NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

Wangiri Scam: Challenges, Safeguards, Prevention and Mitigation

Naveen Kumar Chaudhary[1]
(Corresponding Author)
[1]National Forensic Sciences University (NFSU), Gandhinagar Campus, Gandhinagar, Gujarat, India
naveen.chaudhary@nfsu.ac.in

S. S. Iyenagar[2]
[2]Florida International University (FIU), Miami, Florida, United States of America
iyengar@fiu.edu

Sandeep Munjal[1, 3]
[1]National Forensic Sciences University (NFSU), Gandhinagar Campus, Gandhinagar, Gujarat, India
[3]National Forensic Sciences University (NFSU), Goa Campus, Goa, India
sandeep.munjal@nfsu.ac.in

***Abstract*—Fraud in the telecommunications sector, commonly termed telecom fraud, now poses a serious problem for enterprises, subscribers and network operators across the globe. As connectivity has improved with the progress of telecommunication technology, those behind such frauds have devised ever more elaborate techniques to exploit their targets for financial benefit. The present work takes a closer look at one particular variant of these schemes, the Wangiri scam, examining how it is carried out, the extent and seriousness of the problem, the obstacles to countering it, and the protective measures available against such telecom frauds.**

Keywords*— *telecommunication, fraud, scam, Wangiri, law enforcement

I. INTRODUCTION

Telecom connectivity has grown considerably, driven by the build-out of infrastructure and a growing dependence on communication technologies. Such growth has widened the opportunities for fraudsters who can exploit the same telecommunication infrastructure to reach victims via sophisticated schemes. Today's telecommunication networks are a mix of different technologies, many service providers, roaming arrangements and cross-border service agreements and these have created a huge number of gaps that can be exploited by fraudsters [1]. Telecommunication fraud is any unlawful act that uses telecom services, devices or networks to cheat an individual, organisation or service provider. Such frauds cover a wide spectrum from identity theft and call-forwarding to more sophisticated frauds like VoIP hacking and subscription fraud. These scams are sophisticated and difficult to combat: they take advantage of technical loopholes and human mistakes in many cases. A fraudster might pose as a telecom company and coax victims into disclosing personal information or paying money into fake accounts. Or they may compromise the network or systems of a telecommunication company to route calls and steal data. The fact that there are so many different ways to commit telecom fraud means that it is a recurring problem that affects operators and subscribers severely and it is a huge problem [2]. One such scam, Wangiri, has come to the attention of law enforcement officials in recent years. It's a call-back scam that derives its name from a Japanese term that means 'one ring and cut', a phrase which describes exactly how the fraud works. The term wan means 'one' and giri means 'cut' in Japanese, and operators have

been dealing with this type of fraud since 2009 - the first reported incidents occurred in Japan [3]. It has spread to many countries around the world. In a Wangiri scheme, the fraudster sends a missed call to many victims from a target list, usually using an international or otherwise unknown number. The caller line identification (CLI) is often spoofed to make the caller seem legitimate. If the victim returns the call, the victim may be charged a high per-minute rate because the number is generally linked to a premium-rate service (PRS) number [5]. The goal is to keep the victim on the line as long as possible, so that the bill grows. So the calls play back recorded messages or automated prompts that keep the victim waiting until the call ends and the victim pays the associated charges. For every minute the victim remains connected to the premium-rate service, the fraudster may receive a portion of the call revenue through the revenue-sharing arrangement. Wangiri fraud would be the fraudulent inducement of a subscriber to return a missed call, resulting in charges to the subscriber and potentially revenue to the fraudster [6]. Operators may have to bear both the direct and indirect losses as a result. Subscribers are also hit hard: bill shocks and poor experience cause customer churn. The operator's reputation suffers too, since customers object to being charged premium rates without any prior awareness. Though it looks straightforward to carry out, the scam remains a highly effective attack vector owing to its reliance on psychological manipulation [7]. Recent industry estimates indicate that Wangiri places a heavy load on the telecom sector, with worldwide losses running to more than 40 billion dollars each year [8].

II. STAGES OF WANGIRI SCAM

Wangiri scam comprises of a three-stage process as shown in figure 1. It involves call initiation by the fraudster, the calling back by the victim, and incurring of call charges.

A. Call Initiation

The first stage of the scam begins with the fraudsters using an auto-diallers to call a large number of phone numbers across different regions from the target list. As an alternative trigger for call-back, bulk SMS can also be used, prompting the recipients to dial an unknown number. These calls rings once and then disconnect. This single ring is intended to alert the recipient to notice a missed call from the fraudster number.

B. Call-back

The recipient may call back, without realizing that the number is linked to a premium-rate number that charges exorbitant fees per minute. Once the victim calls back, the fraudster tactics is to keep the victim on line as long as possible.

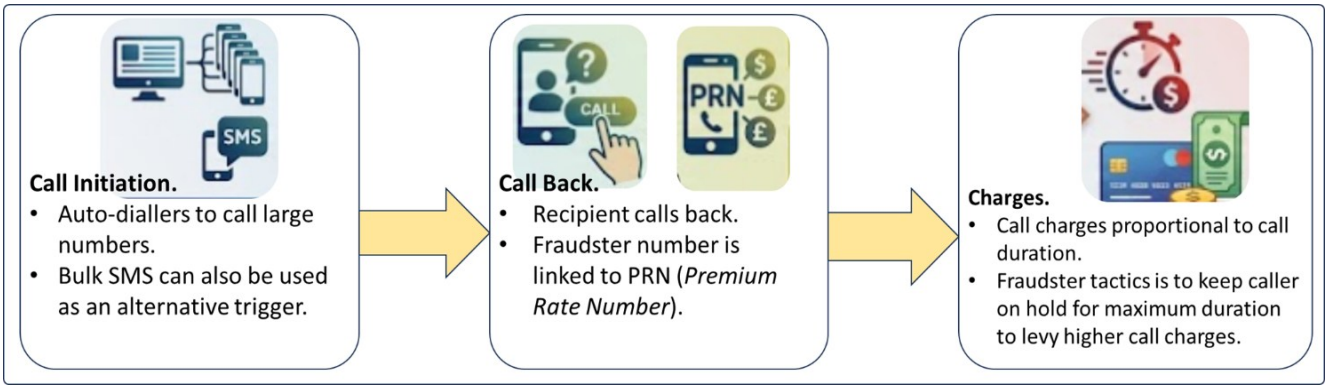


Fig. 1. Three stage process of Wangiri Call.

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

A pre-recorded message or call holding music is played to give the impression that the call will be connected soon.

C. Charges

The call charges are proportional to the call duration so longer the call duration the higher charges the victim will accrue. These charges benefit the scammers who in share the revenue with the telecom operators that host the premium-rate numbers. The call usually ends when the victim realises the nature of the scam and terminates the call or runs out of credit limit if they are using a prepaid phone service. The 03-stage process of Wangiri call is depicted in Figure 1.

III. CHALLENGES IN COMBATING WANGIRI SCAM

Wangiri fraud presents unique-challenges arising from its cross border nature and the rapid pace of the technological advancement. Large volume of brief call attempts across international networks creates significant difficulties in detection. Traditional rule based systems often becomes ineffective in providing preventive safeguards [9,10].

- One of the key challenges is difficulty of tracking and prosecuting criminals, who frequently operate outside national jurisdictions.
- International collaboration becomes essential, but is often hindered by the differing legal frameworks and uncoordinated mechanisms for the information exchange and co-operation among law enforcement agencies (LEAs).
- A second major challenge is the speed, at which fraudsters adapt to the different counter measures. They continually modify their tactics in order to evade the conventional detection mechanisms. For example, they adjust duration, and the frequency of call(s) in order to avoid triggering alarm(s), configured by telecom operators to prevent such offences.
- Further, the limited subscriber awareness also remains a critical vulnerability. Despite of several efforts to educate the users about these Wangiri scams, many individuals remain unaware of risks associated with the returning missed calls from unknown international numbers. Hence, this lack of awareness is exploited routinely for the successful scam execution.
- Telecom providers must also balance the fraud prevention with the service accessibility. Aggressive blocking of suspected Wangiri calls may result in "false positives" also, leading to inadvertent blocking of the legitimate calls/numbers, thereby causing dissatisfaction of the subscriber(s), and potentially damaging service provider and subscriber relationships.

Wangiri fraud imposes substantial financial burdens on telecom-operators. These include not only the direct losses associated with scam, but also significant investments are also required for the deployment and the maintenance of fraud detection and prevention systems.

IV. SAFEGUARDS, PREVENTION AND MITIGATION

Telecom companies inadvertently play a role in the operation of Wangiri scams. They provide the infrastructure that allows calls to be made as well as received internationally. Some telecom operators may also host the premium-rate numbers (PRNs) used by the scammers. While these telecom companies are not directly responsible for the scam, but their networks are exploited to facilitate it. To combat this, telecom companies need to adhere to the following safeguard measures: -

A. Monitoring and Blocking

- Use of cross-validation technology to safeguard against the Wangiri calls.
- Integration of AI and analytics to monitor call patterns.
- Blocking of calls linked to Wangiri scams.

B. Customer Alerts

- Monitoring of incoming calls from the high-risk countries.
- Mechanism for detection of short or unanswered calls.
- Subscribers should be informed about potential scams.

C. International Cooperation

- Sharing of information on Wangiri operations by telecom bodies.

- Develop strategies and share the best practices to counter Wangiri scam.
- Regulatory bodies to block verified Wangiri calls.

A three-stage framework to combat Wangiri scam calls is depicted in Figure 2.

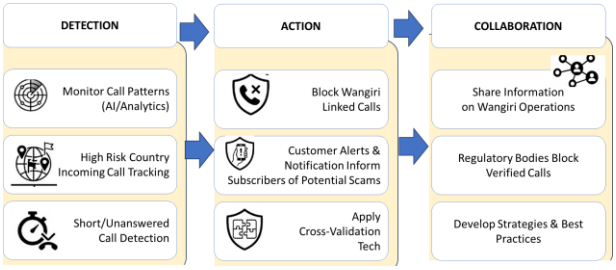


Fig. 2. A three-stage framework to combat Wangiri scam calls.

V. CONCLUSION

The Wangiri scam, as an ever evolving global threat, requires an integrated as well as adaptable approach to prevent and mitigate such frauds. Strategies to counter Wangiri must operate from a global perspective, and incorporate advanced technological measures, while the widespread awareness among telecom subscribers must also form part of the solution. The Wangiri scam is not particularly confined to any specific regions; rather, it represents a global challenge that necessitates coordinated international cooperation. A harmonized legislative framework is required to ensure that the relevant authorities can share information effectively and conduct time bound law enforcement actions, enabling efficient cross-border investigations.

Integration of advanced analytics and artificial intelligence (AI) significantly enhances the capability to detect and to monitor fraudulent activities. The emergence of "Wangiri 2.0" has introduced additional operational complexity. This variant employs automated bots, to generate call backs by disseminating telephone numbers online, after which call centres exploit the resulting traffic using strategies similar to original Wangiri scam. In order to effectively counter Wangiri, sustained awareness campaigns must be conducted to educate the subscribers about the fraudsters' modus operandi, and evolving tactics. Telecom operators must also allocate sufficient resources toward implementing robust security controls and compliant fraud management systems to safeguard subscribers against Wangiri-related threats.

REFERENCES

[1] A. Ravi, M. Msahli, H. Qiu, G. Memmi, A. Bifet, and M. Qiu, "Wangiri Fraud: Pattern Analysis and Machine-Learning-Based Detection," IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6794–6802, 2023, doi: 10.1109/JIOT.2022.3174143.

[2] Balouchi, A., Abdollahi, M., Eskandarian, A., Karimi Pour Kerman, K., Majd, E., Azouji, N., & Baniasadi, A. "Wangiri Fraud Detection: A Comprehensive Approach to Unlabeled Telecom Data". Future Internet, 18(1):15, 2026. https://doi.org/10.3390/fi18010015.

[3] ITU Report. Technical report ITU-T TR. MMWF (02/2025) - Methodologies to Mitigate Wangiri Fraud. Available at https://www.itu.int/epublications/ru/publication/itu-t-tr-mmwf-2025-02-methodologies-to-mitigate-wangiri-fraud. (Accessed on 24 Feb 2026).

[4] Ye, N., Cheng, L., & Zhao, Y. "Identity construction of suspects in telecom and internet fraud discourse: from a sociosemiotic perspective". Social Semiotics, 29(3), 319–335, 2019. https://doi.org/10.1080/10350330.2019.1587847.

[5] Zoldi, S, "Using anti-fraud technology to improve the customer experience". Computer Fraud Security. Vol. 2015, pg. 18–20. https://doi.org/10.1016/s1361-3723(15)30067-1.

[6] Tarmazakov E.I., and Silnov, D.S, "Modern approaches to prevent fraud in mobile communications networks". IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, pp. 379–381, 2018 https://doi.org/10.1109/EIConRus.2018.831711120.

[7] Hu, X.; Chen, H.; Chen, H.; Zhang, S.; Liu, S.; Li, X. "Telecom fraud detection via imbalanced graph learning". IEEE 22nd International Conference on Communication Technology (ICCT), Nanjing, China, 11–14 November 2022.

[8] Taylor, L. Telecoms Fraud Costing Operators $40 Billion Annually. Capacity Media. 2023. Available online: https://cfca.org/telecommunications-fraud-increased-12-in-2023-equating-to-an-estimated-38-95-billion-lost-to-fraud/ (accessed on 21December 2025).

[9] Mawgoud, A.A.; Abu-Talleb, A.; Tawfik, B.S. A Holistic Neural Networks Classification for Wangiri Fraud Detection in Telecommunications Regulatory Authorities. In International Conference on Advanced Machine Learning Technologies and Applications; Springer: Berlin/Heidelberg, Germany, 2021; pp. 175–183.

[10] M. Arafat, A. Qusef and G. Sammour, "Detection of Wangiri Telecommunication Fraud Using Ensemble Learning," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2019, pp. 330-335, doi: 10.1109/JEEIT.2019.8717528.