CFCA 2019 Fraud Loss Survey

A message from the President of the CFCA

*Jason Lane-Sellers*

I always get excited when the hard work of reviewing, assessing and consolidating the results of the Fraud Loss Survey are completed and we can present and discuss the results. It is positive to see our partners supporting this initiative and wish to thank all the CSP’s who have spent time to respond. This year sees more global responses with North American responses for the first time being exceeded by Western European 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. I am always pleasantly surprised by some of the responses and always keen to consolidate the results to see what has changed since the last survey. Thank you for 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.

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.

We hope you enjoy reading the content below, 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

2019 Fraud Loss Survey

Survey Type & Methodology .................................................................................................................................................. 5
In which region are you located? ........................................................................................................................................... 6
Number of employees in your company? .............................................................................................................................. 6
How many subscribers do you have? .................................................................................................................................... 7
What is your annual revenue? ............................................................................................................................................... 7
What percent of YOUR COMPANY’s revenues are monitored by your organization? ................................................................. 8
What percentage of overall revenues requires your organization’s intervention or action to mitigate against fraud? .......... 8
Where is your fraud department situated? .......................................................................................................................... 9
How many levels of management exist between you and your Chief-Executive or Board? ...................................................... 9
How long have you worked within the telecom industry? ...................................................................................................... 10
How long have you been working in your fraud management organization? .................................................................. 10
How long has the fraud management department / team existed? ....................................................................................... 11
What functions apply to your current role and responsibilities? ........................................................................................... 11
How many people (FTE) work on fraud management activities? ............................................................................................ 12
How many are in your fraud department? .......................................................................................................................... 12
Where are job functions outsourced? .................................................................................................................................. 13
When is your fraud department staffed? .............................................................................................................................. 13
Have you created any new positions or new job functions within your organization? If so, what? ........................................ 14

WORKLOAD

How many fraud incidents does your department handle per month? ............................................................................... 15
How many fraud incidents does your department handle per month? ............................................................................... 15
Does your department use automation tools in any of the following areas? ........................................................................... 16
How many cases does your department refer to law enforcement per YEAR? ....................................................................... 16
Of the cases reported to law enforcement, how many result in a law enforcement action per YEAR? ............................... 17
Of the cases reported to law enforcement, how many were related to internal fraud investigations that resulted in a law enforcement action per YEAR? .................................................................................. 17
Why are cases not reported to law enforcement? .................................................................................................................. 18

FRAUD MANAGEMENT SYSTEM (FMS) BENCHMARKING

What is the accuracy of your Fraud Management System*? .................................................................................................. 19
How much time do you spend on average working false-positive cases per week? ............................................................ 20
Do you subscribe to a 3rd party to obtain data for use within your fraud management system? ........................................ 20

© Copyright 2019 CFCA
Fraud Loss Survey 2019
How frequently are Current Fraud Management control rules and thresholds reviewed and adjusted? .................................................. 21
How frequently are New fraud management control rules and thresholds reviewed and adjusted? .................................................. 21

FRAUD TRENDS
Over the past 12 months, do you think GLOBAL fraud losses have trended up, trended down, or stayed the same? .......... 22
Over the past 12 months, has fraud IN YOUR COMPANY trended up, trended down, or stayed the same? ......................... 22
What do you view as the top 5 fraud methods at YOUR COMPANY? ......................................................................................... 23
What do you view as the top 5 fraud methods GLOBALLY? ........................................................................................................ 23
What do you view as the top 5 EMERGING fraud methods at YOUR COMPANY? ................................................................. 24
What do you view as the top 5 fraud types GLOBALLY? .............................................................................................................. 24
What do you view as the top 5 fraud types in YOUR COMPANY? ............................................................................................... 25
What do you view as the top 5 EMERGING fraud types at YOUR COMPANY? ........................................................................ 25
WHERE IS THE FRAUD COMING FROM? .......................................................................................................................... 26
Top 10 Countries That ORIGINATE Fraudulent Calls: ........................................................................................................... 26
Top 10 Countries Where Fraud TERMINATES: ..................................................................................................................... 26

FRAUD LOSS ESTIMATES
What percentage of bad debt is a result of fraud in YOUR COMPANY? .................................................................................... 27
What percentage of the total GLOBAL telecom revenue base do you think is fraud? ................................................................. 27
Of the Global telecom revenue base, what percentage do you think is fraud? ........................................................................ 28
Comparison Between 2013-2019 Survey Results in YOUR COMPANY .......................................................................................... 28
What percentage of YOUR COMPANY'S revenue base do you think is fraud? ........................................................................ 29

ESTIMATED GLOBAL LOSS
Comparison to Previous Years .................................................................................................................................................. 30
2019 Fraud Loss Highlights ....................................................................................................................................................... 31
APPENDIX .................................................................................................................................................................................. 32
  Estimated Fraud Losses by Method ....................................................................................................................................... 32
  Combined Fraud ........................................................................................................................................................................ 33
  Fraud Method Definitions: ......................................................................................................................................................... 34
Survey Type & Methodology

Panel of Experts Survey:

Surveys taken from fraud and security experts working within the industry who are directly involved in identifying and stopping communications fraud.

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

CFCA wish to thank all of our partners who advertised and promoted the survey to their members and the chart below show how many different associations are represented in the survey.
In which region are you located?

We try and encourage as many different operators and regions to complete the survey, but of course are dependent on respondents. Europe is the highest range of respondents; this high number is also influenced by several of the group OpCos which have the headquarters based in Europe.

Number of employees in your company?

The Survey also represents different types and sizes of operations, this spread of company size ensures we get a full view of fraud issues across the spectrum of different telecoms operations.
How many subscribers do you have?

Again, the Survey also represents sizes of operations from a customer perspective, as we want to ensure that all types of different customer operations are represented, covering consumer, enterprise and intercarrier.

What is your annual revenue?

By having different size companies and revenue perspectives, also helps us align an understanding of fraud cost impacts to the organizations in the later responses.
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.

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

The results here reflect that 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.
Where is your fraud department situated?

Reporting via Finance operations still dominate, however compared to 2017, FMOs located under Finance decreased by 10% and under Customer Care decreased by 5%. Corporate Security, Risk Management and Business Operations saw an increase of 2-3%. Several FMOs reported being moved under Revenue Assurance, Product Management, Internal Audit, or being decentralized across their business.

This response does show, there is no real consistency or conformity across the industry, and fraud departments can sit in various areas of the telco.

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

More than 50% of fraud departments are located within 2 levels of management of their senior leadership. Many reported their organizations were becoming flatter.
How long have you worked within the telecom industry?

We wanted to establish the general telecommunications expertise residing within operational departments, and we can see the fraud department does tend to have highly experienced personnel from within the industry within their operations with 57% of respondents have been in the industry more than 15 years and 36% of respondents had 20+ years of experience within the telecom industry.

How long have you been working in your fraud management organization?

However, when analyzing the actual fraud management experience within teams, the results showed a greater variation, we feel that this is a positive message, as it allows fresh ideas and insight to be brought into teams. This allows departments to manage new technologies and risks.
How long has the fraud management department / team existed?

These results show that a fraud department is becoming a standard function and accepted within a telecoms organization and well established which is positive, although we now considering other responses need to look at how it orchestrated and range of operations.

What functions apply to your current role and responsibilities?

This shows that even though fraud departments are established within organisations and have experienced personnel, the operations are still having to perform a diverse range of responsibilities.

This diversity may also be a reason why many fraud operations do not provide full coverage of revenue risks within an organisation, as the operations is not focussed on only fraud related activities.
How many people (FTE) work on fraud management activities?

Compared to 2017, staffing increased by 2%, with the exception of outsourcing which decreased by 5%.

How many are in your fraud department?

<table>
<thead>
<tr>
<th># Subscribers</th>
<th>Average # Employees</th>
<th>Average # Outsourced</th>
<th>Average Total Department Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;10,000</td>
<td>5</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>10,001 to 1,000,000</td>
<td>6</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>1,000,001 to 10,000,000</td>
<td>9</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>10,000,001 to 50,000,000</td>
<td>19</td>
<td>2</td>
<td>21</td>
</tr>
<tr>
<td>50,000,001+</td>
<td>68</td>
<td>13</td>
<td>81</td>
</tr>
<tr>
<td>Wholesale Only (no end user subs)</td>
<td>6</td>
<td>1</td>
<td>7</td>
</tr>
</tbody>
</table>

Compared to 2017, staffing increased by 2%, with the exception of outsourcing which decreased by 5%.

However, the above statistics do show how sparse many operational teams are in terms of resources, especially if these teams are to provide 24/7 operations and a wider revenue coverage.
Where are job functions outsourced?

Compared to 2017, 8% of outsourced jobs were insourced to other internal organizations.

When is your fraud department staffed?

Compared to 2017, Fraud departments are working ~50% fewer business hours on holidays and ~18% fewer non-business hours during the week. More weekend and holiday coverage is being provided by other functions outside the fraud team, whether internal or external.
Have you created any new positions or new job functions within your organization? If so, what?

**New Fraud Department Positions:**

- Anti-Spam
- Online Digital Security
- IOT Fraud Detection
- E-commerce and Payment Fraud Protection
- Digital and Online Sales Risk Management
- Mobile Money Risk Management
- Cyber Security Risk Management
- Data Science
- Staff Augmentation

The creation of these new positions is very interesting, the identification of Online, Digital, Cyber and IOT services shows the direction of potential risks and issues going forward. Organizations are realizing that the next generation of services and risks are going to be digital.
WORKLOAD

How many fraud incidents does your department handle per month?

Compared to 2017, fraud departments reported a 24% increase in incident workload, highlighting the increase in attempts of fraud in the industry.

How many fraud incidents does your department handle per month?

<table>
<thead>
<tr>
<th># Subscribers</th>
<th>Averaged # Incidents per Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;10,000</td>
<td>1,640</td>
</tr>
<tr>
<td>10,001 to 1,000,000</td>
<td>4,375</td>
</tr>
<tr>
<td>1,000,001 to 10,000,000</td>
<td>12,582</td>
</tr>
<tr>
<td>10,000,001 to 25,000,000</td>
<td>6,018</td>
</tr>
<tr>
<td>25,000,001 to 50,000,000</td>
<td>1,640</td>
</tr>
<tr>
<td>50,000,001+</td>
<td>4,924</td>
</tr>
<tr>
<td>Wholesale Only (no end user subs)</td>
<td>546</td>
</tr>
</tbody>
</table>
Does your department use automation tools in any of the following areas?

Rules based systems dominate the types of tools utilized, but ML/AI tools are starting to be utilized. But as reported on the types of positions organizations are looking to recruit, we may see more BI tools and digital online tools in the future.

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

Overall, 7% fewer cases were reported to law enforcement than in 2017.
Of the cases reported to law enforcement, how many result in a law enforcement action per YEAR?

In 2019, 3% fewer investigations were initiated by law enforcement. However, 17% more cases were prosecuted.

Of the cases reported to law enforcement, how many were related to internal fraud investigations that resulted in a law enforcement action per YEAR?

In 2019, 4% fewer internal fraud investigations were initiated. However, 5% more cases were prosecuted.
Why are cases not reported to law enforcement?

The results show that overall operators are submitting less cases to law enforcement, mainly due to the fact there is a perceived lack of interest or understanding of telecoms fraud issues. However, the previous results show that law enforcement are starting to progress more cases successfully, so maybe it has just taken time for Law enforcement to understand and gain an ability to successfully prosecute, and maybe telecoms organizations should look to pursue more with Law enforcement.
FRAUD MANAGEMENT SYSTEM (FMS) BENCHMARKING

What is the accuracy of your Fraud Management System*?

FMS systems showed a wider dispersion of accuracy in correct decision making in relation to fraud cases.

What is the accuracy of your Fraud Management System*?

False alerts within FMS systems are also spread, with higher percentages of respondent reporting that some FMS systems are particularly inaccurate with 28% reported >90% false positive cases being generated by their FMS compared to 19% reported >90% false positive cases being generated by their non-FMS based controls and processes.

The concern here is the impact on operations that are already scarce on resource – and that FMS should be managed and tuned regularly.
How much time do you spend on average working false-positive cases per week?

1/3rd of CSPs reported they did not monitor their false-positive caseloads, nor how much time was spent investigating those cases. This is a particular concern, as these operations could be highly inefficient and therefore exposing their organizations to higher levels of fraud risk.

Do you subscribe to a 3rd party to obtain data for use within your fraud management system?

3rd Party Data Sources include: iconectiv's IPRN number lists, YFCL Prism & YouMail alerts, CFCA & GSMA Hotlists, and CFCA Fraud Alerts
How frequently are **Current** Fraud Management control rules and thresholds reviewed and adjusted?

Although FMS accuracy reported stats were not necessarily a positive picture for the industry, departments are regularly reviewing and adjusting their rules.

How frequently are **New** fraud management control rules and thresholds reviewed and adjusted?

60% or respondents review and adjust new fraud management control rules and thresholds on at least a quarterly basis.
FRAUD TRENDS

Over the past 12 months, do you think GLOBAL fraud losses have trended up, trended down, or stayed the same?

Compared to 2017, 13% fewer CSPs thought fraud was trending up.

Over the past 12 months, has fraud IN YOUR COMPANY trended up, trended down, or stayed the same?

Compared to 2017, 16% more CSPs reported fraud in their company had trended up. 18% fewer reported it had stayed the same. This contrasts with the perception of the general telecoms industry fraud growth.
What do you view as the top 5 fraud methods at YOUR COMPANY?

In 2019, Subscription fraud is still a number one issue – although the form has changed highlighting the growth of synthetic issues. Subscription was also double the level of other reported issues, highlighting its dominance as an issue.

Interestingly payment fraud is on the regrowth, jumping into the top five compared to previous years when it had dropped an issue. Wangiri also jumps into the top five, this is becoming a major worldwide issue.

In 2017, the top five fraud methods were Subscription Fraud (Identity), PBX Hacking, IP PBX Hacking, Subscription Fraud (Application), and Subscription Fraud (Credit Muling/Proxy)

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

In 2017, the top five were: PBX Hacking, IP PBX Hacking, Subscription Fraud (Application), Account Take Over and Subscription Fraud (Credit Muling/Proxy).
What do you view as the top 5 EMERGING fraud methods at YOUR COMPANY?

Account takeover maintains in the top five, but payments and IOT are perceived threats emerging.

In 2017, the top five threats were: IP PBX Hacking, Phishing/Pharming, Account Takeover, Subscription Fraud (Application), Subscription Fraud (Credit Muling/Proxy)

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

In 2017, the top fraud types were: IRSF, Interconnect Bypass, Arbitrage, Premium Rate Service, Commissions Fraud.
What do you view as the top 5 fraud types in YOUR COMPANY?

In 2017, the top fraud types were: IRSF, Interconnect Bypass, Arbitrage, Premium Rate Service, and Theft/Stolen Goods.

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

In 2017, the top five fraud types were: International Revenue Share Fraud (IRSF), Interconnect Bypass, Premium Rate Service, Domestic Revenue Share Fraud and Arbitrage.

It is worth noting (and detailed in the appendix) that although IRSF is still the number one issue listed in the fraud types, as a revenue loss figure it is down to nearly half of the value ($5B) it was recorded in 2015 ($10B).
WHERE IS THE FRAUD COMING FROM?

Top 10 Countries That ORIGINATE Fraudulent Calls:

In 2017, the top 3 countries were United States, Spain and the United Kingdom. The UK has been consistently in the top ten in every survey, but it can be seen that there is an apparent eastern European growth in terms of origination.

It should be stated, that in terms of both the origination and termination of locations for fraud is dependent on the responses from the survey member and their determination of the location.

Top 10 Countries Where Fraud TERMINATES:

In 2017, the top 3 countries were Cuba, Latvia and Lithuania. Cuba is still number one, and this is a worldwide issue, not just north America when we break down the responses. Again, the UK is dominant as it has been for many surveys, due to the structure of its number plan, hiding high risk destination numbers.
**FRAUD LOSS ESTIMATES**

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

In 2019, the number of CSPs reporting 10-20% of their bad debt related to fraud doubled. Showing that a growth in fraud in relation to debt.

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

In 2019, a majority of CSPs believed fraud losses were between 1-2%. In 2015 and 2017, the consensus was between 2-3%.
Of the Global telecom revenue base, what percentage do you think is fraud?

Smaller CSPs generally think fraud losses are higher globally.

Comparison Between 2013-2019 Survey Results in YOUR COMPANY

Beginning in 2013 CSPs reported fewer fraud losses each year. However, in 2019 CSPs began reported an increase in fraud losses. In 2019, 71% of CSPs still reported losses less than 2%, a 10% decrease from 2017.
What percentage of YOUR COMPANY’S revenue base do you think is fraud?

Smaller CSPs generally report higher fraud losses in their company.
ESTIMATED GLOBAL LOSS

2019 Estimated Global Telecom Revenues*:

- $1.625 Trillion (USD)

2019 Estimated Global Loss:

- $28.3 Billion (USD), or 1.74%

Comparison to Previous Years

This data shows us a few aspects...

After several years of reduction, it appears that fraud loss and impact is on the rise in terms of a percentage of revenue for telecoms operations. However, the actual dollar figure of loss in billions is slightly less than previous surveys. This is not a reduction in fraud loss, but due to the fact general revenues in telecoms has reduced since 2017 and as such even though the percentage of fraud has grown this is not reflected in the dollar figure.

Actually, the survey on survey rise in percentage terms is quite significant, as it shows a rise of over 30% on previous loss percentage figures. Another aspect to consider here is this figure is also should be considered in reflection of that many of those responding to the survey stated they did not have fraud operational coverage of over 50% of the revenue streams, and as such this loss figure should be considered as an underestimate of the true fraud loss value.
2019 Fraud Loss Highlights

- Global Fraud Loss Estimate*:
  - **$28.3 Billion** (USD) annually
  - **1.74%** of global telecom revenues
  - The increase from 2017 is attributed to several factors including:
    - Cross-Industry Scams (Wangiri, Account Take-over & financial scams)
    - Less collaboration and coordination within the industry with law enforcement
    - Increased consumer data attacks targeting consumer causing cross over impacts of fraud scams between industries
    - New service and technology revenues starting to be mass utilized and impact revenue streams

- 73% said global fraud losses had increased or stayed the same, 66% said fraud had trended up or stayed the same within their company

<table>
<thead>
<tr>
<th>Top 10 Fraud Methods:</th>
<th>Top 10 Fraud Types*:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1.92 B – Subscription Fraud (Application)</td>
<td>$5.04 B – International Revenue Share Fraud (IRSF)</td>
</tr>
<tr>
<td>$1.82 B – Payment Fraud</td>
<td>$3.28 B – Arbitrage</td>
</tr>
<tr>
<td>$1.82 B – PBX Hacking</td>
<td>$2.71 B – Interconnect Bypass (e.g. SIM Box)</td>
</tr>
<tr>
<td>$1.82 B – IP PBX Hacking</td>
<td>$2.27 B – Domestic Premium Rate Service (In Country)</td>
</tr>
<tr>
<td>$1.82 B – Wangiri (Call Back Schemes)</td>
<td>$2.00 B – Traffic Pumping (includes: Domestic Revenue Share, TFTP)</td>
</tr>
<tr>
<td>$1.63 B – Abuse of network, device or configuration weaknesses</td>
<td>$1.76 B – Commissions Fraud</td>
</tr>
<tr>
<td>$1.44 B – Dealer Fraud</td>
<td>$1.76 B – Device / Hardware Reselling</td>
</tr>
<tr>
<td>$1.34 B – Subscriber Fraud (Identity)</td>
<td>$1.49 B – Theft / Stolen Goods</td>
</tr>
<tr>
<td>$1.25 B – Account Take Over</td>
<td>$1.17 B – Friendly Fraud</td>
</tr>
<tr>
<td>$1.15 B – Internal Fraud / Employee Theft</td>
<td>$ .98B – Wholesale SIP Trunking Fraud</td>
</tr>
</tbody>
</table>

*The top 5 fraud types accounted for 54% of all fraud losses.

Subscription fraud when combined totals the equivalent value of IRSF, and IRSF has hugely reduced in dollar terms from previous fraud loss surveys.
APPENDIX

Estimated Fraud Losses by Method

Estimated Fraud Losses by Method (in $ USD Billions)

<table>
<thead>
<tr>
<th>Method</th>
<th>Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription Fraud (Application)</td>
<td>$1.9</td>
</tr>
<tr>
<td>PBX Hacking</td>
<td>$1.8</td>
</tr>
<tr>
<td>Wangiri (Call Back Schemes)</td>
<td>$1.8</td>
</tr>
<tr>
<td>Abuse of network, device or configuration weakness</td>
<td>$1.6</td>
</tr>
<tr>
<td>Dealer Fraud</td>
<td>$1.4</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>$0.2</td>
</tr>
<tr>
<td>SIM Hijacking</td>
<td>$0.2</td>
</tr>
<tr>
<td>IOT</td>
<td>$0.4</td>
</tr>
<tr>
<td>Clip-on Fraud</td>
<td>$0.5</td>
</tr>
<tr>
<td>Signalling Manipulation and False Answer Supervision</td>
<td>$0.6</td>
</tr>
<tr>
<td>Brand Name / Logo Abuse</td>
<td>$0.6</td>
</tr>
<tr>
<td>Voicemail Hacking (Not associated with PBX Hacking)</td>
<td>$0.7</td>
</tr>
<tr>
<td>IMEI Re-programming</td>
<td>$0.7</td>
</tr>
<tr>
<td>Pre-Paid Equipment &amp; Services</td>
<td>$0.8</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>$0.9</td>
</tr>
<tr>
<td>Robocalling</td>
<td>$0.9</td>
</tr>
<tr>
<td>Spoofering (IP or CL/ANI)</td>
<td>$1.0</td>
</tr>
<tr>
<td>SMS Faking or Spoofing</td>
<td>$1.0</td>
</tr>
<tr>
<td>Subscription Fraud (Identify)</td>
<td>$1.3</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>$1.2</td>
</tr>
<tr>
<td>Internal Fraud / Employee Theft</td>
<td>$1.1</td>
</tr>
<tr>
<td>Phishing / Pharming</td>
<td>$1.1</td>
</tr>
<tr>
<td>Subscription Fraud (Credit Muling/Proxy)</td>
<td>$1.1</td>
</tr>
<tr>
<td>Abuse of Service Terms and Conditions</td>
<td>$1.1</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>$0.2</td>
</tr>
<tr>
<td>Mobile Malware</td>
<td>$0.8</td>
</tr>
</tbody>
</table>
Combined Fraud

Estimated Fraud Losses by Type (in $ USD Billions)

- Interconnect Gypsum (e.g., SIM box): $3.3
- Arbiage: $2.7
- Traffic Pumping (includes: Domestic Revenue Share, Toll Free Traffic Pumping): $2.3
- Mobile Money: $2.0
- Theft / Stolen Goods: $1.8
- Cable or Satellite: $1.8
- Domestic Premium Rate Service (In Country): $1.5
- Device / Hardware Reselling: $1.2
- IOT: $1.0
- Service Reselling (e.g., Call Sell): $0.9
- Commissions Fraud: $0.9
- Denial of Service (DoS) and Distributed Denial of Service (DDoS): $0.9
- Theft / Compromise of data (e.g., logins): $0.6
- Wholesale SIP Trunking Fraud: $0.6
- Theft of Content: $0.6
- Other (please specify): $0.3
- Private Use: $0.4
- Friendly Fraud: $0.5
- International Revenue Share Fraud (IRSF): $5.0

Total Estimated Fraud Losses: $5.04 billion
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>Abuse of Service Terms and Conditions</td>
<td>Violation of the carrier’s service terms and conditions or acceptable use policy.</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>Manipulation and utilization of existing customer account in order to gain devices 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>IOT</td>
<td>Includes all fraud methods associated with IOT services</td>
</tr>
<tr>
<td>IP PBX Hacking</td>
<td>Compromised IP PBX used to make fraudulent calls</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>Phishing / Pharming</td>
<td>Theft of personal info or credentials via hacking, phishing, vishing, etc...</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>Robo-calling</td>
<td>Use of computerized autodialers to deliver pre-recorded messages to perpetrate fraud.</td>
</tr>
<tr>
<td>Signaling Manipulation and False Answer Supervision</td>
<td>Manipulation of the SIP or SS7 signaling message to hide the true origination or identity of a caller. This also includes making incomplete calls appear as completed calls, which may be billed</td>
</tr>
<tr>
<td>SIM Hijacking</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 AMI to hide the true origination or identity of SMS or MMS</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Manipulation of an employee or customer to un-intentionally give out important information</td>
</tr>
<tr>
<td>Spoofing (IP or CL/ANI)</td>
<td>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 authorisation 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 identify without the owners 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</td>
</tr>
<tr>
<td>Wangiri (Call Back Schemes)</td>
<td>Call back fraud schemes</td>
</tr>
</tbody>
</table>

Thank you!

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

President
Jason Lane-Sellers, CCSP
ThreatMetrix

Vice President
Stacy Graham, CCSP
Inteliquent

CFO
Adam Panagia
AT&T

Secretary
Jacob Howell, CCSP
Teoco

Past President
Christopher Walters, CCSP
Charter Communications

Directors
Heather Davis CCSP, Frontier Communications
Mary Hochheimer, CCSP, Inteliquent
Amber Kerr, Union Wireless
Tim Prugar, Next Caller
Stephen Orndel, Mobileum
Stephen Schwed, Verizon
Mark Zmigrodski, CFE, CCSP, AT&T
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 carriers’ 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.