Analysis Of Policies For Handling And Preventing Fraud In International Terminated Traffic

Rio Triawan[1], **Dadang Gunawan**[2]
[1,2]*Department of Electrical Engineering, Universitas Indonesia,*
Depok, West Java 16424, Indonesia
email: [1*]*rio.triawan@gmail.com,* [2]*guna@eng.ui.ac.id*

ARTICLE INFORMATION

Received 20 May 2025
Revised 09 October 2025
Accepted 01 December 2025

Keywords:
International Call Fraud
RIA Method
SIMBOX
Telecommunication Fraud
Telecommunication Policy

ABSTRACT

Fraud in international telecommunications traffic is a serious challenge in Indonesia's telecommunications industry. Practices such as interconnect bypass and CLI spoofing not only cause losses to operators but also threaten national security and public trust. This research aims to analyze Indonesia's current policies for combating fraud in international trade and to identify alternative policies that are more effective and adaptable. The research uses a limited Regulatory Impact Analysis (RIA) approach that covers only the problem definition stage and the formulation of policy alternatives. Data was collected through test calls by the Ministry of Communications and Digital of the Republic of Indonesia (May 2023-October 2024), literature and regulatory studies, and relevant secondary data. The results show that the existing policies still have significant loopholes in the practice of international termination traffic fraud. This research proposes several technical and regulatory policy alternatives that can be used as the basis for further policy development by regulators.

1. Introduction

Indonesia's telecommunications industry has experienced rapid growth in recent decades. However, along with this growth, new challenges have emerged in the form of increasing cases of fraud in international termination traffic. International calls that are supposed to go through official channels are often manipulated through techniques such as interconnect bypass, SIMBOX use, or spoofing to be charged at local rates. Fraud is committed by disguising international calls as local calls, taking advantage of loopholes in technical systems and regulatory weaknesses.

This results in significant financial losses for operators due to loss of revenue from legitimate interconnection rates, the public becoming victims of fraud that is difficult to trace due to the disguised identity of the caller, as well as complicating law enforcement in cases of cross-border fraud. The current policy does not comprehensively regulate all technical and operational aspects of fraud prevention, especially for non-Internet Telephony for Public Purposes (ITKP) service providers such as cellular operators and International Direct Connection (SLI) service providers. This opens a gap for perpetrators to continue to take advantage of system weaknesses.

The main problem in this context is the lack of optimal policies governing fraud prevention and handling mechanisms in international termination traffic. Existing regulations only regulate some service providers, such as ITKP, and do not cover SLI services, considering that fraud potential does not only come from ITKP lines but also from SLI lines. Current policies have not been able to significantly reduce fraud rates despite blocking efforts. Data from the Ministry of Communications and Digital of the Republic of Indonesia shows that while fraud rates dropped to around 7–10% by the end of 2023, they rose sharply in 2024, reaching over 40% in some months.

10.17933/bpostel.v23i2.414

This study aims to analyze the prevailing policies in handling international termination traffic fraud in Indonesia and identify various technical and regulatory policy alternatives that can be offered as solutions. This research focuses on the initial stages of the Regulatory Impact Analysis (RIA) approach, namely problem definition and policy alternative formulation, without involving a stakeholder consultation process or quantitative policy impact evaluation.

The research gap lies in the lack of studies that systematically examine telecommunications fraud from a public policy aspect. Most previous studies only focused on the technical aspects of fraud detection or partial evaluation of the impact of SIMBOX. There is no comprehensive approach that combines technical data with a policy analysis framework such as RIA.

The main contribution of this research is to provide a systematic mapping of the weaknesses of existing regulations and develop alternative technical policies that can be the basis for further policy formulation by the government. This research is expected to strengthen the basis for evidence-based policy-making in the context of tackling international termination traffic fraud.

2. Literature review

2.1. *International Terminated Traffic*

International termination traffic refers to the process of completing calls, messages, or data from one country to another that is handled by an operator in the destination country. This process can be done through a fixed line or an internet protocol-based network (VoIP). In Indonesia, international termination through a fixed network is carried out by the fixed network operator of international connections through the International Direct Connection (SLI) service, while internet-based termination is organized by the Internet Telephony for Public Purposes (ITKP) service provider. These two types of services have different regulations and business models, but both are targets for exploitation by fraudsters.

2.2. *Implementation of International Termination Services*

The implementation of international fixed-line networks is carried out by operators who have official licenses and build Central International Gateways (SGI) as entry and exit points for intercountry traffic (*Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 Tentang Penyelenggaraan Telekomunikasi, 2021*). In Indonesia, only two major operators have SGIs for SLI services, namely Telkom and Indosat. Meanwhile, ITKP services provide Internet Protocol (IP)-based international connections and must use an authorized access code for each call (*Peraturan Menteri Komunikasi dan Informatika Nomor 13 Tahun 2019 Tentang Penyelenggaraan Jasa Telekomunikasi, 2019*). Although both are regulated by the government, there are still loopholes that fraudsters exploit, especially through illegal routes.

2.3. *International Terminated Traffic Business Model*

In general, there are three main business models in international termination traffic services: (1) Direct Termination, which is a direct cooperation between operators without a third party, which guarantees better quality and security but requires infrastructure and bilateral agreements; (2) Wholesale Termination, which uses transit providers and risks degrading service quality if using non-optimal routes; and (3) Gray Route Termination, which is an illegal or unauthorized route that avoids authorized termination fees, usually using SIMBOX or line manipulation. These gray routes harm authorized operators, degrade service quality, and violate regulations.

This gray route model is the main source of fraud in international terminated traffic, as it avoids legal rates and passes through paths that cannot be accurately tracked. This loophole is often exploited by perpetrators to disguise the origin of international traffic as local traffic, causing potential revenue loss and disrupting surveillance systems.

2.4. *Telecommunication Fraud*

Telecommunications fraud is one of the most serious threats in the telecommunications sector, as it can cause financial losses and reputational damage to both operators and customers. It refers to the misuse of telecommunications service products (especially telephone and mobile services) with the aim of illegally profiting from telecommunications service providers or their customers (Europol, 2021). Fraud in telecommunications services is an act or activity of unauthorized (illegal) and intentional use of telecommunications services through telecommunications technology such as wireline telephones, cellular telephones, computer networks, and other technology products (Hanrui Gong, 2022). The forms vary, ranging from bill manipulation to interconnection bypass to sophisticated exploitation of technical systems.

According to the Global System for Mobile Communications Association (GSMA), telecommunications fraud occurs when someone intentionally exploits process, control, or technology weaknesses in telecommunications systems to cause financial or operational losses. The CFCA (Communication Fraud Control Association) also notes that this fraud is classified based on the perpetrator's method of accessing the network and the type of strategy used to gain an advantage. Common forms include interconnect bypass, IRSF (International Revenue Share Fraud), SIMBOX, and CLI spoofing.

Telecommunications fraud falls under the category of transnational cybercrime and requires special attention from regulators. Because its impact can reach all stakeholders, from customers, operators, to the government, addressing fraud requires a strong and data-driven technical policy framework. Previous studies have focused on the technical aspects, while the public policy dimension has not been discussed in depth.

2.5. *Types of Fraud in Telecommunication Services*

Fraud in telecommunications services can occur in various forms and methods, most of which exploit loopholes in network systems and rate regulations. Some common types of fraud include:

a. International Revenue Sharing Fraud (IRSF): occurs when the fraudsters illegally accesses premium rate services, usually through hacking a company's SIM card or PABX, and makes a profit from the premium rate revenue sharing scheme. Figure 1 illustrates the IRSF fraud process.

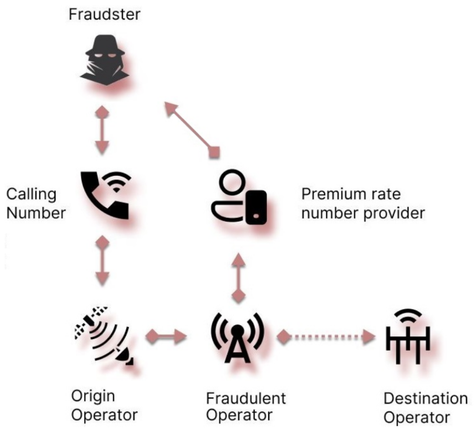

Figure 1. IRSF Fraud Process (B. A. Yehya, 2023)

b. Interconnect Bypass: involves diverting international traffic using devices such as SIMBOX or PABX devices, so that international calls appear as local calls to avoid authorized rates. The Interconnect Bypass fraud process can be seen in Figure 2.

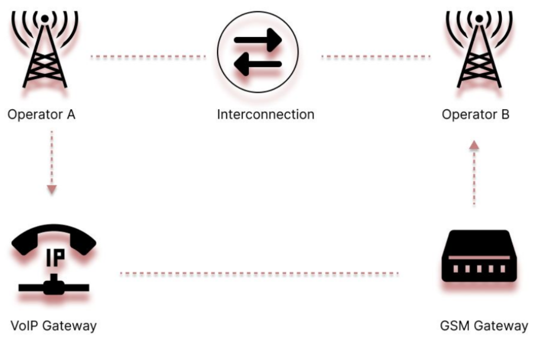

Figure 2. Interconnect Bypass Fraud Process (B. A. Yehya, 2023)

c. Calling Line Identification (CLI) Spoofing: this fraud is done by manipulating the caller number by hiding the real identity of the caller number. This call aims to scam, fraud, obtain personal information such as passwords, bank account information, and other data for personal gain.
d. Wangiri Fraud: a scheme where the perpetrator makes a short call (one ring) in the hope that the recipient will call back to a premium number, resulting in a large bill to the victim. Figure 3 illustrates the Wangiri Fraud process.

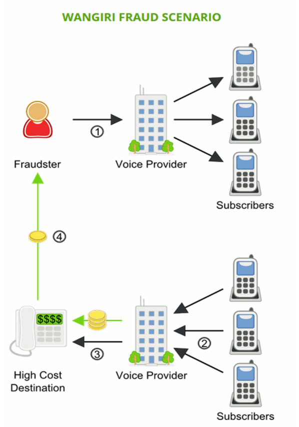

Figure 3. Wangiri Fraud Process (M. Lacuska, 2021)

e. Arbitrage Fraud: taking advantage of rate differences between countries or carriers. Calls are routed through lower-rate countries using local SIM cards or virtual numbers to reduce costs and make a profit.

2.6. *Fraud Detection Methods*

Telecom fraud detection is essential to prevent financial losses, protect customers, and maintain service quality. Operators use various methods to detect anomalous patterns in traffic. Some of the main methods include:

a. Call Detail Record (CDR) Analysis
This method performs metadata analysis of each communication transaction such as number, duration, time, and location. CDR enables identification of normal user profiles and detects suspicious patterns, such as usage by SIMBOX (B. A. Yehya, 2023).
b. Pattern Recognition
It uses statistical techniques to recognize unusual communication patterns based on the duration, purpose, and frequency of calls (B. Jendruszak, 2025).

c. Real-Time Monitoring
Monitor traffic live and automatically to detect and respond to fraud quickly. This technology is often combined with machine learning algorithms to improve accuracy.

d. Rule-Based Systems
This system works with IF-THEN logic rules based on historical fraud patterns. It is used to filter traffic and flag potential fraud based on discrepancies with normal patterns.

e. Machine Learning Algorithms
This method utilizes artificial intelligence to study traffic behaviour and identify anomalies. This algorithm can predict and prevent fraud with high efficiency on a large scale ((M. Lacuska, 2021).

f. Test Call Generator (TCG)
An active testing tool used to verify the validity of international traffic routes (I. Ighneiwa, 2017). TCG can identify bypass and path manipulation directly through test calls.

g. SIM Card Distribution Control (SDC)
Controlling the distribution of SIM cards to limit fraudsters' access to bulk SIM cards commonly used in SIMBOXes (I. Ighneiwa, 2017). This system prevents perpetrators from obtaining the resources needed to commit fraud.

2.7. *Existing Regulations for Handling and Preventing Fraud in Telecommunication Services in Indonesia*

The handling and prevention of fraud in telecommunications services in Indonesia is regulated in several regulations issued by the Ministry of Communications and Digital. These regulations cover legal, technical, and administrative aspects that apply to service providers. Some of the main regulations include:

a. *Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi*: regulates the prohibition against unauthorized access and manipulation of telecommunications networks or services. Violation of this provision is punishable by imprisonment and/or a fine of up to six hundred million rupiah.

b. *Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi*: regulates the obligation to register customers with the Know Your Customer (KYC) principle, limit the number of numbers that can be registered per identity, and the obligation to deactivate numbers that are indicated to be misused. Violations of these provisions are subject to administrative sanctions.

c. *Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2021 (Perubahan atas Permenkominfo Nomor 13 Tahun 2019)*: requires ITKP providers to prevent and stop fraud, as well as ensure the legality of global partners and the ability to trace the origin of calls. Organizers are also responsible for incoming calls from abroad and are subject to administrative sanctions in case of violation.

d. *Peraturan Direktur Jenderal Penyelenggaraan Pos dan Informatika Nomor 1 Tahun 2021 tentang Ketentuan Teknis Penyelenggaraan Jasa Telekomunikasi*: emphasizes technical obligations for ITKP providers, including the prohibition of distributing SIMBOX, tracing capabilities, the use of SIP/VoIP devices with a minimum of 3,000 sessions, and technical requirements for global partners. It also regulates SOPs for fraud prevention and prosecution, as well as complaint handling mechanisms.

2.8. *Benchmark Other Countries*

Various countries have developed policy and technology approaches to deal with fraud in telecommunications services, especially related to spoofing, robocalls, and international bypass. The following policy studies from several countries can serve as a reference for policy development in Indonesia:

a. United States: through the Federal Communications Commission (FCC), the US implemented the STIR/SHAKEN framework from June 30, 2021, to verify the identity of telephone numbers (Federal Communications Commission, 2020). This technology allows embedding a digital certificate on every call and detects spoofing numbers in real-time. Invalid calls can be marked as spam or blocked. STIR/SHAKEN has proven to be effective in reducing fraudulent calls and increasing consumer confidence.

b. India: The Telecom Regulatory Authority of India (TRAI) made it mandatory to block international calls that spoof Indian numbers. India also banned all promotional calls from unregistered callers and blacklisted them for up to two years. This measure aims to protect consumers from scams that utilize Caller ID manipulation to disguise the origin of calls (Telecom Review, 2024).

c. Singapore: through the Infocomm Media Development Authority (IMDA), Singapore implements policies such as SMS Sender ID registration through the Singapore SMS Sender ID Registry (SSIR), blocking of spoofing calls from 2023 (Infocomm Media Development Authority, 2023), and international cooperation with overseas regulators. The use of technology and verification of authorized senders is relied upon heavily to prevent abuse.

d. Malaysia: The Malaysian Communications and Multimedia Commission (MCMC) collaborated with the NFCC and established the National Scam Response Centre (NSRC). Malaysia blocked more than 1.8 billion scam calls since 2017 (Malaysian Communications and Multimedia Commission, 2023). This policy demonstrates the effectiveness of an integrated approach between technical supervision and rapid response across agencies.

e. Japan: through the Consumer Affairs Agency and operators such as NTT DoCoMo, Japan relies on a nationwide system of early warning, public education, and reporting to protect consumers from international scams. Suspicious calls can be recognized by the system, and users are alerted directly.

3. Method

This research uses a qualitative-descriptive approach with a limited Regulatory Impact Analysis (RIA) framework, which only reaches the stages of: (1) Problem definition, (2) Identification of policy alternatives. In-depth evaluation, stakeholder consultation, and cost-benefit analysis were not conducted within the scope of this research. Problem definition is done by first conducting data analysis to identify the main focus and root causes of existing problems.

Furthermore, to overcome existing problems, the goals or objectives to be achieved by a policy or regulation must be clearly formulated. The formulation of policy objectives will then become identification material for formulating policy alternatives. The formulation of policy alternatives aims to explore various alternative solutions that can be used to achieve the previously formulated policy objectives.

3.1. *Research Framework*

The research framework was developed to guide the process of analyzing the policies for handling and preventing fraud in international termination traffic in Indonesia. Figure 4 below explains the steps taken in this research.

3.2. *Data Source*

This research uses secondary data obtained from official and documented sources. The secondary data includes existing regulatory data and international termination test call test results data.

3.3. *Existing Regulatory Data*

This data includes laws and regulations and technical policies relevant to the handling and prevention of international termination traffic fraud in Indonesia. Among them are:

a. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

b. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi

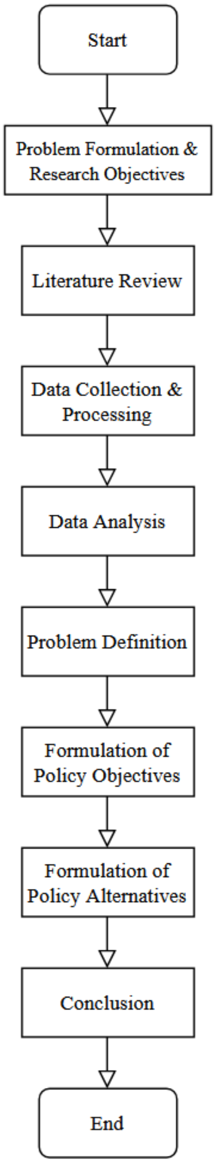
Start
Problem Formulation & Research Objectives
Literature Review
Data Collection & Processing
Data Analysis
Problem Definition
Formulation of Policy Objectives
Formulation of Policy Alternatives
Conclusion
End

Figure 4. Research Flowchart

c. *Peraturan Menteri Komunikasi dan Informatika Nomor Nomor 1 Tahun 2021 tentang Perubahan Kedua Atas Peraturan Menteri Komunikasi dan Informatika Nomor 13 Tahun 2019 tentang Penyelenggaraan Jasa Telekomunikasi*

d. *Peraturan Direktur Jenderal Penyelenggaraan Pos dan Informatika Nomor 1 Tahun 2021 tentang Ketentuan Teknis Penyelenggaraan Jasa Telekomunikasi*

This regulation is used as a basis for analysing the strengths and weaknesses of current policies, as well as for consideration in formulating more effective policy alternatives.

3.4. *International Terminated Call Test Result Data*

This data comes from the results of test calls conducted by the Ministry of Communications and Digital of the Republic of Indonesia during the period 2023-2024. The test was conducted to detect manipulation of international traffic lines by checking the match between the caller number (A Number) and the number detected on the receiving side (B Number).

Calls are categorized as fraud if there are number discrepancies or unauthorized use of local numbers, indicating bypass through devices such as SIMBOX or illegal VoIP lines. This data is limited and only shown in aggregate form to maintain operational confidentiality. Information from test calls is used for:

a. Identify the scale and pattern of fraud incidents
b. Tracking the most commonly used types of manipulation
c. Assessing the effectiveness of policies that have been implemented
d. Provide empirical evidence in the formulation of policy alternatives

3.5. *Regulatory Impact Analysis (RIA)*

Regulatory Impact Analysis (RIA) is an analytical approach used to systematically assess policy impacts, both in terms of benefits and costs (National Development Planning Agency, 2009). This method aims to help policymakers choose the most effective, efficient, and pro-public interest alternatives. Aside from being a regulatory evaluation tool, RIA also serves to increase transparency, accountability, and stakeholder participation in the decision-making process.

According to the Organization for Economic Co-operation and Development (OECD), RIA has four main objectives (Organization for Economic Co-operation and Development, 1997), namely: (1) understanding the real impact of government policies, (2) integrating various policy objectives, (3) increasing transparency and public consultation, and (4) strengthening government accountability. There are several main processes or stages that must be passed in RIA, as shown in Figure 5 below.

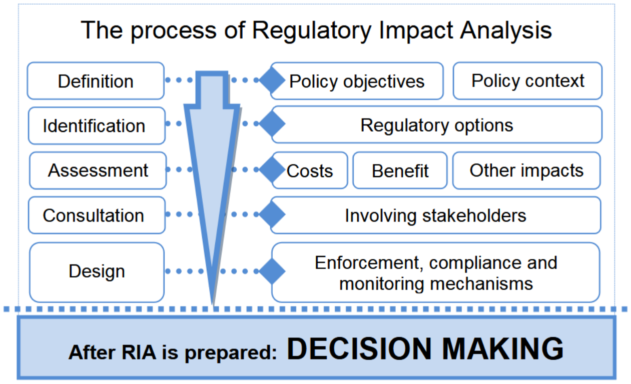

Figure 5. RIA Process Stages (Organisation for Economic Co-operation and Development, 2008)

In this study, the RIA approach was used in a limited way, covering only two initial stages:

1. Problem Definition: identify the main problem in the form of rampant fraud in international termination traffic in Indonesia and the limitations of existing policies.
2. Formulation of Policy Alternatives (Identification): exploring various policy solution options, both regulatory (e.g., issuance of technical regulations or revision of rules) and non-regulatory (e.g., public education or private collaboration), as a basis for consideration for better decision-making.

This study did not proceed to the assessment stage, quantitative impact analysis, public consultation, or policy implementation design, given that the focus of the study was only on preliminary analysis to formulate policy options that could be followed up by policymakers at a later stage.

4. Result and Discussion

4.1. *Data Analysis of International Terminated Call Test Results*

From the data on the results of the international termination test call that has been carried out by the Ministry of Communication and Digital in the period 2023 to 2024, compilation data in aggregate form is obtained, which reflects the percentage trend of fraud calls that occurred in the period 2023 to 2024. Data on the results of the international termination test call can be seen in Table 1 below:

Table 1. International Terminated Call Test Result Data

Month	Year	Number of Test Calls	Number of Legal Calls	Number of Fraud Calls	% Fraud
May	2023	15,016	12,219	2,797	18.63
June	2023	15,155	12,777	2,378	15.69
July	2023	15,033	13,724	1,309	8.71
August	2023	15,058	13,540	1,518	10.08
September	2023	15,094	13,786	1,308	8.67
October	2023	14,966	13,491	1,475	9.86
November	2023	15,446	14,292	1,154	7.47
December	2023	15,236	14,162	1,074	7.05
March	2024	13,647	9,448	4,199	30.77
April	2024	14,926	10,618	4,308	28.86
May	2024	14,075	9,066	5,009	35.59
June	2024	14,105	9,185	4,920	34.88
July	2024	13,702	8,039	5,663	41.33
August	2024	13,888	7,825	6,063	43.66
September	2024	13,673	7,751	5,922	43.31
October	2024	13,650	8,056	5,594	40.98

Source : (*Direktorat Pengendalian Ekosistem Digital,* 2024)

Based on the results of tests conducted regularly every month by the Ministry of Communications and Digital, an average of 13,000-15,000 international calls is tested. During 2023, the percentage of calls indicated as fraud showed a downward trend, from 18.63% in May to 7.05% in December. This decrease is largely attributed to the efforts of the Ministry of Communications and Digital of the Republic of Indonesia to ask mobile operators to block numbers that are indicated to be used for traffic manipulation (fraud), although the mechanism and SOP are not yet regulated in a standardized regulation.

However, the trend reversed in 2024. The data shows a significant spike in the percentage of fraud, starting from 30.77% in March to a peak of 43.66% in August 2024. This figure remained high in the following months, at 43.31% (September) and 40.98% (October). The trend of the percentage of fraudulent calls that occurred in the period 2023 to 2024, based on data processing of the results of international termination test calls that have been carried out by the Ministry of Communication and Digital, can be seen in Figure 6.

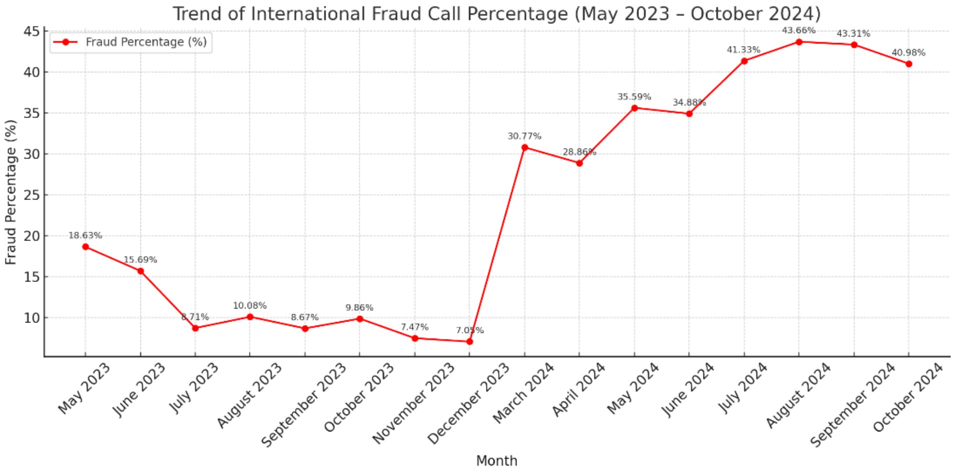

Figure 6. Trend in Percentage of Fraud Calls Occurring in the Period of 2023 to 2024

The increase in the percentage of fraud indicates a worsening of fraud control conditions. This finding emphasizes the urgency of updating policies and strengthening technical regulations to tackle fraud practices more systematically and sustainably.

Meanwhile, aggregate data on the results of identifying the number of fraud calls based on the number category can be seen in Table 2 below.

Table 2. Data Identification of the Number of Fraud Calls by Category Number

Month	Year	Number of Fraud Calls	Number of Fraud Calls				
			Anonymous	Foreign Number	Fixed Line (PSTN)	Off-Net Mobile	On-Net Mobile
May	2023	2,797	213	183	77	66	2,558
June	2023	2,378	118	295	92	1,062	811
July	2023	1,309	79	142	15	293	780
August	2023	1,518	89	130	10	675	614
September	2023	1,308	4	122	0	808	374
October	2023	1,475	2	183	6	529	755
November	2023	1,154	43	295	5	67	744
December	2023	1,074	8	73	1	635	357
March	2024	4,199	1,437	2,108	6	1	647
April	2024	4,308	1,608	1,826	1	2	871
May	2024	5,009	2,263	1,927	6	169	644
June	2024	4,920	1,722	2,229	17	416	986
July	2024	5,663	1,389	2,713	13	318	1,230
August	2024	6,063	1,730	3,091	2	122	1,118
September	2024	5,922	1,495	2,842	13	192	1,380
October	2024	5,594	1,087	2,898	13	226	1,370

Source : (*Direktorat Pengendalian Ekosistem Digital, 2024*)

The trend graph of the number of fraud calls based on the number category can be seen in Figure 7.

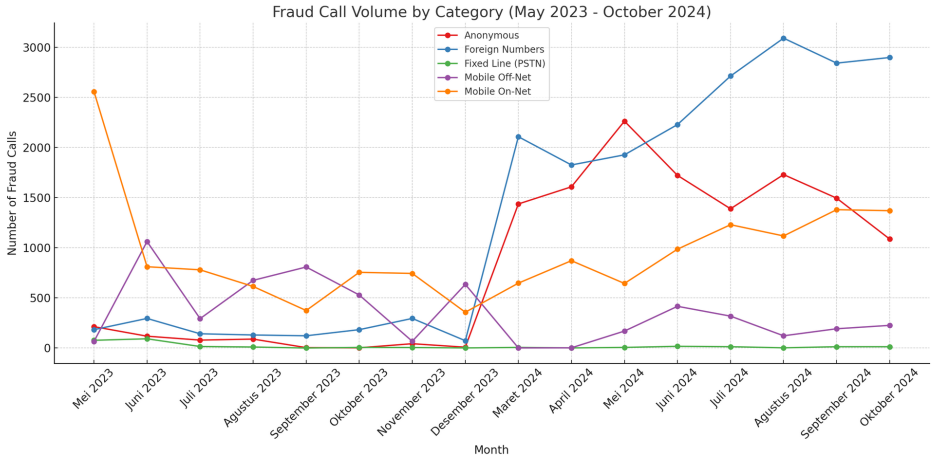

Figure 7. Trends in the Number of Fraud Calls by Number Category

In the past one year, the trend of fraud calls showed significant dynamics. The highest number of fraud calls in 2023 occurred in May, with 2,797 cases, but experienced a gradual decline until it reached its lowest point in December 2023 with 1,074 calls. This changed dramatically in March 2024, when the number of fraudulent calls jumped to 4,199 and continued to increase until it peaked at 6,063 in August 2024.

By category, fraud calls using anonymous and calls from foreign numbers experienced the sharpest increase. Fraudulent calls using anonymous numbers rose from 213 (May 2023) to 2,263 (May 2024), while fraud calls from foreign numbers increased from 183 to 2,898 in the same period. In contrast, the category of fraud through local numbers, such as fixed line (PSTN) and mobile off-net, showed a more stable trend although it continued to fluctuate.

This increasing phenomenon is estimated to be caused by the use of increasingly sophisticated fraud methods, including the exploitation of loopholes in the surveillance system and telecommunications network security. Changes in the perpetrator's strategy to avoid prevention efforts that have been carried out by relying on anonymous methods and spoofing foreign numbers also complicate the early detection process by operators.

In response, it is necessary to strengthen the fraud detection system. Implementation of fraud monitoring and detection systems, automatic blocking of suspicious sources are also crucial in mitigation efforts.

Based on the results of the data analysis above, various problems that still occur related to international termination traffic fraud can be identified as follows:

1. The trend of international termination fraud cases is still uncontrolled and tends to increase, despite monitoring and blocking requests by the Ministry of Communications and Digital to numbers indicated to be used for fraud.
2. Fraudulent calls were identified using anonymous numbers, foreign numbers, fixed lines, and mobile numbers both On-Net and Off-Net, with the number of fraudulent calls from anonymous and foreign numbers rising sharply in 2024.
3. There has been a shift in fraudsters strategies from using local number masking (e.g. through SIMBOX) to international spoofing techniques, where the identity of the caller's number is manipulated or hidden. This trend reflects the weak control mechanisms against spoofed calls and calls with hidden identities.
4. The absence of binding technical regulations and the lack of a comprehensive and sustainable monitoring mechanism have led to the ineffective implementation of the fraud number blocking policy

4.2. *Analysis of Existing Regulations*

The problem of fraud in international termination traffic has a serious impact on the integrity of telecommunications services, potential state losses, and public trust in telecommunications service providers. Along with the development of digital crime modes, it is necessary to review the effectiveness of applicable regulations, both from a normative and an implementational perspective.

1. *Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi*
   This law prohibits unauthorized access and manipulation of telecommunications networks, and serves as the legal basis for fraud enforcement. However, these provisions are not yet supported by adequate derivative technical regulations to regulate operational monitoring and enforcement procedures at the operator level.
2. *Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi*
   This regulation regulates customer registration and deactivation of numbers that are indicated to be used for illegal acts. However, its scope is still limited to general number misuse and does not yet regulate technical obligations such as international traffic monitoring, fraud detection, or mechanisms for systematic automatic blocking of fraudulent numbers.
3. *Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2021 tentang Penyelenggaraan Jasa Telekomunikasi dan Peraturan Dirjektur Jenderal Penyelenggaraan Pos dan Informatika Nomor 1 Tahun 2021* tentang *Ketentuan Teknis Penyelenggaraan Jasa Telekomunikasi*
   This regulation regulates the obligations of ITKP providers in preventing and handling fraud, including masking. However, the focus is still limited to ITKP-based VoIP service lines and does not cover SLI lines, which are also vulnerable to fraudulent traffic. The absence of technical provisions for surveillance on SLI services is a significant regulatory gap, considering that the potential for fraud is not only limited to ITKP lines, but can also occur through SLI lines.

In general, the applicable regulations are still partial and have not touched on the technical needs as a whole, both for monitoring and fraud detection systems, as well as fraud number blocking mechanisms. Strengthening regulations is needed through technical standards and operational procedures that cover all types of services, namely SLI and ITKP, so that policies can be implemented consistently by all providers.

4.3. *Problem Formulation*

Based on the results of the analysis that has been carried out, the focus of the problem in this study is the number of international termination fraud calls in Indonesia which is still high and uncontrolled, despite the existence of a number of regulations in the telecommunications sector. This indicates an ineffective implementation or regulatory vacuum in the aspect of the necessary technical arrangements. This problem has the potential to have a negative impact on several things as described in Table 3.

Table 3. The Potential Impact of High and Uncontrolled International Termination Traffic Fraud Activity

Stakeholders	Impact
Regulator	1). Potential loss state revenue 2). Opening a loophole for crime through telecommunication services 3). Decreased credibility of regulators
Telecommunication Operator	1). Revenue leakage 2). Potential loss of customers 3). Decline in reputation

Stakeholders	Impact
Community	1). Financial loss due to potential loopholes for crime and fraud 2). Declining public trust in telecommunications services 3). Insecurity and concern due to potential crime and fraud through telecommunications services

Based on data released by The Communications Fraud Control Association (CFCA), telecommunications fraud cases, especially for the type of Interconnect Bypass Fraud, have cost the telecommunications industry globally $2.71 billion in 2019 (The Communications Fraud Control Association, 2021). This makes telecommunications operators lose their revenue due to fraudulent activities in telecommunications services.

The loss or decline of telecommunication operator revenue will also have an impact on the potential loss of Non-Tax State Revenue (PNBP) from the telecommunications sector, because each telecommunication operator must pay Telecommunication Rights Fee (BHP) of 0.5% of gross revenue to the state every year (*Peraturan Menteri Komunikasi dan Informatika Nomor 17 Tahun 2016*).

International termination traffic fraud can also be a very serious loophole for criminals and fraudsters that can harm the public. International traffic bypass fraud makes tracking criminals difficult for law enforcement and service providers because it is hidden behind an illegal bypass system. The losses experienced by the public as users of telecommunications services will certainly cause concern and have an impact on the decline in the level of trust, and can also have an impact on the decline in the reputation of telecommunications operators as telecommunications service providers.

Based on the results of the analysis that has been carried out, the causes of the emergence of international termination fraud problems in Indonesia that are still high and uncontrolled can be identified as follows:

1. There are no provisions that specifically regulate fraud prevention and handling mechanisms in International Direct Connection (SLI) services, considering that the potential for fraud is not only limited to ITKP lines, but can also occur through SLI lines.
2. There is no technical regulation that requires telecommunications operators to implement a fraud monitoring and detection system, as well as blocking numbers that are indicated to be used for international termination traffic fraud.
3. Supervision carried out by regulators on efforts to prevent and handle fraud in international termination traffic has not been carried out comprehensively, including in the aspect of strict law enforcement. This condition causes responses to fraud threats to tend to be reactive and still rely on incidental reports, not through a proactive and systematic prevention approach.
4. The lack of rules regarding technology-based approaches to prevent fraud in telecommunications services in Indonesia.

4.4. *Formulation of Policy Objectives*

Based on the results of the identification and analysis of problems that have been carried out, it currently shows that there are still a number of fundamental weaknesses in terms of preventing and handling fraud in international terminated traffic in Indonesia. To overcome the existing problems, it is necessary to clearly formulate the goals or objectives to be achieved by a policy or regulation. The formulation of policy objectives is carried out using gap analysis as described in Table 4.

Table 4. Gap Analysis of International Terminated Traffic Fraud Issues in Indonesia

Current Condition	Desired Condition
High and uncontrolled number of fraud calls in international termination traffic	Low and controlled number of international initiated traffic fraud calls
The absence of provisions governing fraud prevention and handling mechanisms in SLI services	The existence of provisions that comprehensively regulate the mechanism for preventing and handling fraud in international termination traffic, both for ITKP and SLI services.
The absence of standardized rules and SOPs that require telecommunications operators to monitor, detect, and block fraudulent numbers in international termination traffic	Telecommunications operators actively and effectively monitor, detect, and block numbers that are indicated to be used for fraud.
Supervision carried out by regulators has not been carried out comprehensively, including in terms of law enforcement	Regulators conduct comprehensive and continuous supervision to ensure the prevention and handling of international termination traffic fraud is effective.
Lack of technology-based approach to international termination traffic fraud prevention	Effective and adaptive application of technology in international traffic fraud prevention

Based on the results of the gap analysis, it can be indicated that there is an urgent need to formulate a comprehensive regulation to regulate the mechanism of prevention and handling of international termination traffic fraud activities in Indonesia. The following points are the main focus of corrective action efforts to achieve the expected conditions, namely as follows:

1. Create more comprehensive rules regarding the prevention and handling of international termination traffic fraud, both from SLI lines and from ITKP lines, considering the potential for fraud not only comes from ITKP lines but also from SLI lines.
2. Require all telecommunications operators to implement a comprehensive and continuous fraud monitoring and detection system, as a preventive measure against international termination traffic fraud activities.
3. Implement a blacklist database of fraud numbers, which is a database containing a list of fraud numbers that must be blocked by all operators.
4. Require all telecommunications operators to block and blacklist all numbers that are indicated to be used for fraud activities.
5. Implementing technology in international termination traffic fraud monitoring and detection systems to enhance the accuracy and effectiveness of fraud prevention efforts.

4.5. *Formulation of Policy Alternatives*

Based on the results of the analysis and identification that has been carried out, it is necessary to formulate technical provisions that contain the corrective action efforts described previously in a systematic manner. These technical provisions are useful as a reference for all telecommunications operators to perform better and more effective handling and prevention of international termination traffic fraud, so as to overcome the current problems.

At this stage, policy makers need to consider both regulative and non-regulative alternatives, taking into account the effectiveness, feasibility of implementation, as well as the experience of other countries that have implemented similar policies. The policy alternatives proposed in this research are focused on the regulative approach, by considering effectiveness and prioritizing the principle of adaptability to technological developments, so as to achieve the objectives of overcoming the problems previously identified.

On the other hand, the formulated policy must still be able to provide legal certainty, protect the public interest, and support the sustainability of the national telecommunications industry. Based on the results of the analysis that has been carried out, there are several alternative policy proposals that can be used as a reference in the formulation of technical regulations for the prevention and handling of international termination traffic fraud, as shown in Table 5 below.

Table 5. Alternative Technical Provisions for Handling and Preventing Fraud of International Termination Traffic

Alternative	Description
Alternative 1	Status Quo (no policy change)
Alternative 2	Regulated technical provisions by setting certain method standards for the system monitoring and fraud detection, such as STIR/SHAKEN, AI-based real-time traffic monitoring, Test Call Generator (TCG), and so on.
Alternative 3	Regulated technical provisions without setting specific method standards, by providing flexibility to operators to determine the technology of monitoring dan fraud detection systems used.

a. Alternative 1
This alternative maintains current policies and regulations without technical strengthening or new supervisory systems. Fraud handling is reactive and relies on limited reports or monitoring results. Although it does not incur additional costs, this approach is high-risk because it is unable to keep up with the complexity of modern fraud, such as spoofing, SIMBOX, and abuse of international lines through SLI and ITKP.

b. Alternative 2
This alternative emphasizes the formulation of technical regulations that require the application of certain methods by all operators to prevent and handle international termination traffic fraud. This approach encourages standardization of detection systems, such as STIR/SHAKEN, AI-based monitoring, and Test Call Generator (TCG), to improve monitoring effectiveness and uniformity of implementation. While more regulatory robust, this alternative requires transitional support and investment for operators who are not yet technically ready. In the long run, this approach has the potential to create a more standardized and resilient telecommunications security ecosystem.

c. Alternative 3
This alternative offers a flexible regulatory approach, where regulators require operators to implement fraud monitoring and detection systems without specifying specific technical methods. Operators are given the freedom to choose the appropriate technology, such as AI/ML-based detection or big data analytics. This approach is output-based (prevention results) and encourages innovation and efficiency among operators. However, its effectiveness still requires regular monitoring and evaluation mechanisms from the regulator.

5. Conclusion

Fraud in international trade in Indonesia is still a critical issue that has not been addressed optimally. Analysis of test call data shows a significant upward trend in fraud cases since early 2024, especially through spoofing techniques and the use of anonymous or foreign numbers. Although regulations are in place, weaknesses in technical aspects (such as monitoring and fraud detection systems) as well as supervisory mechanisms mean that existing policies have not been able to provide adequate protection.

Through a limited approach of Regulatory Impact Analysis (RIA), this study successfully identified three policy alternatives: (1) no policy change (status quo), (2) regulate technical provisions by setting specific method standards for fraud monitoring and detection systems, and (3) regulate technical provisions without setting specific method standards. Each alternative has different implications for implementation effectiveness and industry readiness.

This research recommends the importance of comprehensively updating technical regulations for both ITKP and SLI services, as well as implementing a scalable technology-based fraud monitoring and detection system. This step is needed to strengthen the supervisory system, increase operator accountability, and protect the public interest in the face of increasingly complex telecommunications fraud challenges.

6. Acknowledgements

The author would like to thank all parties who have helped complete this research, especially the Ministry of Communication and Digital of the Republic of Indonesia.

References

B. A. Yehya; N. Salhab. (2023). *Telecommunications Fraud Machine Learning-based Detection*. IEEE 4th International Conference on Data Analytics for Business and Industry (ICDABI). Doi:0.1109/ICDABI60145.2023.10629612.

B. Jendruszak. (2025). *Balancing AI's Benefits and Threats Across Fraud and Cybersecurity*. Retrieved from https://seon.io/resources/balancing-ais-benefits-and-threats/

Badan Perencana Pembanungan Nasional. (2009). *Arti Penting Analisis Dampak Peraturan Perundang-Undangan "Regulatory Impact Assessment (RIA)"*. Jakarta.

Europol. (2021). *Telecommunications Fraud*. Retrieved from https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/telecommunications-fraud#:~:text=Telecommunications%20fraud%20(aka%20Telecom%20fraud)%20represents%20a,can%20take%20many%20different%20forms%2C%20among%20others:

Federal Communication Commission. (2020). *FCC Mandates That Phone Companies Implement Caller ID Authentication To Combat Spoofed Robocalls*. Retrieved from https://docs.fcc.gov/public/attachments/DOC-363399A1.pdf

Hanrui Gong. (2022). *The Dilemma of Telecommunication Fraud Crime - An Analysis of China's Governance Model as a Sample*. SHS Web of Conferences 148, 03049. https://doi.org/10.1051/shsconf/202214803049.

I. Ighneiwa, H. S. Mohamed. (2017). *Bypass Fraud Detection: Artificial Intelligence Approach*. doi:10.48550/arXiv.1711.04627, 2017.

Infocomm Media Development Authority. (2023). *Scam measures implemented by IMDA*. Retrieved from https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2023/09/scam-measures-implemented-by-imda/scam-measures-implemented-by-imda.pdf

M. Lacuska, T. Peracek. (2021). *Trends in Global Telecommunication Fraud and Its Impact on Business*. In book : Developments in Information & Knowledge Management for Business Applications (pp.459-485). doi:10.1007/978-3-030-62151-3_12

Malaysian Communications and Multimedia Commission. (2023). *MCMC blocked 1.8 billion scam calls from 2017 to 2022*. Retrieved from https://www.mcmc.gov.my/en/media/press-clippings/fahmi-mcmc-blocked-1-8-billion-scam-calls-from-201

Organisation for Economic Co-operation and Development. (2008). *Building an Institutional Framework for Regulatory Impact Analysis (RIA): Guidance for Policy Makers*. Paris.

Organisation for Economic Co-operation and Development. (1997). *Regulatory Impact Analysis : Best Practices in OECD Countries*. Paris.

Peraturan Direktur Jenderal Penyelenggaraan Pos dan Informatika Nomor 1 Tahun 2021 tentang Ketentuan Teknis Penyelenggaraan Jasa Telekomunikasi. (2021).

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 Tentang Penyelenggaraan Telekomunikasi. (2021).

Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2021 tentang Perubahan Kedua Atas Peraturan Menteri Komunikasi dan Informatika Nomor 13 Tahun 2019 Tentang Penyelenggaraan Jasa Telekomunikasi. (2021).

Peraturan Menteri Komunikasi dan Informatika Nomor 13 Tahun 2019 Tentang Penyelenggaraan Jasa Telekomunikasi. (2019).

Peraturan Menteri Komunikasi dan Informatika Nomor 17 Tahun 2016 Tentang Petunjuk Pelaksanaan Tarif Atas Penerimaan Negara Bukan Pajak Dari Pungutan Biaya Hak Penyelenggaraan Telekomunikasi Dan Kontribusi Kewajiban Pelayanan Universal/ Universal Service Obligation. (2016).

Telecom Review. (2024). *DoT Mandates Telcos to Block International Spoofed Calls Using Indian Numbers*. Retrieved from https://telecomreviewasia.com/news/industry-news/4266-dot-mandates-telcos-to-block-international-spoofed-calls-using-indian-numbers/

The Communications Fraud Control Association. (2021). *CFCA 2019 Global Fraud Loss Survey*. Retrieved from https://cfca.org/wp-content/uploads/2021/02/CFCA-2019-Fraud-Loss-Survey.pdf

Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi. (1999).