УДК 004.056.5:621.395.3:343.53.003.2
DOI: 10.31673/2412-9070.2022.061720

**V. A. SAHAIDAK**, student;
**M. M. LYSENKO**, applicant;
**O. V. SENKOV**, Candidate of Technical Sciences,
State University of Telecommunications, Kyiv

# TELECOM FRAUD AND IT'S IMPACT ON MOBILE CARRIER BUSINESS

***In this article was described most common types of fraud on mobile network and its impact on carrier business. Most common fraud types were described such as IRSF, wangiri, interconnect bypass fraud, arbitrage, traffic pumping. IRSF takes advantage of premium phone rates, which are then dialed unwittingly by users. Reviewed OTP-based IRSF and wangiri fraud realization. Wangiri is a telephone scam where criminals trick you into calling premium rate numbers. Interconnect bypass fraud takes advantage of something called a termination rate to make cheaper phone calls. VoIP bypass was studied as type of Interconnect bypass fraud. Arbitrage is the general practice of capitalizing on price differences in the long-distance rates between countries. Traffic pumping is a dubious practice by which some local exchange telephone carriers in rural areas of the United States inflate the volume of incoming calls to their networks to profit from the greatly increased inter-carrier compensation fees. Following conclusions were made: Telecom fraud is very complex and variable phenomenon due to carrier network specifics. With new technologies and services delivered on their network telecom operators should adapt their fraud monitoring and analysis methods up to date with minimum delay; In reviewed fraud examples we can see that one fraud activity can use realization technics of several different fraud types. Detection of such activities will require a flexible solution, that can adapt with or without man interaction; Fraud happens, when victim is not expecting it. Fraudsters can make calls, when subscriber is outside of business hours, they can make attempts to multiple subscribers during day and carrier won't notice it until subscriber complain or someone notice strange trend. Scammers can even hack subscriber device or PBX and owner won't even notice it until service payment;***

***Premium or service number can be used by fraudster in order to realize scam. In such case there should be an agreement with carrier and business for list of allowed or blacklisted numbers; Fraud is not limited only to voice services. Realization methods can be used to SMS or IP network services.***

**Keywords:** CFCA; IRSF; Wangiri; Interconnect bypass fraud; Arbitrage; Traffic pumping.

### *Introduction*

What is telecom fraud? The GSMA defines telecommunications fraud as something that is perpetrated where process, control or technical weaknesses are intentionally exploited, resulting in a financial or other loss. The GSMA acknowledges that the term 'fraud' is defined in many national legal frameworks, and operators may use different definitions within their own businesses and countries. The perpetrators can either steal telecommunication services or misuse them to incur losses or defraud innocent subscribers into incurring huge bills or stealing private data.

In 2019-year, Communications Fraud Control Association (CFCA) have published a survey and study. Following survey showed that the global telecom fraud loss was estimated at $28.3 Billion (USD). It was to 1.74% of the 2019 estimated global telecom revenues, with the top 5 fraud types accounting for 54% of all fraud losses. This was an increase from the 2017 figures of 1.27% loss of global telecom revenues. 89% of surveyed operators reported that fraud losses had increased or stayed the same within their own companies, however many companies are now reporting far fewer cases to law enforcement.

How usually fraud impacts mobile carrier except revenue loss? It damages brand and reputation, increases spending on customer service, requires time and manpower to repair damage.

How fraud impacts consumer? It causes loss of money, loss of personal data and repercussion from it, requires time to spent on data recover due to inaccurate billing, loss of trust.

### *The main part*

According to CSFA report most common fraud types with biggest revenue lost are International Revenue Share Fraud (IRSF), Arbitrage, Interconnect Bypass (e.g. SIM Box), Domestic Premium Rate Service (In Country), Traffic Pumping (includes: Domestic Revenue Share, TFTP).

**IRSF** fraud, takes advantage of premium phone rates, which are then dialed unwittingly by users. It can be realized by several ways:

- bad agents sign up to lease a premium phone number.
- fraudster break into a business's phone systems and make calls to that number (PBX – Private branch exchange hacking).
- fraudsters use hacked phones or stolen device/SIM card.

The calls often happen outside of working hours and companies only realize they've been made when it's time to foot the bill. Many attackers opt for low-and-slow attacks to bypass the attack identification rules.

Businesses also lack visibility into downstream activities, which prevents them from arresting IRSF early in its tracks. Let's have a look on two examples of such IRSF fraud like OTP-based on fig. 1 and Wangiri on fig. 2.

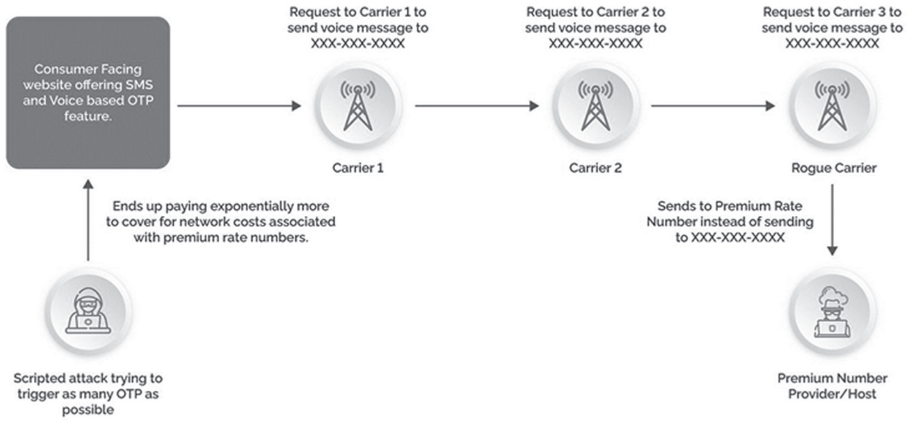
Consumer Facing website offering SMS and Voice based OTP feature.
Request to Carrier 1 to send voice message to XXX-XXX-XXXX
Carrier 1
Request to Carrier 2 to send voice message to XXX-XXX-XXXX
Carrier 2
Request to Carrier 3 to send voice message to XXX-XXX-XXXX
Rogue Carrier
Ends up paying exponentially more to cover for network costs associated with premium rate numbers.
Sends to Premium Rate Number instead of sending to XXX-XXX-XXXX
Scripted attack trying to trigger as many OTP as possible
Premium Number Provider/Host

**Fig. 1. OTP-based IRSF**

The steps of an OTP-based IRSF are:

1. An attacker initiates a manual or a scripted attack on a webpage to trigger voice- or SMS-based OTPs. Depending on the returns, attackers can opt for high-volume attacks or low-and-slow attacks.

2. The consumer-facing business forwards the OTP request to a cloud communication provider.

3. The provider forwards the request to a carrier. This request is necessary as multiple network providers in the region are involved before the OTP can reach the intended consumer.

4. A compromised carrier, colluding with an attacker, forwards the request to an IPR number instead of the intended recipient.

5. «Terminating» a call on an IPR number is expensive; and ultimately it is the consumer-facing business that must absorb the losses.

6. Attackers earn huge profits from their share of the fraud, usually $1 or more per transaction.

**Wangiri** is a Japanese word meaning 'one (ring) and cut'. It's a telephone scam where criminals trick you into calling premium rate numbers. A fraudster will set up a system (for instance using botnets) to dial a large number of random phone numbers. Each calls rings just once, then hangs up, leaving a missed call on the recipients' phone. Users often see the missed call and, believing it was a legitimate call, call back the missed number. An SMS variant of this also exists, where fraudsters send a message prompting customers to call back a certain number, or even text it. The typical red flags for this kind of telecommunications fraud are spikes in traffic to high-cost destinations, which telcos should be able to monitor with their internal system. The key here is to know that, as a business, you should keep an eye on which numbers are automatically dialed.

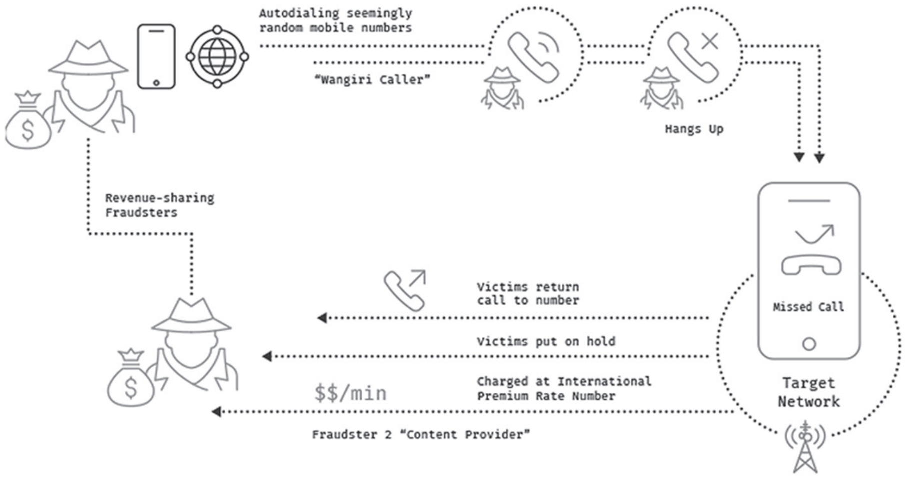
Autodialing seemingly random mobile numbers
"Wangiri Caller"
Hangs Up
Revenue-sharing Fraudsters
Missed Call
Target Network
Victims return call to number
Victims put on hold
$$/min
Charged at International Premium Rate Number
Fraudster 2 "Content Provider"

**Fig. 2. Wangiri**

**Interconnect bypass fraud**, also known as SIM box fraud, takes advantage of something called a termination rate to make cheaper phone calls. To understand it, let's look at a scenario with two operators in different countries:

1. A customer of Operator A calls a customer of Operator B.
2. Operator A charges its customer a fee per minute.
3. Operator B charges Operator A fee for providing the call to its customer.

That last charge, where the call terminates, is the termination rate. These rates vary wildly depending on the contracts between the two operators. Some of them are expensive, others are close to 0. This is where a fraudulent operator comes into the picture. They reroute these international calls using a SIM box or GSM gateway, effectively hijacking the connection to achieve cheaper termination rates. They are essentially making long-distance calls much cheaper, but the caller pays the same price – so the fraudster telco pockets the difference. This also impacts telecom customer satisfaction because more often than not, the quality of these calls will be inferior to standard international calls. On fig. 3 we can see an example of VoIP bypass fraud, where call is routed on internet instead of agreed telecom carrier routes.

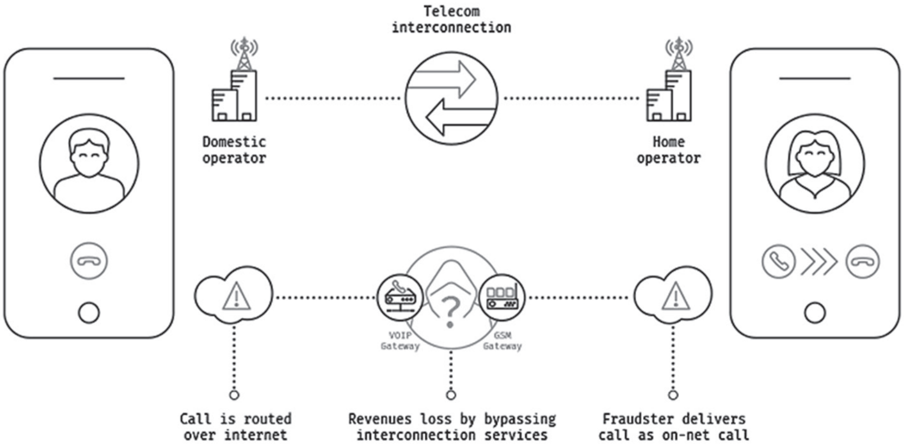
Telecom interconnection
Domestic operator
Home operator
VOIP Gateway
GSM Gateway
Call is routed over internet
Revenues loss by bypassing interconnection services
Fraudster delivers call as on-net call

**Fig. 3. VoIP bypass fraud**

**Arbitrage** is the general practice of capitalizing on price differences. In the telco world, these differences appear in the long-distance rates between countries. Just like with international bypass fraud, it can lower the international cost for customers, but also open the door to fraudulent companies who insert themselves between operators. They claim to connect directly from country A to B, whereas, in fact, they go through a cheaper rate country to connect the call.

**Traffic pumping**, also known as access stimulation, is a dubious practice by which some local exchange telephone carriers in rural areas of the United States inflate the volume of incoming calls to their networks to profit from the greatly increased inter-carrier compensation fees. In order to spur competition for Incumbent Local Exchange Carriers (ILECs), the FCC allows rural Competitive Local Exchange Carriers (CLECs) and Incumbent Local Exchange Carriers (ILECs) to charge high terminating access charges for completing calls they accept from Inter-Exchange Carriers (IXCs).

### *Conclusions*

1. Telecom fraud is very complex and variable phenomenon due to carrier network specifics. With new technologies and services delivered on their network telecom operators should adapt their fraud monitoring and analysis methods up to date with minimum delay.
2. In reviewed fraud examples we can see that one fraud activity can use realization technics of several different fraud types. Detection of such activities will require a flexible solution, that can adapt with or without man interaction.
3. Fraud happens, when victim is not expecting it. Fraudsters can make calls, when subscriber is outside of business hours, they can make attempts to multiple subscribers during day and carrier won't notice it until subscriber complain or someone notice strange trend. Scammers can even hack subscriber device or PBX and owner won't even notice it until service payment.
4. Premium or service number can be used by fraudster in order to realize scam. In such case there should be an agreement with carrier and business for list of allowed or blacklisted numbers.
5. Fraud is not limited only to voice services. Realization methods can be used to SMS or IP network services.

### *References*

*1. **Understanding** international telecoms fraud // BICS [Електронний ресурс]. URL: https://www.bics.com/wp-content/uploads/2022/02/Telco-Fraud-Whitepaper.pdf*

*2. **Putting** telecom fraud loss into perspective... // CFCA [Електронний ресурс]. URL:*
*https://cfca.org/putting-telecom-fraud-loss-into-perspective/*

*3. **Telecommunications** Fraud // EUROPOL [Електронний ресурс]. URL:*
*https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/telecommunications-fraud*

*4. **11 Types** of Telecommunications Fraud: How to Detect & Prevent It // SEON [Електронний ресурс]. URL:*
*https://seon.io/resources/telecommunications-fraud-detection-and-prevention/*

*5. **Telecom** Wholesale Fraud // Mobileum [Електронний ресурс]. URL:*
*https://www.mobileum.com/products/risk-management/fraud-management/telecom-wholesale-fraud/*

*6. **International** Revenue Share Fraud (IRSF): What it is and How to Stop it // Arkose Labs [Електронний ресурс]. URL:*
*https://www.arkoselabs.com/explained/international-revenue-share-fraud/*

*7. **Telecom** Wholesale Fraud // Mobileum [Електронний ресурс]. URL:*
*https://www.mobileum.com/products/risk-management/fraud-management/bypass-fraud/*

*8. **Telecom** Wholesale Fraud // Mobileum [Електронний ресурс]. URL:*
*https://www.mobileum.com/products/risk-management/fraud-management/revenue-share-fraud/*

*В. А. Сагайдак, М. М. Лисенко, О. В. Сеньков*

## ШАХРАЙСТВО У СФЕРІ ТЕЛЕКОМУНІКАЦІЙ ТА ЙОГО ВПЛИВ НА БІЗНЕС ОПЕРАТОРІВ ЗВ'ЯЗКУ

*Наведено опис найбільш відомих видів шахрайства в мобільній мережі та їх вплив на бізнес операторів телекомунікацій. Описано найпоширеніші типи шахрайства, такі як IRSF, wangiri, interconnect bypass fraud, arbitrage, traffic pumping. В IRSF використовуються преміальні телефонні номери, які потім мимоволі набирають користувачі. Переглянуто реалізацію шахрайства на основі OTP та wangiri. Wangiri — це телефонне шахрайство, в якому зловмисники обманом змушують вас дзвонити на преміальні номери. Interconnect bypass fraud використовує різницю цін на з'єднання, щоб зробити телефонні дзвінки більш дешевшими. VoIP bypass було досліджено як тип Interconnect bypass fraud. Arbitrage — це загальна практика отримання прибутку від різниці тарифікації відстані між країнами. Traffic pumping є сумнівною практикою, за допомогою якої деякі місцеві мобільні оператори в сільській місцевості Сполучених Штатів збільшують обсяг вхідних дзвінків до своїх мереж, щоб отримати прибуток від значно збільшених компенсаційних комісій між операторами. Було зроблено такі висновки: телекомунікаційне шахрайство є дуже складним і мінливим явищем через специфіку мережі оператора. Завдяки новим технологіям і послугам, які надаються в їхніх мережах, оператори зв'язку мають адаптувати свої методи моніторингу та аналізу шахрайства з мінімальною затримкою; у розглянутих прикладах шахрайства ми бачимо, що одна шахрайська діяльність може використовувати технології реалізації кількох різних типів шахрайства. Виявлення таких дій вимагатиме гнучкого рішення, яке може адаптуватися з або без взаємодії людини; шахрайство відбувається тоді, коли жертва цього не очікує. Шахраї можуть здійснювати дзвінки за межами робочих годин абонента або дзвонити кільком абонентам протягом дня і мобільний оператор не помітить цього, доки абонент не поскаржиться чи хтось помітить дивну тенденцію. Аферисти також можуть зламувати абонентський пристрій або АТС, що абонент теж не помітить, доки не отримує рахунок за використані послуги; преміальний або сервісний номер може бути використаний шахраєм для здійснення афери. У такому разі має бути угода з оператором і компанією щодо списку дозволених чи заборонених номерів; шахрайство не обмежується лише голосовими послугами. Методи реалізації можна використовувати для мережних послуг SMS або IP.*

**Ключові слова:** CFCA; IRSF; Wangiri; Interconnect bypass fraud; Arbitrage; Traffic pumping.