>
</tr>
<tr>
<td>50-60%</td>
<td>5.71%</td>
</tr>
<tr>
<td>60-70%</td>
<td>0.00%</td>
</tr>
<tr>
<td>70-80%</td>
<td>2.86%</td>
</tr>
<tr>
<td>80-90%</td>
<td>2.86%</td>
</tr>
<tr>
<td>90-99%</td>
<td>5.71%</td>
</tr>
<tr>
<td>100% (All)</td>
<td>28.57%</td>
</tr>
</tbody>
</table>

Untrained employees working within a fraud team is a significant risk to operations, with changes in fraud methods, environments, and the fraud landscape, it is critical to ensure that all employees dealing with fraud and risk management are trained and confident in the understanding of fraud modus operandi and impacts to the consumer and the business to adequately manage fraud.

Does your hiring policy include the following (where permitted by law)?

Other including vetting for high-risk roles.

It is satisfying to see that due diligence and checks were undertaken on employees when hired to remove the risk of security and internal fraud.
Does your company have an effective fraud reporting mechanism in place? (For example, a fraud hotline)?

The survey highlighted that some communication service providers are missing a fraud reporting mechanism for their employees and customers. Whistleblowing is likely to have fallen considerably during Covid-19 and remote working environments and it will be interesting to see how the ‘new norm’ in regards working will impact internal fraud monitoring and whistleblowing.

Are surprise fraud audits performed in addition to regularly scheduled audits?

68% said no or not sure. Surprise audits can be an effective way for a business to deter internal theft and improve security and ensure employees are aware that the business is taking fraud and security seriously.
Do managers actively review the controls, processes, accounts, or transactions for adherence to company policies and expectations?

Although a majority (80%) said that managers actively review controls, processes, accounts, and transactions, 20% who responded that did not know or did not undertake reviews should look at this area. Adherence to company policies and expectations will mitigate both oversights, weaknesses, voids, and areas that could be improved.

Does your internal audit department have adequate resources and authority to operate effectively and without undue influence from senior management?

It is clear that the response to this question means that many respondents are not confident that internal audit teams have the necessary resource or authority to operate effectively. This is a concern and should be further investigated and expanded in future surveys.
Are data analytics techniques used to proactively search for fraud and has the use of such techniques been made known throughout the organization?

Fraud detection systems can be an effective way of deterring fraud and abuse within the communication service provider, it is positive to see that 65% of respondents stated that data analytic techniques are being used and made aware throughout the business.
FMS Benchmarks

Which tools do you use to detect fraud?

Adoption of AI/ML, Decision Engines and external resources continues to remain low, even though risk management vendors are promoting new technologies and techniques to improve fraud management effectiveness.

How frequently are Existing Fraud Management control rules and thresholds reviewed and adjusted?

More than 20% of communication service providers update their fraud detection rules on a Daily or Weekly basis.

Compared to 2019, 18% fewer people reported they update their rules on an ad hoc/as needed basis.

The continual updating of rules on a daily basis seems to align to the need for more automated tools and techniques such as machine learning etc. to reduce the need for manual updating and adoption of rules and thresholds.
The need to update rules and thresholds on a daily basis could reflect the changing behavior of fraud being perpetrated or inadequate understanding of fraud and/or the systems used.

**How frequently are New Fraud Management control rules and thresholds reviewed and adjusted?**

Well over half of the respondents are adding new rules on a monthly/ad-hoc basis reflecting the changing dynamics for fraud being perpetrated.

**How many false positives does your fraud management system generate?**

Communication service providers’ fraud management systems tend to detect fraud cases with an average False Positives rate of either 13% or 88%.
The previous results from updating or adding new rules along with the diverse false positive figures could reflect the need for training on systems and in the fraud domain. Some telecoms service providers are clearly managing the fraud management systems in place and maintaining low false-positive results, whilst on the other end of the spectrum, some fraud management systems are close to not functioning or actually not functioning. This may be due to user error, vendor responsibility, data being digested by the systems, resource availability.

Note: False Positive Rate = Number of non-fraud incidents / Total number of fraud incidents investigated

How much time does your department spend researching false-positive cases?

It is obvious from the previous survey responses, that the topic of systems and their capability needs further detailed review to fully understand the diverse responses.

Compared to 2019 time spent researching false-positive cases decreased approximately 26%.

However, a few departments reported spending 50%+ of their time researching false positive cases.
On average, how much time does your department spend re-tuning or fine-tuning the rules and thresholds of your FMS?

The above figures demonstrate that a majority of respondents were spending some time in re/fine tuning the rules within the incumbent fraud management systems.

Do you maintain a database or list of suspicious or fraudulent numbers?

Nearly all respondents state that they maintain a list or database of fraudulent numbers.

Some communication service providers spend more than 10+ hours per week adjusting the fraud rules and thresholds.
How willing are you to share intelligence (incident reports, fraudulent numbers, IMEIs, fraud alerts, etc.) with industry forums?

More than two-thirds of all respondents said they were willing to share information on fraud incidents within industry forums. With another third willing to share such data. This collaborative aspiration is a positive sign that with the correct legal and data protection policies and processes in place that sharing information on fraud with their peers could assist in managing fraud nationally/in country.
Do you subscribe to any third-party data sources for your fraud management system?

Adoption of some third-party data sources remains low.

Other data sources include:

- CFCA Fraud Forum
- Crowdsourcing
- Consultancy Information

It is a positive sign to see that communication service providers are willing to use third party sources of intelligence to provide further insight into risk management and fraud controls. As frauds become more complex and evolve, using tools and data sources available to detect fraud is paramount.
Fraud Trends

What percent of YOUR COMPANY’s revenues are monitored by your organization?

21% of communication service providers reported that they monitored less than 10% of their company’s revenues. 12% reported they monitored all company revenues. These two figures are surprisingly low. With only a total of 54% covering more than 50% of their companies’ revenues.

Note: “Company” refers to the range of activities of your fraud management function.

What percentage total fraud losses are investigated using fraud management application or prevention tools?

57% of communication service providers reported using their FMS or equivalent applications to investigating more than 75% of the known fraud losses.
What percentage of overall revenues requires your organization’s intervention or action to mitigate against fraud?

25% of fraud organizations intervene or take action to mitigate against fraud involving less than 1% of their revenues. 43% intervene and take action on more than 10% of their company’s revenues.

What percentage of fraud costs are paid by your customers?

35% of communication service providers have customers pay less than 10% of fraud costs. 3% have they pay more than 50%. This may require more in-depth analysis, as this may include business type fraud issues like PABX fraud, where the loss maybe due to lax security undertaken by the customer.
What percentage of your voice traffic is fraudulent or low value calling utilizing techniques such as spoofing, spamming or robocalling?

33% of communication service providers report that 0-2% of their traffic volumes are fraudulent or low value such as spoofing, spamming or robocalls. 15% of communication service providers reported it was more than 10% of their traffic.

Over the past 12 months, have fraud alerts, trended up, trended down or stayed?

42% of communication service providers reported fraud alerts had increased globally. This reflects media coverage of increased fraud attacks on consumers with numerous scams being perpetrated, taking advantage of Covid-19 restrictions and concerns. 51% respondents reported fraud alerts had increased within their business.
Over the past 12 months, have fraud losses trended up, trended down, or stayed the same?

29% of communication service providers reported fraud losses had increased globally. However, 23% reported fraud losses had increased within their business. This would align to although an increase in fraud attacks, the rise in fraud perpetrated against consumers was not a direct financial loss to the communication service provider but directly impacted the consumer and financial services.

Top 10 Countries That ORIGINATE Fraudulent Calls:
Top 10 Countries Where Fraud TERMINATES:

What do you view as the top 5 fraud methods GLOBALLY?

The top 5 methods are ~26% of all fraud losses.

In 2019 the top 5 fraud methods were:

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>% Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Fraud</td>
<td>7.6%</td>
</tr>
<tr>
<td>Wangiri (Call Back Schemes)</td>
<td>6.2%</td>
</tr>
<tr>
<td>Subscription Fraud (Application)</td>
<td>5.7%</td>
</tr>
<tr>
<td>Abuse of network, device or configuration weakness</td>
<td>5.2%</td>
</tr>
<tr>
<td>IP PBX Hacking</td>
<td>4.8%</td>
</tr>
</tbody>
</table>
What do you view as the top 5 fraud methods at YOUR COMPANY?

The top 5 methods are ~27% of all fraud losses.

In 2019 the top 5 fraud methods were:

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>% Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription Fraud (Application)</td>
<td>6.8%</td>
</tr>
<tr>
<td>Payment Fraud</td>
<td>6.4%</td>
</tr>
<tr>
<td>PBX Hacking</td>
<td>6.4%</td>
</tr>
<tr>
<td>IP PBX Hacking</td>
<td>6.4%</td>
</tr>
<tr>
<td>Wangiri (Call Back Schemes)</td>
<td>6.4%</td>
</tr>
</tbody>
</table>

What do you view as the top fraud types at in YOUR COMPANY?

The top 5 types are 53+% of all fraud losses.

In 2019 the top 5 fraud methods were:

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>% Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Revenue Share Fraud (IRSF)</td>
<td>17.5%</td>
</tr>
<tr>
<td>Arbitrage</td>
<td>11.0%</td>
</tr>
<tr>
<td>Interconnect Bypass (e.g. SIM box)</td>
<td>11.0%</td>
</tr>
<tr>
<td>Domestic Premium Rate Service (In Country)</td>
<td>9.1%</td>
</tr>
<tr>
<td>Traffic Pumping (includes: Domestic Revenue Share, Toll Free Traffic Pumping)</td>
<td>8.4%</td>
</tr>
</tbody>
</table>
What do you view as the top fraud types at in YOUR COMPANY?

The top 5 types are 61% of all fraud losses.
In 2019 the top 5 fraud methods were:

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>% Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Revenue Share Fraud (IRSF)</td>
<td>18.1%</td>
</tr>
<tr>
<td>Arbitrage</td>
<td>12.0%</td>
</tr>
<tr>
<td>Theft / Stolen Goods</td>
<td>8.4%</td>
</tr>
<tr>
<td>Interconnect Bypass (e.g. SIM box)</td>
<td>7.2%</td>
</tr>
<tr>
<td>Domestic Premium Rate Service (In Country)</td>
<td>6.0%</td>
</tr>
</tbody>
</table>

What do you view as the top fraud types at in YOUR COMPANY?

The top 5 types are 53+% of all fraud losses.
In 2019 the top 5 fraud methods were:

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>% Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Revenue Share Fraud (IRSF)</td>
<td>17.8%</td>
</tr>
<tr>
<td>Interconnect Bypass (e.g. SIM box)</td>
<td>11.6%</td>
</tr>
<tr>
<td>Arbitrage</td>
<td>9.6%</td>
</tr>
<tr>
<td>Traffic Pumping (includes: Domestic Revenue Share, Toll Free Traffic Pumping)</td>
<td>8.0%</td>
</tr>
<tr>
<td>Mobile Money</td>
<td>7.1%</td>
</tr>
</tbody>
</table>
What do you view as the top 5 EMERGING fraud methods at YOUR COMPANY?

The top 5 methods are ~30% of all fraud losses.
In 2019 the top 5 fraud methods were:

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>% Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Fraud</td>
<td>7.4%</td>
</tr>
<tr>
<td>IP PBX Hacking</td>
<td>6.4%</td>
</tr>
<tr>
<td>Abuse of network, device or configuration weakness</td>
<td>5.9%</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>4.8%</td>
</tr>
<tr>
<td>IOT</td>
<td>4.8%</td>
</tr>
</tbody>
</table>

What do you view as the top 5 EMERGING fraud types at YOUR COMPANY?

The top 5 types are ~47% of all fraud losses.
In 2019 the top 5 fraud methods were:

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>% Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Fraud</td>
<td>7.4%</td>
</tr>
<tr>
<td>IP PBX Hacking</td>
<td>6.4%</td>
</tr>
<tr>
<td>Abuse of network, device or configuration weakness</td>
<td>5.9%</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>4.8%</td>
</tr>
<tr>
<td>IOT</td>
<td>4.8%</td>
</tr>
</tbody>
</table>
IOT & 5G Fraud

Does your organization monitor IOT traffic for fraud and abuse?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>41%</td>
<td>38%</td>
<td>21%</td>
</tr>
</tbody>
</table>

With only 41% of respondents stating they have fraud management activities around IoT services and technology in place, there seems a large risk with the increase in IoT services that IoT could face significant fraud abuse and currently not adequately protected within the telecoms industry.

What is your organization’s role in ensuring the security of IoT Devices?

- Protecting connectivity of the IoT device for the customer: 46%
- Protecting information generated by the IoT devices: 26%
- Protecting connectivity of IoT data for the carrier: 24%
- IoT customers should protect their own assets (connectivity, devices delivered by them, identities they store, etc.): 26%
- Don’t know: 40%
- Other (please specify): 4%
In what ways are IOT devices being used to commit fraud?

- Distributed Denial of Service (DDOS) Attacks: 32.5%
- Botnets: 23.7%
- Ransomware: 13.2%
- Abuse of unlimited data services: 37.7%
- Disruption of Public Services: 7.9%
- Disruption of Business Operations: 10.5%
- Sim Swaps: 35.1%
- Exploitation of Traffic Policies: 23.7%
- Other (please specify): 21.9%

How do you think fraud will impact 5G services?

- 5G will experience same fraud scenarios we’ve seen before on other previous technologies: 23%
- 5G is much more safe against fraud because of how it has been designed: 0%
- We expect to see an increase of 5G fraud because of protocols and the number of devices connected: 32%
- Don’t know: 55%
- Other (please specify): 0%
Which department monitors signaling security?

Currently the fraud management department is not leading in the major area of responsibility for signaling security with dedicated IT security departments and Network Operations Centre (NOC) being the most common departments responsible for this function. As telecom networks steadily become IP based, we would expect to see fraud management departments and legacy departments to collaborate further.
Fraud Loss Estimates

What percentage of bad debt is a result of fraud in YOUR COMPANY?

With over 40% of respondents stating that less than 10% of fraud losses being attributed to bad debt, this could reflect the respondents being a mixture of pre and post-paid businesses. The outcome of the survey question is also not taking into account the definition of bad debt from each communication service provider which could all possibly be different, i.e., not paying first bill is bad debt, not paying three months bills, etc.

Does your organization distinguish between bad debt and synthetic identity fraud?

50% reported they are able to distinguish bad debt and synthetic ID fraud. ~37% were not sure. Synthetic fraud is a complex form of identity theft in which the thing being imitated is a person. A fraudster combines for instance a stolen Social/National Security Number and fake information, such as a false name, incorrect address, made-up date of birth or new phone number to create a false identity.
If you measure synthetic identity fraud within your business, what percentage of bad debt is related to synthetic identity fraud within YOUR COMPANY?

~57% of communication service providers are not sure if bad debt is related to synthetic identity fraud, this reflects that currently these frauds are not being reported and reviewed in-depth to allow for further insight to be known.

What percentage of the total GLOBAL telecom revenue base, do you think is fraud?

33% reported global fraud losses are less than 2%
45% reported global fraud losses are between 4-10%
9% reported global fraud losses are greater than 10%
What percentage of YOUR COMPANY’S service revenue base do you think is fraud?

- 51% reported their company’s fraud losses are less than 1%
- 75% reported their company’s fraud losses are less than 2%
- 8% reported their company’s fraud losses are greater than 10%

Both large and small communication service providers reported fraud losses less than 1% and between 1-2%.
Of the global telecom revenue base, what percentage do you think is fraud?*

<table>
<thead>
<tr>
<th>Fraud Loss as a % of Revenue</th>
<th>&lt;1,000,000</th>
<th>1,000,001 to 10,000,000</th>
<th>10,000,001 to 50,000,000</th>
<th>25,000,001 to 50,000,000</th>
<th>50,000,001+</th>
<th>Wholesale</th>
<th>% Total Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 1%</td>
<td>11.1%</td>
<td>15.1%</td>
<td>2.0%</td>
<td>2.0%</td>
<td>15.1%</td>
<td>6.0%</td>
<td>51.4%</td>
</tr>
<tr>
<td>1-2%</td>
<td>5.2%</td>
<td>7.2%</td>
<td>1.0%</td>
<td>1.0%</td>
<td>7.2%</td>
<td>2.9%</td>
<td>24.3%</td>
</tr>
<tr>
<td>2-3%</td>
<td>0.6%</td>
<td>0.8%</td>
<td>0.1%</td>
<td>0.1%</td>
<td>0.8%</td>
<td>0.3%</td>
<td>2.7%</td>
</tr>
<tr>
<td>3-4%</td>
<td>1.2%</td>
<td>1.6%</td>
<td>0.2%</td>
<td>0.2%</td>
<td>1.6%</td>
<td>0.6%</td>
<td>5.4%</td>
</tr>
<tr>
<td>4-5%</td>
<td>0.6%</td>
<td>0.8%</td>
<td>0.1%</td>
<td>0.1%</td>
<td>0.8%</td>
<td>0.3%</td>
<td>2.7%</td>
</tr>
<tr>
<td>5%-10%</td>
<td>1.2%</td>
<td>1.6%</td>
<td>0.2%</td>
<td>0.2%</td>
<td>1.6%</td>
<td>0.6%</td>
<td>5.4%</td>
</tr>
<tr>
<td>&gt; 10%</td>
<td>1.7%</td>
<td>2.4%</td>
<td>0.3%</td>
<td>0.3%</td>
<td>2.4%</td>
<td>1.0%</td>
<td>8.1%</td>
</tr>
</tbody>
</table>

*Note: Percentages taken from CSP self-reported revenue losses.
2021 Global Fraud Loss Estimate

2021 Estimated Global Telecom Revenues*:
$1.800 Trillion (USD)

2021 Estimated Global Telecom Fraud Loss:
$39.893 Billion (USD), or 2.22%

Loss Calculation:
\[ \sum \left( \frac{(CSP \ Size \times \% \ by \ Group) \times \text{Group Midpoint}}{100} \right) \times \text{Global Telecom Revenues} \]

Note: Fraud losses were weighted based on CSP size to avoid bias created when small and large CSP responses were combined.

2021 Survey Highlights

2021 Estimated Global Telecom Revenues*: $1.80 Trillion (USD)
   - Global Telecom Revenues grew by ~11% since 2019

2021 Global Fraud Loss Estimate: 2.22% or $39.89 Billion (USD)
   - The 28% increase is attributed to many factors including:
     - Increase in cross-industry targeted social engineering schemes (Wangiri, SMS Phishing/Pharming, Social Engineering, Robocalls)
     - Increase in financial services impersonation frauds using stolen credentials from data breaches
     - Use of faceless transaction portals to commit Subscription Fraud and Account Take-overs
     - Increase in theft of stolen equipment and services
     - Compromise of network, device or configuration weaknesses associated with voice-over-IP technologies
     - Abuse of Voice & Data Service Terms & Conditions
   - 81% said global fraud alerts had increased or stayed the same—a 1% increase from 2019.
   - 64% said global fraud losses had increased or stayed the same—a 4% increase from 2019.

Summary - Comparison to Previous Surveys

<table>
<thead>
<tr>
<th>Year</th>
<th>Estimated Global Revenues (USD)</th>
<th>Estimated Global Fraud Loss (USD)</th>
<th>% Loss*</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>$1.7 Trillion</td>
<td>$60.1 Billion</td>
<td>3.54%</td>
</tr>
<tr>
<td>2011*</td>
<td>$2.1 Trillion</td>
<td>$40.1 Billion</td>
<td>1.88%</td>
</tr>
<tr>
<td>2013</td>
<td>$2.2 Trillion</td>
<td>$46.3 Billion</td>
<td>2.09%</td>
</tr>
<tr>
<td>2015</td>
<td>$2.25 Trillion</td>
<td>$38.1 Billion</td>
<td>1.69%</td>
</tr>
<tr>
<td>2017</td>
<td>$2.30 Trillion</td>
<td>$29.2 Billion</td>
<td>1.27%</td>
</tr>
<tr>
<td>2019</td>
<td>$1.63 Trillion</td>
<td>$28.3 Billion</td>
<td>1.74%</td>
</tr>
<tr>
<td>2021</td>
<td>$1.80 Trillion</td>
<td>$39.9 Billion</td>
<td>2.22%</td>
</tr>
</tbody>
</table>

% Var: 10.8%

*Note: Starting in 2011 losses were recalculated using a weighting methodology.

Summary – Top Fraud Methods

The majority of the top ten Fraud Methods are fraud attack methods victimizing the communication service providers’ subscribers, with Spoofing, Wangiri, SMS Phishing (Smishing), Account Takeover, Sim Swapping, Phishing and Robocalling used against subscribers and a direct financial impact to consumers and financial service providers.

Targeted social engineering – to undertake impersonation through collection of data from various sources through various frauds methods and scams to receive One-time passwords (OTP) for access to financial services.

Top 10 Fraud Methods from 2019:
- $1.92 B – Subscription Fraud (Application)
- $1.82 B – Payment Fraud
- $1.82 B – PBX Hacking
- $1.82 B – IP PBX Hacking
- $1.82 B – Wangiri (Call Back Schemes)
- $1.63 B – Abuse of network, device or configuration weaknesses
- $1.44 B – Dealer Fraud
- $1.34 B – Subscriber Fraud (Identity)
- $1.25 B – Account Take Over
- $1.15 B – Internal Fraud / Employee Theft
Summary – Top Fraud Types

For the year 2021, the top fraud types and the corresponding losses are as follows:

<table>
<thead>
<tr>
<th>Fraud Type</th>
<th>Loss (Billion USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Revenue</td>
<td>$6.69</td>
</tr>
<tr>
<td>Traffic Pumping (includes: Arbitrage)</td>
<td>$4.54</td>
</tr>
<tr>
<td>Voice Interconnect Bypass</td>
<td>$3.11</td>
</tr>
<tr>
<td>Theft / Stolen Goods</td>
<td>$3.11</td>
</tr>
<tr>
<td>Domestic Premium Rate</td>
<td>$2.39</td>
</tr>
<tr>
<td>Commissions Fraud</td>
<td>$2.15</td>
</tr>
<tr>
<td>Data Charging Bypass</td>
<td>$1.91</td>
</tr>
<tr>
<td>Voice Service Reselling</td>
<td>$1.91</td>
</tr>
<tr>
<td>Device / Hardware Reselling</td>
<td>$1.67</td>
</tr>
</tbody>
</table>

Comparing to 2019, the top fraud types and their losses are:

- $5.04 B – International Revenue Share Fraud
- $3.28 B – Arbitrage
- $2.71 B – Interconnect Bypass (e.g. SIM Box)
- $2.27 B – Domestic Premium Rate Service (In Country)
- $2.00 B – Traffic Pumping (includes: Domestic Revenue Share, Toll Free Traffic Pumping)
- $1.76 B – Commissions Fraud
- $1.76 B – Device / Hardware Reselling
- $1.49 B – Theft / Stolen Goods
- $1.17 B – Friendly Fraud
- $0.98B – Wholesale SIP Trunking Fraud
APPENDIX

Fraud Methods in YOUR COMPANY

Fraud Methods in YOUR COMPANY ($Billion USD)
Emerging Fraud Methods GLOBALLY

Emerging Fraud Methods GLOBALLY ($Billion USD)
Fraud Types (EMERGING; Home & Roaming)

Fraud Types (YOUR COMPANY; Onnet & Roaming) ($Billion USD)
## Definitions

### Fraud Method Definitions

<table>
<thead>
<tr>
<th>Fraud Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abuse of network, device, or configuration weakness</td>
<td>Exploitation of a configuration weakness to gain access to a network or device; Includes VoIP equipment such as a modem or router</td>
</tr>
<tr>
<td>Covid Related – Abuse of network vulnerabilities</td>
<td>Exploitation of weaknesses in conferencing platforms and VPN such as sending malicious files related to Zoom, Skype, or Teams</td>
</tr>
<tr>
<td>Abuse of Voice Service Terms and Conditions</td>
<td>Violation of the communication service provider's voice service terms and conditions or acceptable use policy. For example, abuse of unlimited voice usage plans</td>
</tr>
<tr>
<td>Abuse of Data Service Terms and Conditions</td>
<td>Violation of the communication service provider's data service terms and conditions or acceptable use policy. For example, abuse of unlimited data usage plans</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>Manipulation and utilization of existing customer’s account in order to gain access to a device or service</td>
</tr>
<tr>
<td>SIM Swapping / SIM Jacking</td>
<td>Replacing a new SIM card in order to gain access to the device or service</td>
</tr>
<tr>
<td>Brand Name / Logo Abuse</td>
<td>Acquisition and use of a company’s logo without permission</td>
</tr>
<tr>
<td>Clip-on Fraud</td>
<td>Stealing service by attaching wires to another customer's phone equipment</td>
</tr>
<tr>
<td>Dealer Fraud</td>
<td>All types of fraud conducted by indirect and 3rd party dealers</td>
</tr>
<tr>
<td>IMEI Reprogramming</td>
<td>Changing the IMEI of a handset to hide the true origination or identity of a caller</td>
</tr>
<tr>
<td>Internal Fraud / Employee Theft</td>
<td>Theft of service or equipment by employees; Also includes abuse of company's credit and adjustment policy</td>
</tr>
<tr>
<td>Mobile Malware</td>
<td>Compromised Mobile Applications</td>
</tr>
<tr>
<td>Payment Fraud</td>
<td>Utilization of stolen credit cards, debit cards or counterfeit checks in order to obtain goods and services</td>
</tr>
<tr>
<td>PBX Hacking</td>
<td>Compromised PBX systems used to make calls</td>
</tr>
<tr>
<td>IP PBX Hacking</td>
<td>Compromised IP PBX used to make fraudulent calls</td>
</tr>
<tr>
<td>Phishing / Pharming</td>
<td>Theft of personal info or credentials via hacking, phishing, vishing, etc...</td>
</tr>
<tr>
<td>Covid Related – Phishing / Pharming</td>
<td>Phishing / Pharming-Theft of personal info or credentials via hacking, phishing, vishing, etc... related to the Covid-19 Pandemic</td>
</tr>
<tr>
<td>SMS Phishing/Pharming</td>
<td>Theft of personal info or credentials via hacking, phishing, vishing, etc.</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Covid Related – SMS Phishing/Pharming</td>
<td>Theft of personal info or credentials via hacking, phishing, vishing, etc... related to the Covid-19 Pandemic</td>
</tr>
<tr>
<td>Pre-Paid Equipment &amp; Services</td>
<td>All types of fraud and abuse involving pre-paid equipment and services</td>
</tr>
<tr>
<td>Signaling and Manipulation</td>
<td>Manipulation of the SIP or SS7 signaling message to hide the true origination or identity of a caller</td>
</tr>
<tr>
<td>False Answer Supervision</td>
<td>Making incomplete calls appear as completed calls, which may be billed</td>
</tr>
<tr>
<td>SIM Cloning</td>
<td>Duplicated SIM card used to charge phone calls back to the original SIM card</td>
</tr>
<tr>
<td>SMS Faking or Spoofing</td>
<td>Manipulation of the ANI to hide the true origination or identity of SMS or MMS</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Manipulation of an employee or a customer to unintentionally give out important information. For example: law enforcement and government impersonation scams, 9-0-# Scams, IRS Scams, etc.</td>
</tr>
<tr>
<td>Covid-Related Social Engineering</td>
<td>Manipulation of an employee or a customer to unintentionally give out important information related to the Covid-19 Pandemic</td>
</tr>
<tr>
<td>Spoofing (IP or CLI/ANI)</td>
<td>Manipulation of the IP address/CLI/ANI to hide someone's true origination or identity</td>
</tr>
<tr>
<td>Covid-Related Spoofing (IP or CLI/ANI)</td>
<td>Covid-Related Social Engineering Manipulation of the IP address/CLI/ANI to hide someone's true origination or identity</td>
</tr>
<tr>
<td>Subscription Fraud (Application)</td>
<td>Creation of false details to gain access to goods and services with no intention to pay</td>
</tr>
<tr>
<td>Subscription Fraud (Credit Muling/Proxy)</td>
<td>Utilization of real identity details (with authorization for payment) to obtain goods and services with no intention to pay</td>
</tr>
<tr>
<td>Subscription Fraud (Identify)</td>
<td>Utilization of a real or synthetic identity with or without the owner’s knowledge to obtain goods and services with no intention to pay</td>
</tr>
<tr>
<td>Voicemail Hacking (Not associated with PBX Hacking)</td>
<td>Compromised voicemail system used to make calls or transfer messages, which are billed to the mailbox owner</td>
</tr>
<tr>
<td>Wangiri (Call Back Schemes)</td>
<td>Call back fraud schemes</td>
</tr>
<tr>
<td>Robocalling</td>
<td>Use of computerized auto</td>
</tr>
<tr>
<td>5G</td>
<td>Includes all fraud methods related to 5G services</td>
</tr>
<tr>
<td>IoT</td>
<td>Includes all fraud methods related to IoT services.</td>
</tr>
</tbody>
</table>
## Fraud Type Definitions

<table>
<thead>
<tr>
<th>Fraud Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arbitrage</td>
<td>Exploitation of the differences in rates between different countries</td>
</tr>
<tr>
<td>Cable or Satellite</td>
<td>Signal theft or retransmission from a cable or satellite provider</td>
</tr>
<tr>
<td>Commissions Fraud</td>
<td>Schemes used by dealers to collect additional commissions and spiffs</td>
</tr>
<tr>
<td>Denial of Service (DoS) and Distributed Denial of Service (DDoS)</td>
<td>An explicit attempt to make a machine or network resource unavailable to the users of a service</td>
</tr>
<tr>
<td>Traffic Pumping (includes: Domestic Revenue Share, Toll Free Traffic Pumping and International Toll Free Traffic Pumping)</td>
<td>Abuse of Communication service provider Interconnect agreements through such things as Traffic Pumping, Switch Access Stimulation, 8yy Dip Pumping and CNAM Revenue pumping schemes</td>
</tr>
<tr>
<td>Device / Hardware Reselling</td>
<td>Resale of equipment such as handsets, tablets, IPTV devices, routers, etc.</td>
</tr>
<tr>
<td>Friendly Fraud</td>
<td>Utilization of Charge Backs, Returned Checks, Card Holder Not Present, etc.... to perpetuate services</td>
</tr>
<tr>
<td>Voice Interconnect Bypass (e.g. SIM box)</td>
<td>Unauthorized insertion of traffic onto another communication service provider’s network. This includes Interconnect Fraud and GSM Gateway Fraud or SIM Boxing</td>
</tr>
<tr>
<td>Data Charging Bypass</td>
<td>Exploitation of network and protocol misconfigurations to bypass charging. For example, interjecting voice traffic onto Viber, Skype or WhatsApp</td>
</tr>
<tr>
<td>International Revenue Share Fraud (IRSF)</td>
<td>Artificial inflation of traffic terminating to international revenue share providers</td>
</tr>
<tr>
<td>Domestic Premium Rate Service (In Country)</td>
<td>Artificial inflation of traffic terminating to domestic premium service providers</td>
</tr>
<tr>
<td>Voice Service Reselling (e.g.: Call Selling)</td>
<td>Resale of voice services.</td>
</tr>
<tr>
<td>Data Service Reselling (e.g.: Reselling Hotspot Services)</td>
<td>Resale of data services</td>
</tr>
<tr>
<td>Theft / Compromise of data (e.g. logins)</td>
<td>Includes such things as the acquisition of personal information or intellectual property</td>
</tr>
<tr>
<td>Theft / Stolen Goods</td>
<td>Equipment theft</td>
</tr>
<tr>
<td>Theft of Content</td>
<td>Stealing content such as ringtones, games, or applications</td>
</tr>
<tr>
<td>Wholesale SIP Trunking Fraud</td>
<td>Exploitation of wholesale SIP trunking services to terminate calls</td>
</tr>
<tr>
<td>IoT Fraud</td>
<td>Includes all frauds related to IoT devices (For example: Denial of Service or Ransomware attacks).</td>
</tr>
<tr>
<td>Mobile Money Fraud</td>
<td>Transfer of funds from a victim’s mobile money account under false pretenses</td>
</tr>
</tbody>
</table>
This report is dedicated to Mark Zmigrodsiki

Mark Zmigrodsiki, CFE, CCSP who collaborated and contributed to this Fraud Loss report. Mark was involved in the CFCA for many years and served on the CFCA board as well as contributing and chairing a number of committees including the Communicator newsletter. CFCA will be forever grateful for his contribution and collaboration.

4th February 1960 – October 1st 2021

Thank you

CFCA Board and Executive Committee wish to thank all the contributors to this survey

President
Stacy Graham, CCSP
Inteliquent

Vice President
Tim Prugar,
Next Caller

CFO
Adam Panagia
AT&T

Secretary
Jacob Howell, CCSP
Teoco

COO
Jason Lane-Sellers
Lexis Nexis Risk Solutions

Directors
Mary Hochheimer, CCSP,
Inteliquent

Amber Kerr,
Union Wireless

Stephen Ornadel,
Mobileum

Stephen Schwed,
Verizon

Directors
Adrian, Lazar Adler
T-Mobile

Jamie Zetterstrom, CCSP
Intrado

Terry Powell, CCSP
Lumen
About Communications Fraud

Communications fraud is the use of telecommunications products or services with no intention of payment. Fraud negatively impacts everyone, including residential and commercial customers. The losses increase the communications service providers’ operating costs. Although communications operators have increased measures to minimize fraud and reduce their losses, criminals continue to abuse communications networks and services. Therefore, communications operators tend to keep their actual loss figures and their plans for corrective measures confidential. Due to the sensitive nature of this topic, CFCA used a confidential opinion survey of global communications operators to support the global fraud loss study.

About CFCA

CFCA is a not-for-profit global educational association that is working to combat communications fraud. The mission of the CFCA is to be the premier international association for revenue assurance, loss prevention and fraud control through education and information. By promoting a close association among telecommunications fraud security personnel, CFCA serves as a forum and clearinghouse of information pertaining to the fraudulent use of communications services. For more information, visit CFCA at www.CFCA.org.

Correspondence should be sent to fraud@cfca.org

Disclaimer of Liability

The material and information contained in this document is for general information purposes only. You should not rely upon the material or information in this document as a basis for making any business, legal or any other decisions.

Whilst we endeavor to provide correct information, CFCA makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability, or availability with respect to the information and graphics contained in this document for any purpose. Any reliance you place on such material is therefore strictly at your own risk. CFCA will not be liable for any false, inaccurate, inappropriate, or incomplete information presented in this document.

To the extent not prohibited by law, in no circumstances shall CFCA be liable to you or any other third parties for any loss or damage (including, without limitation, damage for loss of business or loss of profits) arising directly or indirectly from your use of information contained in this document.