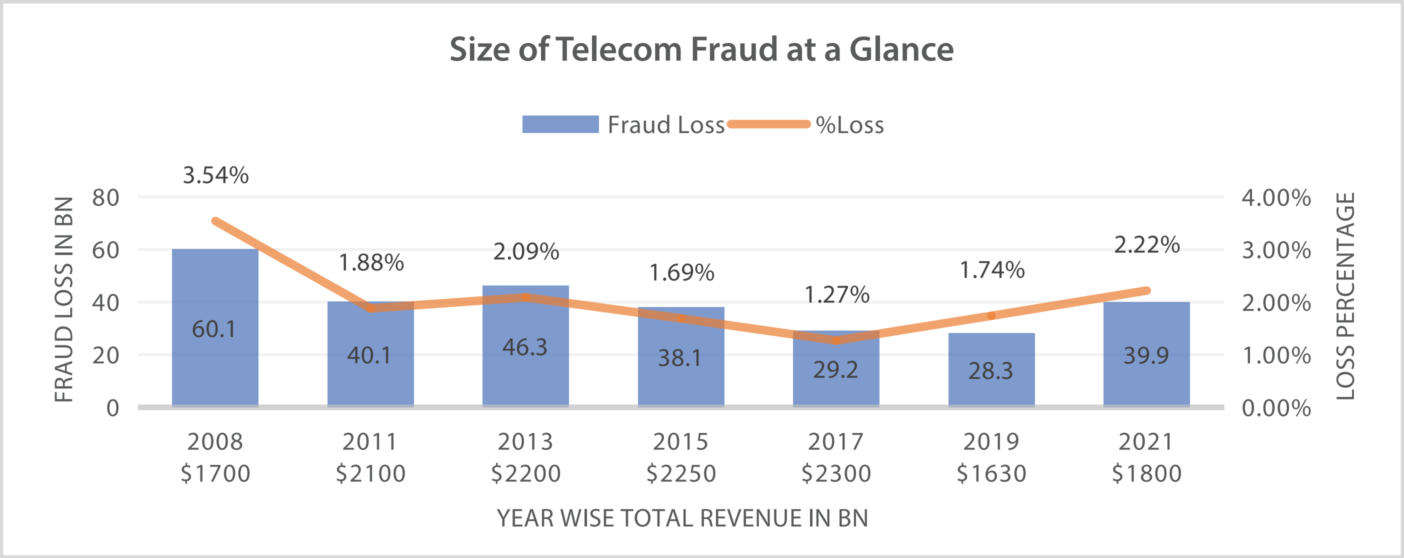
WHITE PAPER

FRAUD MANAGEMENT FOR CSPs: A PARADIGM SHIFT IN THE ERA OF 5G AND DIGITAL

Infosys®
Navigate your next

Introduction



Source of Data: CFCA survey Report 2021

Telecom fraud is the main contributor towards revenue loss for Communications Service Providers CSPs with figures averaging between 3-5 percent of CSPs annual revenue.

This is the most substantial risk to the communications business, eroding profit margins, high network capacity consumption and exposing customer relationships.

In this rapidly evolving new digital technology environment, with introduction of 5G or 5th generation mobile network with roll out of new features and services of 5G, we will see a complete translation of usage for individuals as well as enterprises. This will make telecom networks more complex and vulnerable as massive amount of data volume is expected.

From the analysis of the latest **CFCA** report 2021, it is evident that communication sector's revenue declined in 2019 and started moving upwards in 2021. In the view of increasing revenue also seen an up-trend in loss due to fraud.

According to the CFCA survey, total revenue loss of CSPs due to fraud in telecommunication in 2021 was $39.89 billion (around 2.2% of the global revenue). This is 28% (approximately $11.6 billion) increase in losses compared with 2019.

This number can increase in future due to introduction of 5G and new edge digital services which will pose threat to the telecom landscape and provide opportunities to malicious players to take advantage of network security vulnerabilities.

As per the survey conducted by **Kaleidointelligence** in the year 2020, it was predicted that telco fraud loss will increase, and it is evident from the CFCA report.

CSPs are still implementing strategies to effectively cope with traditional fraud types. With the introduction of new features and services of 5G, they are going to face newer types of threats. So, they need to rework on their assurance strategy by adopting future proof intelligent solutions.

In this paper we will provide our expert view on how to combat fraud in the 5G era, with our vision and recommended approach to implement the Next Generation fraud detection and prevention solution.

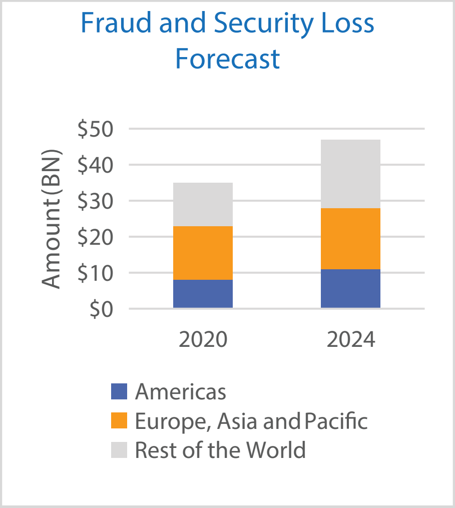
Top Fraud Leakage Type

IRSF Fraud Type ($6.69bn)

Next Highest Fraud Leakage Type

Traffic Pumping Fraud ($4.54bn)
(Domestic Revenue Share, Toll-Free Traffic Pumping)

Source of Data: CFCA survey Report 2021



Source of Data: Kaleidointelligence Report

Challenges and potentials for Fraud in new 5G Digital Era

Inherently more complex than prior avatars. It's a software driven network, with powerful Edge computing capabilities and ecosystem driven solutions to end customers. This ushers in a new paradigm with additional challenges in securing the underlying network and the CSPs services.

In telecommunications traditional services will continue (Voice, Text, Data, TV) and new 5G services will be offered (Industrial automation, remote medical, smart city, autonomous vehicles, AR, IOT, Internet of Medical Things (IoMT), etc.). In these 5G services, the communication interchange is done through access to cloud databases and by protocols established to support specific services, such as SIP, V2V, V2N, Zigbee, Xbee, Cat-M, NB-IoT among others which use traditional technology such as WIFI, Bluetooth, satellite or wired internet connection. But all of them have a common flexible IP-based core network. Cybercriminals know how to exploit the IP vulnerabilities to execute fraud attacks. So, these vulnerabilities become an abundant source for hackers and fraudsters to carry out their attacks.

Traditional and known frauds for Voice, SMS and Data will continue to occur. With added IP based 5G services, the main risks can be summarized as: authentication spoofing (Voice, SMS, Web portal-DNN), SIM swap/cloning, virus, malware, hijacking (devices, web portal) and man-in-the-middle exploiting application vulnerabilities (CVE, OWASP).

Mobile Network slicing is an important feature of 5G which helps CSPs in addressing many diverse and varied service demands. Network slicing allows service providers to create multiple virtualized and standalone logical networks within same physical network to provide desired services as per demand. The differentiated levels of services based on network slicing (which can be brought down post offering the service in a defined time window) will necessitate completely radical Fraud prevention algorithms and real time interventions.

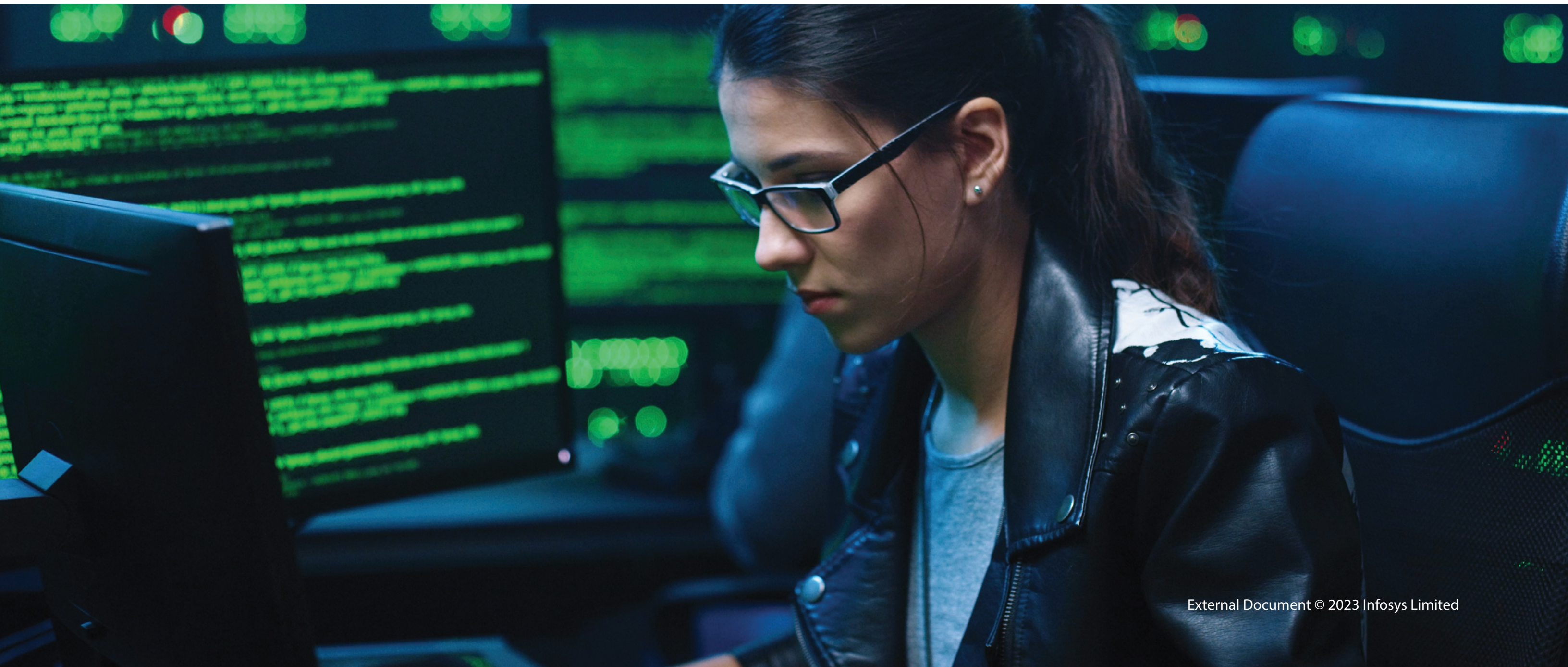
As 5G evolves, **IoT** services are going to gain popularity. These IoT devices have become an excellent target for hackers. With the increase in connected devices and sensors, there will be increased opportunity to capitalize on intelligence around data. This also provides hackers with a larger attack surface to hijack IoT devices and run **DDOS** attacks. Most IoT applications need an extension beyond the Telco boundary with a partner ecosystem. This adds complexity dictated by the level of maturity of those extended infrastructure and application tiers for the CSPs.

IT Security Challenges

Advancement of technology and use of new architecture and features such as network slicing, virtualization and cloud will create new challenges for CSPs like

- Not enough knowledge/tools to deal with security Vulnerabilities
- Vulnerabilities related to Network virtualization (NFVi) and software driven Network (SDN)
- Limited pool of security experts
- Increased attack surface
- Risk related to legacy technologies

In the "Emerging Fraud Methods" shows the fraud trends: Spoofing (IP or CLI/ANI), Wangiri, SIM swapping / jacking, PBX hacking, Robocalling, IoT. In general, these methods have in common the IP message manipulation to disguise the identity of the origin, or to manipulate the content of the IP message, to seize, hack, or impersonate users or IoT devices, with the purpose of committing fraud.



How can CSPs effectively monitor the sheer volume, speed, variety, and complexity of fraud events and threats in the 5G era?

With rollout of 5G across the sector, it will have more acceptance and subscriber base will increase with increase in revenue. So, it is important to have better assurance mechanism in place to protect their network and subscribers. CSPs should work out on the new strategies to build and in place a Next Generation FMS solution to prevent their revenue from these new challenges.

Analyze available data from multiple channels:

Traditional method of feeding data from different sources generating millions of events per second for analysis

Automatic monitoring and prevention of fraudulent transactions:

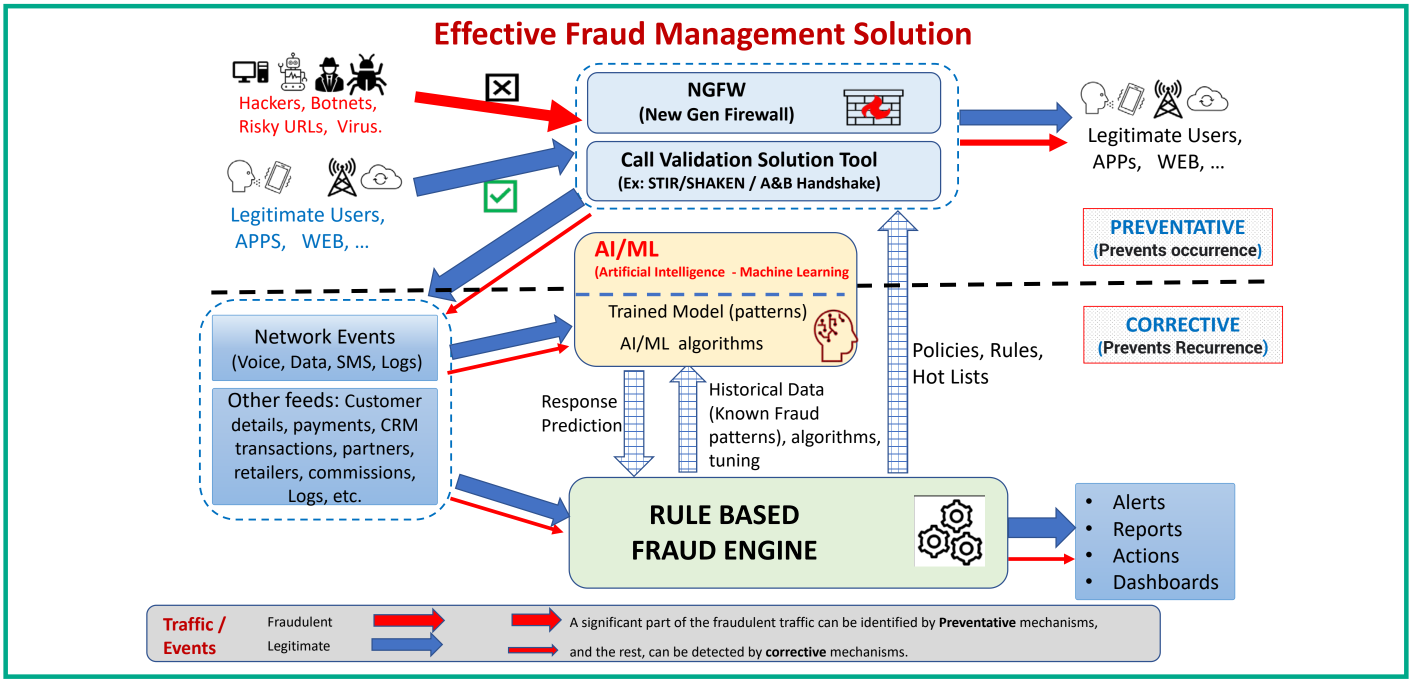
Real time decision making before event completion

Real-time intelligence and event processing:

Intelligent insights using attribute analysis and ML models for predictive interventions

Use of tools for network protection:

Network security mechanisms complementing fraud management


Effective Fraud Management Solution

Next Generation Fraud management solution:

Service providers are currently using the traditional rule-based tool with deterministic fraud detection methods. It includes an expression evaluated as part of a Rules engine, triggers alerts when thresholds are breached.

In 5G, the number of events that circulate through the network are increasing exponentially and the usage volume is also going to increase multi-fold due to services like IoT (with millions of devices). So, the traditional rule-based telecom fraud prevention tools need enhancement to prevent fraud.

Broadly, the discipline has two constituents, namely Corrective and Preventive mechanisms.

Corrective mechanisms:

The typical corrective mechanisms are undergoing a transformation that covers both the modus and its practitioners..

Rule-Based Fraud Management System

The rule-based fraud management system is necessary for traditional voice, text and data frauds, these kinds of attacks will continue, with more sophisticated and different mechanisms. Also, to use it as an integration point for all additional fraud tools (AI, ML, NGFW, Call Validation), and to allow you to manage all the information, alerts, cases, investigations, etc.

Practitioner persona

Experienced 5G network fraud analysts required with desirable knowledge in AI/ML, IP protocols, cloud, in addition to traditional telecom fraud knowledge. Skilled personnel with the domain knowledge are difficult to obtain in today's job market, so specialized training is required here to understand the new edge fraud behaviors.

Preventive mechanisms:

Due to the network architecture new preventive mechanisms are required. Here we are going to discuss few of these mechanisms

Network Protection tools

In addition to the traditional tools used by cybersecurity teams for protecting and blocking cyberattacks on infrastructure, network equipment, applications and data stored or in transit, the following two tools are essential in preventing attacks and fraud attempts.

Call Validation Solution tools

Call validation tools are essential to control CLI spoofing and guarantee the identity of the originator. The most used tools are STIR/SHAKEN (mandatory in the US), and A&B Handshake (in deployment in Europe). These tools can detect most CLI spoofing, but they are neither foolproof nor all possible spoofing events.

Next-generation firewalls (NGFW)

NGFW technology is designed to protect the telecom networks from advanced security threats. This technology uses deep packet inspection firewalls combined with intrusion prevention system (IPS) or intrusion detection system (IDS).

It can block and control the security threats at application level. By using these kinds of firewalls, service providers can protect their networks from threats like, ransomware, malware and SQL injection which fraudster use for attacking by URL filtering or sandboxing.

All these mechanisms from the new age security domain need to synergize and play well together with the Fraud Mgt. domain to deliver the business assurance for the Digital Telco of tomorrow.

Common to Corrective and Preventative mechanisms:

Whichever solution we are implementing should have intelligence analysis inbuilt to analyze the pattern of fraud and generate alert proactively.

Artificial Intelligence + Machine Learning tools (AI + ML)

Fraud management is adopting AI and ML to monitor and analyze a large volume of data in real time, to discover, investigate, detect frauds, and mitigate data breaches. Fraud Detection with ML becomes possible due to the ability of ML algorithms to learn from historical fraud patterns and recognize them in the network traffic. AI and ML algorithms generate insights, provide suggestions on "how to move ahead" while detecting a particular scenario, can apply supervised and unsupervised learning in different scenarios.

The effectiveness of the AI and ML toolset depends on the Robustness, Flexibility and Agility of the Learning Models designed and deployed in the CSPs chosen fraud management solution

Conclusion.

To prevent and reduce fraud risks it is important to understand the nature of 5G, which has a software driven network. Cybercriminals can potentially exploit the vulnerabilities to execute fraud attacks.

Traditional and known frauds for Voice, SMS and Data usage will continue to occur. With added 5G services, the main risks can be summarized as: authentication spoofing (voice. SMS, web portal-DNN-), sim swap/clone, virus, malware, hijacking (devices, web portal) and man-in-the-middle exploiting application vulnerabilities.

Therefore, the effective solution for Fraud prevention and detection, is a combination of traditional Rule based Fraud management system, with AI/ML tools that can help to monitor and analyze a large volume of data in real time and supported by cybersecurity tools, such as Next-generation firewalls (NGFW), and Call Validation Solution tools (such as STIR/SHAKEN, or A&B Handshake). Industry forums like CVE & OWASP are working on addressing some of these challenges. Efficiency of any Fraud Mgt. solution also depends on knowledgeable SMEs in the discipline to tailor tools effectively.

We have presented different facets of the ongoing renaissance in the Fraud Management domain and the Next generation mechanisms to be deployed by CSPs to secure their revenue and margins. It promises to be a very interesting time with continuous discovery as application of 5G for Industry 4.0 evolves, bringing a fusion of multiple domains, necessitating designing upfront for robustness, flexibility and agility for the Digital Telco of tomorrow.

Infosys Business Assurance practice has experience of more than 20 years in the Telecom domain, complemented by robust alliances with leading OSS/BSS/Business Assurance product vendors. With a strong pool of consultants with expertise across the spectrum, repository of artifacts, cutting-edge tools, methodologies and processes we are well positioned as a leader in this space, providing a range of advisory, design, implementation, validation and support services to CSPs.

Abbreviations:

ANI	-	Automatic Number Identification
Cat-M	-	It refers to Category M, the second generation of LTE chipsets meant for IoT applications.
CFCA	-	Communications Fraud Control Association
CLI	-	Calling line identification
CSPs	-	Communications Service Providers
CVE	-	Common Vulnerabilities and Exposures
DDOS	-	Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks.
DNN	-	Data Network Name. The DNN is typically in the form of an APN (Access Point Name).
FMS	-	Fraud Management System
IoMT	-	Internet of Medical Things
IoT	-	Internet of Things
NB-IoT	-	Narrowband-Internet of Things (NB-IoT) is a standards-based Low Power Wide Area (LPWA) technology developed to enable a wide range of new IoT devices and services.
NFVi	-	Vulnerabilities related to Network virtualization
OSWAP	-	Open Web Application Security Project
SDN	-	Software driven Network
SIP	-	Session Initiation Protocol
V2N	-	vehicle-to-network
V2V	-	Vehicle-to-vehicle
Xbee	-	It is a family of radio modules and is a registered trademark of Digi International.
Zigbee	-	It is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) network

References

1. https://cfca.org/slug/2021-fraud-loss-survey/
2. https://roaming.kaleidointelligence.com/mobile-operator-losses-from-fraud-and-security-breaches-to-reach-41-billion-in-2024-kaleido-intelligence/

About the Authors

Arvind Balakrishnan

Industry Principal, Infosys Communications, Media Technology Domain Consulting Group

Arvind Balakrishnan is a O/BSS, Digital & Business Assurance practice leader for the Infosys Communications, Media Technology Domain Consulting group. He brings 24+ years of experience in the Communications & Wireless Industry working with leading service providers & OEMs globally.

He can be reached at Arvind_Balakrishnan@infosys.com

Manu Chugh

Industry Principal, in Domain Consulting Group for Telecommunication, Infosys Ltd.

Manu has over 22 years of experience in Telecom & IT industry working with clients across Americas, Europe & APAC. He has helped some of the top CSPs across the globe in executing large scale BSS & Business Assurance programs including integration, transformations, 5G & greenfield implementations.

He can be reached at Manu_Chugh@infosys.com

Jorge Palacios

Lead Consultant in Domain Consulting Group for Telecommunication, Infosys Ltd.

Jorge has 25+ years of experience in Telecom and IT industry working with global communication service providers across North, South & central America, in Business Assurance, and Billing projects.

He can be reached at jorge.palacios@infosys.com

Debi Dalai

Lead Consultant in Domain Consulting Group for Telecommunication, Infosys Ltd.

Debi has more than 14 years of experience in Telecom & IT Industry working with clients across Americas, Europe, Africa & Asia Pacific region. He has served many of the world's leading telcos to implement/migrate Business Assurance solutions.

He can be reached at debi.dalai@infosys.com

Rishi Pal

Consultant in Domain Consulting Group for Telecommunication, Infosys Ltd.

Rishi has over 8 years of experience in the Telecom & IT industry working with clients globally. He has been involved in BSS program implementations for several global service providers. He specializes in the Fraud Management and Revenue Assurance domain and has hands-on experience in business process consulting and analysis.

He can be reached at Rishi.pal@infosys.com

Shilpy Bhomia

Senior Consultant in Domain Consulting Group for Telecommunication, Infosys Ltd.

Shilpy has more than 11 years of experience in Telecom, media, IT Industry working with clients across Americas, Europe & Asia Pacific region. She has expertise in Revenue Assurance and Fraud management domain and currently working on the business process consulting side.

She can be reached at Shilpy.bhomia@infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next