SUBEX

fraud
management

Combating Handset Fraud

Whitepaper

Abstract

Telecom operators have been dealing with declining revenue from traditional services like voice, SMS, and data, forcing them to explore new business avenues like handset/device sales, IoT services, and OTT services. This paper focuses on the sale of handsets/devices, fraud associated with handset sales, and the must-have capabilities in an anti-fraud solution.

Introduction

Global smartphone penetration has significantly grown thanks to 4G. Data from Newzoo shows that the number of global smartphone users has increased by 40% from 2016 to 2020. By the end of 2021, smartphone users are expected to reach about 3.8 billion [1]. The number of devices sold annually in 2010 was 296.65 million, which would rise to 1589.2 million by 2021 [2]. This year, despite the COVID-19 pandemic, the number of handsets shipped is over 275 million [3]. Also, the growing adoption of connectivity, digital applications, and wearable technology is expected to drive growth for players in the 5G devices market, including drones, VRs, gaming consoles, etc.

The meteoric rise in the number of smartphone users should mean increasing revenue for telecom operators because of higher voice, SMS, and data consumption. However, 4G allows over-the-top (OTT) players to challenge the high prices of traditional voice services with free voice/video calling applications, thereby reducing telco's revenues and forcing them to explore other business avenues. While some have partnered with OTT players or launched their own OTT platforms, some operators have also focussed on selling handsets/devices. At present, based on annual reports of various operators in North America and Europe, the device/handset sales contribute between 7-22% revenue for telecom operators in multiple markets.

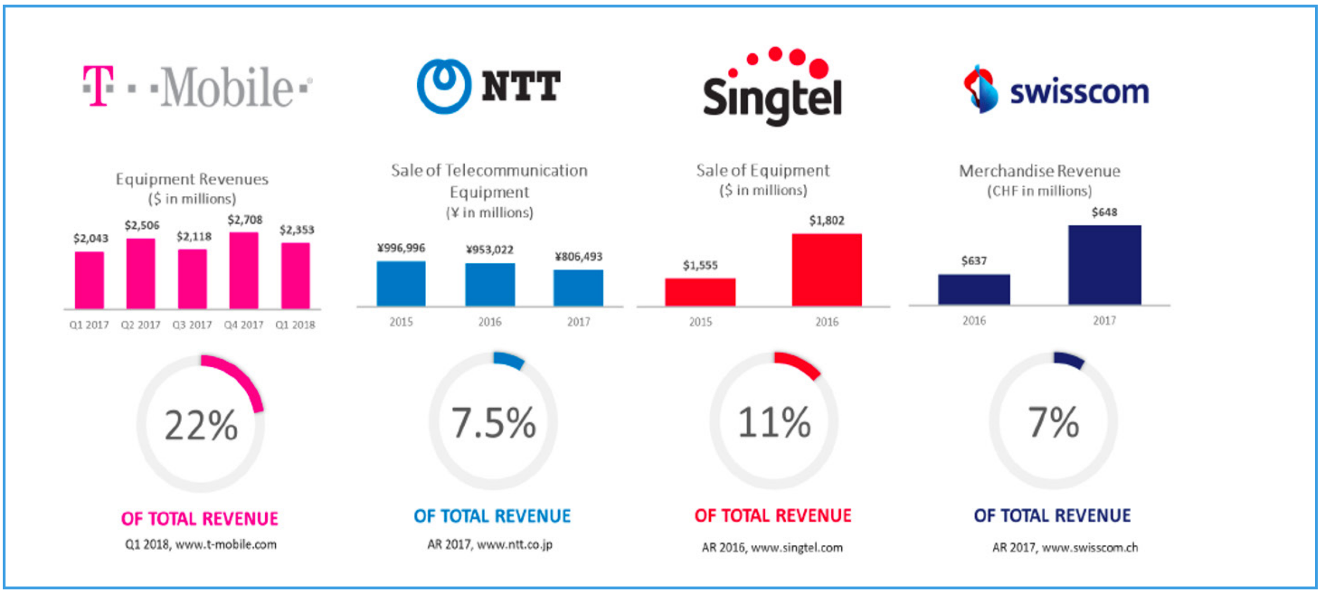


Figure 1: Revenue from device sales across global markets

Brief history of handset sales

Handset sales in the telecommunication industry refers to the selling of mobile phones, fixed-line devices, and routers to retail and enterprise customers. With the advent of smart technologies, it now also includes smartwatches, earphones, and headsets. Hence, it is also referred to as 'device sales' to cover the growing range and diversity of products.

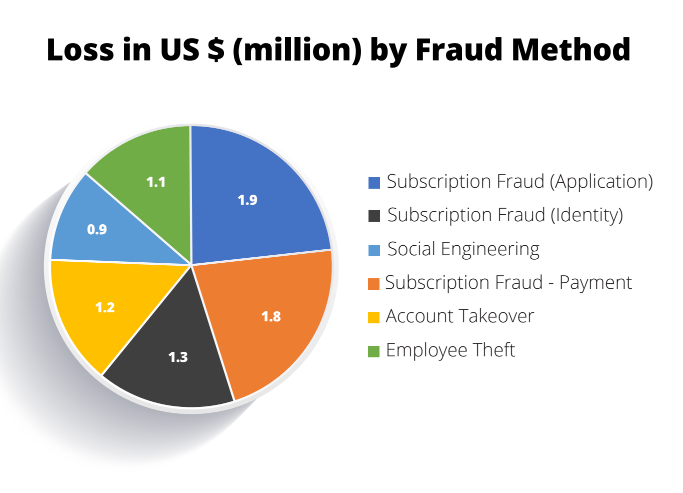
Initially, these devices were sold at discounted prices compared to actual market rates to entice customers to purchase handsets from their operators. Later, monthly contracts emerged whereby customers could pay off the device cost over installments. These flexible payment options were quite attractive. It allowed customers to walk into a store and leave with an expensive high-end phone without any down payment – a facility easily exploited by fraudsters.

Thus, besides increasing operator revenues, device sales have also unfolded opportunities for fraudsters to acquire high-value devices at almost zero price and with no intention to pay. As digital sales channels become popular, users can order a phone via a mobile app or a web-based browser or by calling the customer sales center or through the traditional way of retail point of sale (POS). Each of these sales channels is vulnerable to the risk of fraud.

Handset fraud has caused a significant threat to telecom operators in terms of fraud loss, reputation, and trust. In June 2019, members of a US-based gang were indicted for abetting USD 19 million fraud related to stolen phones and devices. Another case from the UK saw a group of 7 people arrested for being involved in a £2 million mobile phone fraud targeting students. Some operators are forced to write off such losses as bad debt.

Fraud techniques

Fraudsters exploit any loophole within the order booking, management, and delivery systems like inadequate credit vetting, weaker policies, and ineffective verification and validation processes. As seen in Fig 2, data from CFCA 2019 indicates that operators have lost 3.25 billion US Dollars from device theft and fraudulent reselling [4]. Another survey by CFCA on fraud loss highlights that five methods in the top 10 fraud methods are related to handset, device, or payment fraud (see fig 2). Also, the recent RAG RAFM survey reveals that 18.5% of global fraud loss is related to subscription & identify fraud [5]. Furthermore, handset crime accounts for 8.98% of the total fraud loss [5].



Top 10 Fraud Methods:

- $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 Dealer Fraud
- $1.34 B - Subscriber Fraud (Identity)
- $1.25 B - Accound Takeover
- $1.15 B - Internal Fraud/Employee Theft

Figure 2: Revenue losses based on different fraud methods as well as the top 10 fraud techniques

Fraudsters use various tools and techniques to obtain products (handsets/devices) or gain services. Some of the main methods include [4]:

Subscription fraud by identity theft	Subscription fraud by falsifying data	Account takeover	Payment fraud	Credit muling or proxy fraud
where the real identity of a person is obtained through phishing, smishing, etc., and used without their knowledge to buy goods or services with no intention to pay	like ID credentials to purchase handsets/devices without any intention to pay	using genuine customer details that are obtained illegally and used to order handsets/devices	using stolen credit or debit cards or counterfeit cards to purchase handset/devices	whereby a genuine customer colludes with the fraudster to get goods or services without any intention of paying

Identity theft is not just limited only to the telecom space but is also seen in other areas. According to the Insurance Information Institute, there were 3.2 million identity theft cases in 2019. Of these, nearly 1.7 million were fraud-related, and in 23% of these cases, the victims reported losing money. The total fraud loss was about USD 1.9 billion [6].

Control methods

The fraud methods used by fraudsters vary based on the sales channel that the fraudster intends to exploit. Statistics show that fraud on retail POS has reduced over the years, thanks to certain controls.

In general, the control measures should include:

Policy control

These pertain to documents for address proof (like government-issued identity cards), the upper limit of handsets that can be sold to a single customer, frequent upgrades or purchases, etc.

People training

All front-end personnel should be trained in simple yet effective ways of verifying personal identity and payments. This can include checking that photos and date of birth match between the person and the submitted documents, the name in the credit card matches with the ID provided, etc.

Anti-fraud software

Fraud management solutions can avert fraud at POS by thwarting fraudsters with false ID cards or even validating whether the customer has a good credit history.

Key capabilities in anti-fraud software

Digital or web-order sales channels are perhaps the most vulnerable to handset fraud. Thus, any unified software solution aiming to combat handset/device fraud must have, at minimum, the following capabilities:

Data quality

This is the foremost and most basic guardrail needed in any software solution. It includes validating names, postcodes, email addresses, age, credit card numbers, and phone numbers provided as part of the device purchase.

Policy Compliance

All policy controls like upgrades, number of devices per customer, minimal upgrade fees, etc., must be fed into the system and appropriately verified before selling the device.

Rule-based Checks

Appropriate rules must be created and run automatically by the system to monitor fraudulent transactions. These rules should include checks like dedupe controls, velocity checks for high-value handsets, stolen or counterfeit credit cards, ordering after business hours, email ID and geo-IP verification, and tracking suspicious sequences of activities.

Orchestration Capability

To improve efficiency and success rate, the anti-fraud system should have the capacity to integrate with other specific/pointed solutions. Combining the results of two or more solutions makes anti-fraud measures more stringent and highly accurate.

AI/ML Capabilities

Current software systems would not be complete without AI/ML-based capabilities extending into the software suite for device/handset fraud. The AI/ML-based solution should automatically detect patterns and anomalies that cannot be identified manually or through rule-based systems. These AI/ML-based solutions could have one or multiple models to detect various types of fraud methods/types.

Biometrics Verification with Deep Learning

Deep learning algorithm based facial biometrics and document ID processing and verification are particularly useful to verify high-value purchases being made through a mobile app or browser. This can be paired with the rule-based checks mentioned earlier to gauge the applicant's risk score. For POS transactions, scanners can help confirm the authenticity of the ID.

Link Analysis

This data analysis technique identifies and evaluates relationships between various entities in a given dataset. This has two benefits: It can highlight whether new order requests are related to past transactions flagged as fraudulent. It also helps fraud analysts tasked with investigating cases to visualize suspicious relationships between current and past orders.

Response Time

The user experience for any customer purchasing devices online is of the utmost importance to the operator. The typical time from checkout to order confirmation is 10-15 seconds in most e-commerce solutions, giving anti-fraud solutions a mere 2-5 seconds to determine whether the request is genuine.

Integration with Dispatch and Delivery Systems

Anti-fraud solutions should integrate with the operator's delivery system to enable end-to-end device lifecycle management. This will alert operators when the handset has reached its final destination and whether any fraudulent activity has been detected before delivery, allowing them to take appropriate action and stop the delivery.

Conclusion

Telecom operators must protect themselves and their customers from handset fraud through comprehensive fraud management solutions. Subex Fraud Management contains pre-requisite checks across policy control, rule-based detection, AI/ML-based real-time risk scoring, and deep learning algorithm based biometric and document identification. Additionally, FM also provides the orchestration capability providing the option to integrate with other point solutions. We help operators build consolidated, robust, and effective anti-fraud safeguards with automation and real-time decision-making.

References

[1] Sourced from newzoo.com, published in
https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[2] Sourced from gartner.com, published in
https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/

[3] IDC Quarterly Mobile Phone Tracker, Apr 29, 2020, published in
https://www.idc.com/getdoc.jsp?containerId=prUS46264320

[4] CFCA Fraud Loss Survey, 2019

[5] RAG RAFM Survey, 2020

[6] Facts + Statistics: Identity Theft and cybercrime by Insurance Information Institute (IIS).
https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

SUBEX

www.subex.com

About Subex

Subex is a pioneer in enabling Digital Trust for businesses across the globe. Founded in 1994, Subex helps its customers maximise their revenues and profitability. With a legacy of having served the market through world-class solutions for business optimisation and analytics, Subex is now leading the way by enabling all-round Digital Trust in the business ecosystems of its customers. Focusing on risk mitigation, security, predictability and intelligence, Subex helps businesses embrace disruptive changes and succeed with confidence in creating a secure digital world for their customers.

Through HyperSense, an end-to-end augmented analytics platform, Subex empowers communications service providers and enterprise customers to make faster, better decisions by leveraging Artificial Intelligence (AI) analytics across the data value chain. The solution allows users without a knowledge of coding to easily aggregate data from disparate sources, turn data into insights by building, interpreting and tuning AI models, and effortlessly share their findings across the organisation, all on a no-code platform.

Subex also offers scalable Managed Services and Business Consulting services. Subex has more than 300 installations across 90+ countries. For more information, visit **www.subex.com**

Subex Limited

Pritech Park, SEZ Block -09,
4th Floor B Wing
Outer Ring Road
Karnataka, India

Tel: +91 80 37451377
Fax: +91 80 6696 3333

Subex, Inc

12303 Airport Way,
Bldg. 1, Ste. 390,
Broomfield, CO 80021

Tel : +1 303 301 6200
Fax : +1 303 301 6201

Subex (UK) Ltd

1st Floor, Rama
17 St Ann's Road,
Harrow, Middlesex,
HA1 1JU

Tel: +44 0207 8265300
Fax: +44 0207 8265352

Subex (Asia Pacific) Pte. Limited

175A, Bencoolen Street,
#08-03 Burlington Square,
Singapore 189650

Tel: +65 6338 1218
Fax: +65 6338 1216

For more information write to **info@subex.com**

Regional offices: Dubai | Ipswich

Although every endeavour has been made to ensure that the information contained within this document is up to date and accurate, Subex Limited cannot be held responsible for any inaccuracy or error in the information contained within this document. 20052021.