Journal of Business and Management Sciences, 2026, Vol. 14, No. 2, 12-19
Available online at http://pubs.sciepub.com/jbms/14/2/1
Published by Science and Education Publishing
DOI:10.12691/jbms-14-2-1

Adaptive Governance and Management of Telecom and Online Fraud: Evidence from Taiwan

Fu-Hsiang Kuo[1,2,3,*], Mei-Mei Lin[3]

[1]School of Economics and Management, Guangzhou Institute of Science and Technology, Guangzhou, China
[2]Department of Finance, National Yunlin University of Science and Technology, Yunlin County, Taiwan 640301, R.O.C
[3]Department of Hospitality Management, Tung Nan University of Technology, New Taipei City, Taiwan 222304, R.O.C
*Corresponding author: s1185072@gmail.com

Received March 04, 2026; Revised April 07, 2026; Accepted April 14, 2026

Abstract This study conducts a longitudinal analysis of telecommunication and online fraud in Taiwan from 2022 to 2025, examining the evolution of crime structure, the improvement of judicial efficiency, and the adaptability of governance strategies. The findings indicate a three-stage transformation in offender roles: initially relying on identity accounts as the operational foundation; shifting to direct perpetrators as account controls intensified; and, more recently, exhibiting a "displacement effect" toward cashiers and money laundering agents under enforcement pressure, reflecting the high adaptability of criminal networks. With respect to judicial efficiency, the study uses the average convictions per case (ACPC) as an indicator, revealing a sustained increase in conviction momentum, which reflects the enhanced effectiveness of the judicial system in investigating, prosecuting, and adjudicating complex cases. Finally, in alignment with the United Nations Sustainable Development Goals, this study proposes policy recommendations to strengthen financial integrity, enhance the resilience of digital infrastructure, and improve institutional governance capacity to address the continuously evolving nature of fraud.

Keywords: *Telecommunication fraud, online fraud, fraud networks, criminal role structure, anti-fraud strategies*

Cite This Article: Fu-Hsiang Kuo, and Mei-Mei Lin, "Adaptive Governance and Management of Telecom and Online Fraud: Evidence from Taiwan." *Journal of Business and Management Sciences*, vol. 14, no. 2 (2026): 12-19. doi: 10.12691/jbms-14-2-1.

1. Introduction

Fraud and scams represent major global challenges that have been further intensified by the rapid development of new technologies [1]. Moreover, fraudulent activities always exist. Research has consistently emphasized the detrimental effects of these crimes—not only on the psychological and physical well-being of victims but also on society as a whole. However, this phenomenon does not appear to be diminishing [2,3]. In contrast, scammers' strategies have become increasingly sophisticated and supported by advanced technologies.

According to the Global State of Scams Report 2024, which was jointly released by Feedzai and the Global Anti-Scam Alliance, scams caused an estimated global loss of up to USD 1.03 trillion over the past year, with the United States being the most severely affected country [4]. In 2023, the United States recorded 880,418 cybercrime complaints, with potential losses exceeding USD 12.5 billion—representing a 10% increase in the number of complaints and a 22% increase in total losses compared with 2022 (Internet Crime Complaint Center [IC3], 2023) [5]. Reports further indicated that complaints from older adults increased by 14% in 2023, with total losses surpassing USD 3.4 billion, nearly 11% higher than in 2022. Most of these losses stemmed from online fraud and scams [5].

On the other hand, Taiwan is also among the countries significantly affected by fraud. According to judicial statistics (Ministry of Justice, R.O.C. (Taiwan), in 2025), the number of cases of telecommunication fraud between 2021 and 2025 exhibited a fluctuating trend of "increase, decline, and rebound." From 2021--2022, the number of cases sharply increased, reflecting the rapid expansion of fraudulent activities in the digital environment. In 2023, a notable decline occurred, suggesting the effectiveness of strengthened law enforcement and increasing public awareness of fraud prevention. However, in 2024, case numbers surged again to a new peak, indicating that fraud schemes had become more active when emerging technologies were integrated. By the first half of H1 for 2025, the case numbers had slightly stabilized, showing a moderate fluctuation pattern that reflects the dynamic interplay between fraudulent behaviors and governmental countermeasures. As shown in Figure 1.

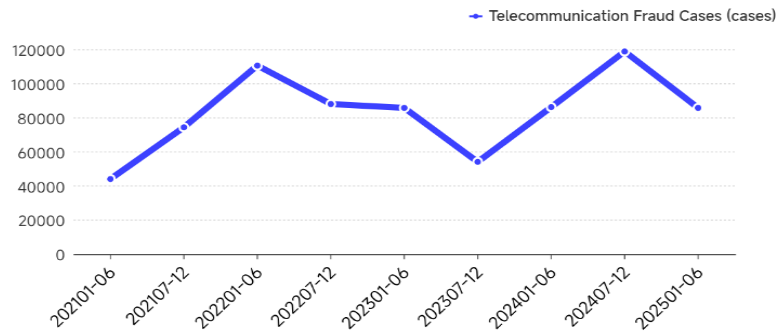

Figure 1. Fraud Trend Chart for Taiwan for 2021 to 2025 H1

This study addresses three key dimensions—crime structure transformation, role composition, and law enforcement efficiency—and extends the analysis by incorporating dynamic adaptation and sustainable governance perspectives. This integrated framework enhances the study's policy implications and ensures its long-term relevance. Detailed explanations are provided as follows:

1. How has the composition of different types of telecommunication and online fraud crimes in Taiwan changed?
2. How does the structural proportion of each crime role change annually?
3. What is the efficiency of law enforcement in handling telecommunication and online fraud cases?
4. How can law enforcement strategies be adapted to ensure the long-term sustainability and effectiveness of combating telecommunication and online fraud in Taiwan?

The research framework of this study is organized into five main sections. The introduction presents the background, research motivation, and objectives. The literature review examines relevant theories and empirical studies, identifies research gaps, and justifies the study's significance. The methodology describes the research design, data sources, variables, and analytical methods. The empirical results of the research analysis are presented, the data are interpreted, and the findings in relation to the research questions are discussed. Finally, the conclusions and recommendations summarize key findings, discuss practical implications, and offer suggestions for future research and policy-making.

2. Literature Review Integration

2.1. The Global Context of Telecom Fraud

Telecom fraud has become a major challenge faced by the global telecommunications industry, causing enormous financial losses and having profound psychological and physical effects on victims. According to Dadà et al. (2025) [1], the terms "fraud" and "scam" are often used interchangeably to describe various deceptive practices intentionally carried out for economic gain. Unlike other types of crime, fraud typically requires the active participation of the victim, such as providing personal information or transferring money [6].

From the victim's perspective, the consequences of fraud can be described as a form of "double harm" or "double loss," as it results in both financial damage and psychological trauma [7]. Moreover, substantial financial losses further undermine victims' overall well-being and quality of life [8]. Previous studies have shown that victims of fraud may experience severe psychological and physical health problems, including stress, anxiety, depression, and loss of self-esteem [9,10]. These findings indicate that fraud is not merely an economic crime but also a significant social and psychological health issue.

2.2. The Social Context and Characteristics of Telecom Fraud in Taiwan

In Taiwan, patterns of fraudulent activities are closely related to the widespread use of instant messaging applications. Given that more than 93% of Taiwanese people use LINE as their primary communication tool, fraud groups often exploit this platform to create "investment scam groups," luring the public to participate in fake investment schemes [11]. According to official statistics, investment fraud in 2023 caused financial losses of up to NT$5.34 billion, accounting for 60% of the total annual fraud-related property losses. Fraudsters frequently impersonate celebrities and disseminate misleading investment information across social media and instant messaging platforms to attract potential victims to join LINE groups.

Victims are typically asked to add "professional consultants" or "assistants" as friends and are subsequently guided into fraudulent investment groups or counterfeit trading websites, eventually transferring money within a fabricated trading environment [12]. This type of fraud combines social trust with information manipulation, leveraging the authenticity of social interaction and the pervasiveness of social media to achieve both psychological persuasion and economic exploitation.

In summary, the threat of telecom fraud arises not only from advancements in technology and communication methods but also from deep-rooted dependencies on social interaction and media connectivity. Taiwan's heavy reliance on instant messaging applications has enabled fraud groups to manipulate social trust for psychological control and economic exploitation.

Future prevention strategies should integrate technological regulation, educational awareness

campaigns, and psychological protection mechanisms to increase public vigilance and digital security literacy. Such efforts could reduce potential victimization risks and help maintain societal trust and information security.

Therefore, this study aims to investigate and analyze the current status and major patterns of fraud activities and further assess the effectiveness of existing prevention measures, with the goal of providing empirical evidence for future policymaking and practical counterfraud initiatives.

3. Methodology

This study aims to analyze the dynamic evolution and effectiveness of the governance of telecommunication and internet fraud in Taiwan, focusing on three core dimensions: crime structure, role composition, and law enforcement efficiency. The research methodology assesses changes in criminal activities using the structural ratio and semiannual change rate and further incorporates the judicial efficiency indicator to evaluate the effectiveness of law enforcement in handling cases. This integrated analytical framework facilitates a comprehensive understanding of both the evolution of criminal behavior and the effectiveness of governance.

3.1. Statistical Methods

3.1.1. Proportion of Each Offender Type (Structural Ratio Indicator)

The proportion of each offender type (POEOT) measures the structural share of each category of offenders among the three major types of fraud perpetrators. This indicator reflects the constituent characteristics and distribution structure of participants involved in fraudulent activities, as expressed in Equation (1) below:

$$POEOT_{i,t} = \frac{N_{i,t}}{\sum_{i=1}^{3} N_{i,t}} \times 100\% \quad (1)$$

- $\mathrm{POEOT}_{i,t}$: Proportion of offender type i in period t (%).
- $N_{i,t}$: Number of offenders of type i in period t .
- $i = 1$: Providing only bank accounts; $i = 2$: General Telecommunications Fraud; $i = 3$: Only money rules.

3.1.2. Trend Analysis by Offender Type (Trend Dynamics Indicator)

Trend analysis by offender type (TABOT): This formula calculates the semiannual growth or decline of each variable, capturing short-term trend dynamics, as presented in Equation (2).

$$\mathrm{TABOT_t} = \frac{N_t - N_{t-1}}{|N_{t-1}|} \times 100\% \quad (2)$$

- TABOT_t : Semiannual change rate in period t (%).
- N_t : Number of offenders in each role during the current period.
- N_{t-1} : Number of offenders in each role during the previous period

3.1.3. Average Convictions Per Case (Judicial Efficiency Indicator)

The average convictions per case (ACPC) indicator is employed as a proxy variable to capture judicial prosecution and case-handling efficiency. Notably, this indicator does not correspond to the official case clearance rate. Rather, it reflects the average number of defendants who are ultimately convicted per fraud case, thereby providing a quantitative measure of judicial effectiveness in processing fraud-related offenses. The operational definition of this indicator is formally specified in Equation (3).

$$ACPC_t = \frac{Final\ Convicted\ Persons_t}{Telecommunications\ Fraud\ Cases_t} \quad (3)$$

- $ACPC_t$: Average number of final convicted persons per case in period t.
- $Final\ Convicted\ Persons_t$: Total final convicted persons in period t.
- $Telecommunications\ Fraud\ Cases_t$: Total number of fraud cases in period t.

3.2. Data Sources and Description

The data employed in this study were sourced from the Ministry of Justice of Taiwan (2025) and cover a four-year period from January 2022 to December 2025. The dataset comprises statistics on telecommunication and internet fraud cases handled by district prosecutors' offices across Taiwan. Compared on a semiannual basis, the data provide authoritative and comprehensive information, reflecting recent trends and developments in telecommunication and internet fraud. These data serve as a fundamental basis for subsequent analyses of growth rates and trend dynamics [13,14].

4. Results and Analysis

This analytical section is structured into three parts. First, the study variables are defined and examined through descriptive statistical analysis. Second, empirical analyses are conducted using the structural ratio indicator of POEOT, the trend dynamics indicator of TABOT, and the judicial efficiency indicator of ACPC. Finally, an integrated analytical framework is constructed to systematically present and synthesize the evolving trends and structural relationships of cases of telecommunication fraud.

4.1. Definitions of Basic Variables and Statistical Analysis

4.1.1. Definitions of Basic Variables

This study explores primarily the composition ratio and structural changes in cases of telecommunication fraud. To facilitate subsequent analyses, the definitions and

explanations of the variables used in this research are presented below.

In accordance with the relevant data, the main analytical variables used in this study include the number of cases of telecommunication fraud, the proportion of cases of telecommunication fraud among all newly investigated cases (%), the number of individuals who solely provided dummy bank accounts, the number of general cases of telecommunication fraud, the number of money mules, the number of individuals convicted by final judgment, and the conviction rate (%). A summary is presented in Table 1.

Table 1. Definitions and descriptions of the variables used in the study

No.	Variable Name	Unit	Definition
X_1	Providing Only Bank Accounts (Dummy Accounts)	Persons	Number of offenders who only provide personal bank accounts (dummy accounts) for telecommunications fraud gangs, without participating in other fraud behaviors.
X_2	General Telecommunications Fraud	Persons	Number of offenders who directly implement telecommunications fraud, excluding those who only provide accounts or act as money mules.
X_3	Only Money Mules	Persons	Number of offenders who only withdraw, transfer or launder illegal funds for fraud gangs, acting as cash handlers.
X_4	Final Convicted Persons	Persons	Number of offenders whose criminal judgments have become final and legally binding (no appeal pending).
X_5	Telecommunications Network Fraud Cases	Cases	Total number of new telecommunications fraud cases accepted for investigation in the current period.

Source: Compiled by this study.

4.1.2. Statistical Analysis

Table 2 presents the dataset used in this study, covering 8 semiannual periods over 4 years. It includes variables X1 to X5, with a total of 40 observations.

Table 2. Data structure and variable description (2022–2025, Semi-Annual data)

Period	X_1	X_2	X_3	X_4	X_5
202201	851	623	841	751	5711
202202	1105	1075	772	951	7126
202301	1108	1057	608	1110	7784
202302	1406	1053	987	1167	8268
202401	509	1625	1018	1346	5974
202402	615	1261	1852	1351	5353
202501	692	1533	1871	1878	6196
202502	697	1307	2832	2162	5634

Source: Compiled and calculated in this study.

Descriptive statistics for all the variables are presented in Table 3. Each variable consists of eight observations, ensuring a consistent sample structure across the study period. In terms of mean values, X_5 has the highest average (6505.75), indicating that it is substantially larger than the other variables. This is followed by X_3 (1347.63) and X_4 (1339.50), whereas X_2 (1191.75) and X_1 (872.88) have relatively lower mean levels.

With respect to dispersion, the standard deviation (SD) reveals that X_3 (765.83) and X_5 (1083.86) display greater variability, suggesting that these variables are more sensitive to external influences or policy changes. In contrast, X_1 (306.23) and X_2 (315.49) exhibit lower standard deviations, indicating more stable and concentrated distributions.

An examination of the range (minimum and maximum values) further highlights the variability across variables. X_3 shows the widest range, from 608 to 2832, indicating substantial fluctuations over time. X_5 ranged from 5353 to 8268, reflecting a relatively high level with moderate variability.

Finally, the standard error (SE) values indicate that X1 and X_2 have lower estimation uncertainty, whereas X_3 and X_5 exhibit higher standard errors, further confirming their greater variability. Overall, the results suggest notable differences in both scale and volatility across variables, providing a solid foundation for subsequent trend and structural analyses.

Table 3. Descriptive statistics of the variables

Variable	N	Min	Max	Mean	SE	SD
X_1	8	509	1406	872.88	108.27	306.23
X_2	8	623	1625	1191.75	111.54	315.49
X_3	8	608	2832	1347.63	270.76	765.83
X_4	8	751	2162	1339.50	166.17	470.01
X_5	8	5353	8268	6505.75	383.20	1083.86

Source: Compiled and calculated in this study.

4.1.3. Structural Ratio Indicator of POEOT Analysis

In this study, the POEOT was calculated on the basis of Equation (1), and the final estimated values are summarized in Table 4.

Table 4. POEOT estimates based on equation (1)

Period	POEOT (X_1) %	POEOT (X_2) %	POEOT (X_3) %
202201	36.7603	26.9114	36.3283
202202	37.4323	36.4160	26.1518
202301	39.9567	38.1176	21.9257
202302	40.8010	30.5572	28.6419
202401	16.1485	51.5546	32.2969
202402	16.4968	33.8251	49.6781
202501	16.8945	37.4268	45.6787
202502	14.4127	27.0265	58.5608

Source: Compiled and calculated in this study.

With reference to Table 4, from 2022 to 2025, the role structure of telecommunication and online fraud in Taiwan underwent a phased and significant transformation, with distinct differences in the proportion trends of the three roles. These patterns clearly reflect the dynamic adjustments in the division of labor within fraud groups in response to law enforcement actions and policy interventions.

First, the proportion of individuals solely providing "front accounts" (X_1) initially increased but then sharply decreased and remained at low levels. From 2022 to the second half of 2023, the proportion steadily increased from 36.7603% to 40.8010%, indicating that fraud groups

heavily relied on front accounts for their operations. However, in the first half of 2024, the proportion decreased sharply to 16.1485% and subsequently stabilized at a low range of 14%–17%, declining further to 14.4127% by the second half of 2025. This trend demonstrates the effectiveness of regulatory and source-control measures targeting bank front accounts, which successfully disrupted the account supply chain and curtailed the proliferation of this type of fraud.

Second, the proportion of general telecommunication fraud perpetrators (X_2) displayed a pattern of fluctuating increase followed by a peak and subsequent decline. From 2022 to the first half of 2023, the percentage of the total population increased from 26.9114% to 38.1176%, slightly decreasing to 30.5572% in the second half of 2023. It then reached a peak of 51.5546% in the first half of 2024, becoming overwhelmingly dominant, indicating that fraud activities during this period were concentrated in the direct execution phase. Thereafter, the proportion gradually declined, reaching 27.0265% by the second half of 2025, and returned to the level observed at the beginning of the study, which reflects that direct fraud behaviors were increasingly controlled, with fraud groups shifting their focus toward more covert downstream financial operations.

Finally, the proportion of exclusive "mules" or cash-out agents (X_3) showed a pattern of continuous increase and countertrend growth, being the only category to maintain a long-term upward trajectory. Initially, the proportion was 36.3283%, declining to a low of 21.9257% during 2022–2023. From 2024 onward, it entered a rapid growth phase, surpassing 49% in the second half of 2024 and further soaring to 58.5608% by the second half of 2025, becoming the core dominant role far exceeding the other two categories. This trend indicates that as front account control intensified and direct fraud was more strictly targeted, fraud groups gradually restructured their division of labor toward downstream activities such as cash extraction, transfer, and laundering, significantly increasing the importance of mules as the core participants in telecommunication and online fraud.

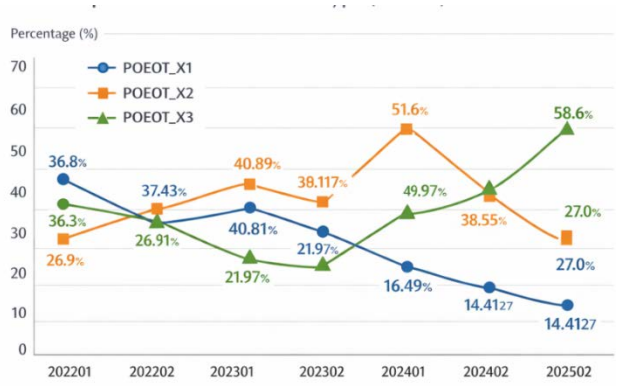

Figure 2. Trend Trajectories of the Proportions of Three Offender Roles (2022–2025)

In summary, during the study period, Taiwan's telecommunication and online fraud roles completed a structural transformation from front-account dominance to direct-fraud dominance and ultimately to mule dominance. The fraud patterns became increasingly covert and downstream oriented, presenting new challenges and strategic considerations for subsequent law enforcement efforts.

Finally, the proportions of the three roles were visualized in Figure 2 as a line chart showing trend trajectories and in Figure 3 as a percentage stacked area chart, providing an intuitive representation of their structural changes.

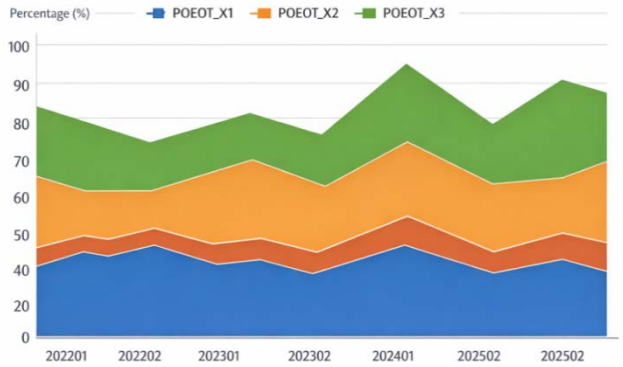

Figure 3. Percentage Stacked Area Chart of the Structural Composition of Three Offender Roles (2022–2025)

4.1.4. Analysis of Trend Dynamics Indicators

The trend dynamics indicator TABOT was computed using Equation (2), with the estimated values presented in Table 5.

Table 5 and Figure 4 present the estimated values of the trend dynamics indicator (i.e., TABOT) for the three offender roles over eight semiannual periods from 2022 to 2025. The TABOT captures the short-term growth or decline rates of each role, providing insights into dynamic structural shifts in telecommunication fraud activities.

As observed, the proportion of X_1 (Front Accounts) fluctuates substantially. In the early periods (202201–202202), no data were available for the initial period, but starting at 202202, X1 shows a rapid increase to 29.85%, followed by a sharp decrease in 202301 to 0.27%, reflecting temporary stabilization. Subsequent periods present alternating rises and declines, with a notable negative peak in 202401 (-63.80%), indicating a significant contraction, likely due to intensified regulatory interventions on bank accounts used by fraud groups.

The X2 (direct fraud) role displays a wave-like pattern, with periods of both growth and decline. After a high point of 72.55% in 202202, the value briefly becomes negative in 202301 (-1.67%), followed by moderate recovery in 202302 (-0.38%) and a strong peak in 202401 (54.32%). This trend suggests that direct fraud activities intensified temporarily but later experienced regulatory or operational constraints, resulting in fluctuating involvement across periods.

In contrast, X^3 (Mules) shows a clear rising trajectory in the latter periods. Initially, negative in 202202 (-8.20%) and 202301 (-21.24%), it experiences a substantial surge in 202302 (62.33%) and continues to increase, reaching 81.93% in 202402 and maintaining high levels through 202502 (51.36%). This pattern indicates that as upstream roles (X_1 and X_2) faced stricter control, the operational focus of fraud groups shifted downstream, increasing reliance on mules for fund collection and laundering.

Overall, the TABOT analysis highlights the dynamic and adaptive nature of telecommunication fraud operations in Taiwan. The roles exhibit alternating phases of growth and contraction, reflecting the combined effects of law enforcement pressure, policy interventions, and internal reorganization within fraud networks. X_1 and X_2 are more sensitive to regulatory actions, whereas X_3 plays a consistently growing and increasingly dominant role in later periods.

Table 5. Estimated values of the trend dynamics indicator (TABOT) based on equation (2)

Period	(X_1)	(X_2)	(X_3)
202201	-	-	-
202202	29.8472	72.5522	-8.2045
202301	0.2715	-1.6748	-21.2435
202302	26.8953	-0.3784	62.3355
202401	-63.798	54.321	3.1408
202402	20.8251	-22.4	81.9253
202501	12.5203	21.5702	1.0259
202502	0.7225	-14.7423	51.363

Source: Compiled and calculated in this study.

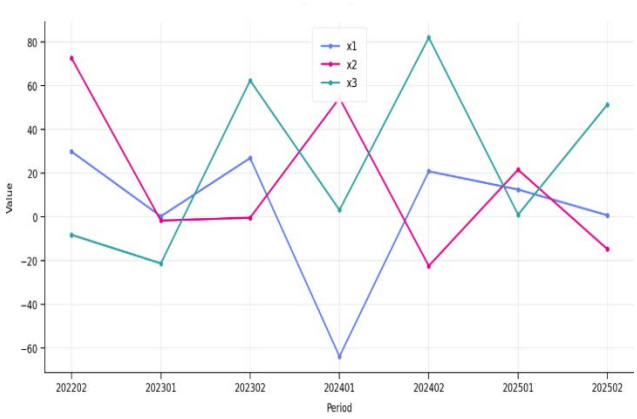

Figure 4. Trend Line of the Estimated Trend Dynamics Indicator (TABOT) (2022–2025)

4.1.5. Judicial Efficiency Indicator Analysis

In this study, the ACPC values for each period are calculated on the basis of Equation (3), and the results are summarized in Table 6 and Figure 5.

Table 6. ACPC values calculated in this study

Period	202201	202202	202301	202302	202401	202402	202501	202502
ACPC	0.1315	0.1335	0.1426	0.1411	0.2253	0.2524	0.3031	0.3837

Source: Compiled and calculated in this study.

The ACPC values computed for each period on the basis of the method in this study are shown in Table 4 and Figure 4. The results show a clear upward trend across the eight periods from 202201 to 202502. The ACPC begins at 0.1315 in 202201 and increases steadily throughout the subsequent periods. Moderate growth is observed between 202201 and 202302, with values rising from 0.1315 to 0.1411.

A more substantial increase emerges starting from 202401, when the ACPC increases sharply to 0.2253, followed by 0.2524 in 202402. The upward momentum continues into 202501 and 202502, reaching 0.3031 and ultimately peaking at 0.3837, which represents the highest recorded ACPC value in the dataset.

Overall, the results indicate a consistent and accelerating growth pattern in the ACPC over time. This suggests that the underlying factors contributing to ACPC—whether operational, behavioral, or structural—have intensified across the observed periods. The increasing trajectory implies strengthening dynamics in the measured phenomenon and offers evidence of sustained upward movement within the system analyzed.

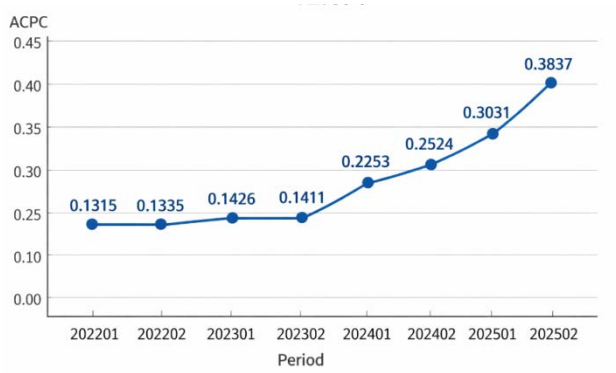

Figure 5. Trend Chart of the ACPC Values (2022–2025)

4.2. Integrated Analytical Results on Crime Structure and Judicial Efficiency

1. Evolution of Crime Structure

Between 2022 and 2025, telecommunication fraud in Taiwan underwent a clear evolution in offender roles. Initially, identity accounts (X_1) dominated, reaching 40.8% in 2023. As enforcement intensified, direct perpetrators (X_2) surged to 51.55% in the first half of 2024, becoming the primary offender group. By the second half of 2024 through 2025, criminal operations shifted toward downstream roles, with cashiers and money laundering agents (X_3) rising to 58.56%, reflecting a strategic move toward more covert financial activities.

2. Judicial efficiency and dynamic relationships

Judicial efficiency, measured by the ACPC, remained low and stable (0.13–0.14) during the initial phase but increased rapidly from 0.2253 to 0.3837 in 2024–2025, indicating strengthened investigative and prosecutorial capacity. This dynamic illustrates a displacement effect, whereby enforcement reduced X1 and X_2 proportions but redirected criminal activity toward resilient downstream roles (X_3). Simultaneously, the increase in ACPC demonstrates judicial resilience in countering evolving fraud structures. TABOT analysis revealed that X_1 was highly responsive to interventions (e.g., -63.8% in early 2024), whereas X3 exhibited strong resistance and growth potential.

3. Governance and Strategic Implications

To address the continuous evolution of digital fraud, governance strategies should adopt a collaborative approach aligned with SDG 8 (financial integrity), SDG 9 (digital infrastructure), and SDG 16 (institutional capacity). Measures include strengthening consumer protection, developing resilient digital systems, and enhancing mechanisms against organized crime and illicit

fund flows. Overall, fraud has transitioned from front-end identity accounts to downstream cashiers, while judicial efficiency has correspondingly improved, emphasizing the need for integrated approaches combining technology, education, and legal resilience.

5. Conclusion and Policy Implications

The conclusions of this study are organized into two parts, namely, conclusions and policy implications, with the aim of systematically summarizing the research findings and providing practical recommendations.

5.1. Conclusion

1. The composition of telecommunication and online fraud crimes in Taiwan has changed over time.

The overall volume of telecommunication and online fraud in Taiwan has exhibited a "rise, decline, and subsequent rebound" pattern. Early increases corresponded with the expansion of the digital environment, whereas strengthened enforcement and heightened public awareness temporarily reduced case numbers. However, as criminal networks adopted emerging technologies, fraud incidents surged again before they stabilized under recent government interventions.

2. The structural proportion of each crime role has evolved annually.

The offender role structure has undergone significant stage-based transformations, reflecting criminal networks' adaptive responses to regulatory pressure. Initially, operations relied heavily on identity accounts (X1) as the primary operational foundation. During the mid-phase, the focus shifted to direct perpetrators (X2), whose dominant role as source account controls intensified. Most recently, the structure has evolved around cashiers and money laundering agents (X3), indicating that criminal activity has migrated from front-end account provisions toward more covert downstream financial operations.

3. Law enforcement efficiency in handling these cases has increased over time.

Judicial efficiency has demonstrated continuous and accelerating growth, as measured by the ACPC indicator. This trend indicates that law enforcement and judicial agencies have increasingly strengthened their capacity to investigate, prosecute, and secure convictions in fraud cases, reflecting improved responsiveness to the evolving nature of digital crime.

4. Law enforcement strategies must adapt to ensure long-term sustainability and effectiveness.

To ensure sustainable and effective crime prevention, enforcement strategies should adopt a collaborative governance framework: aligning with the SDGs to strengthen financial integrity (SDG 8), resilient digital infrastructure (SDG 9), and institutional capacity to combat organized crime (SDG 16). Strategies should integrate multilayered measures, including technological oversight, public education, and judicial action, to reduce victimization at its source. Furthermore, policies must account for the displacement effect, whereby enforcement pressures can shift criminal activity to more resilient or covert roles, necessitating adaptive and resilient law enforcement mechanisms.

5.2. Policy Implications for Telecommunication and Online Fraud in Taiwan

On the basis of the study findings, effective policy should adopt a collaborative governance approach that integrates technological oversight, economic protection, and judicial resilience to address the evolving tactics of fraud networks. Strategies should align with the SDGs by strengthening financial integrity and consumer protection (SDG 8), promoting secure and resilient digital infrastructure (SDG 9), and enhancing institutional capacity to combat organized crime and illicit financial flows (SDG 16).

Prevention measures must be multilayered, combining the continuous regulation of digital platforms, public education to improve digital literacy and fraud awareness, and psychological defenses to reduce susceptibility to manipulation. Policies should also be adaptive to crime structure shifts, addressing the displacement of criminal activity toward downstream roles such as cashiers and laundering agents while maintaining upstream account oversight. Finally, judicial resilience should be reinforced through optimized resource allocation, efficient prosecution, and dynamic trend monitoring to ensure sustained deterrence and long-term effectiveness.

References

[1] Dadà, C. B., Colautti, L., Rosi, A., Cavallini, E., Antonietti, A., & Iannello, P. (2025). Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review. Computers in Human Behavior, 172, 108734.

[2] Junger, M., Koning, L., Hartel, P., & Veldkamp, B. (2023). In their own words: Deception detection by victims and near victims of fraud. Frontiers in Psychology, 14, 1135369.

[3] Korsell, L. (2020). Fraud in the twenty-first century. European Journal on Criminal Policy and Research, 26(3).

[4] Feedzai, & Global Anti-Scam Alliance. (2024). Global state of scams report 2024. Feedzai.

[5] Internet Crime Complaint Center (IC3). (2023). 2023 internet crime report. Federal Bureau of Investigation.

[6] Hanoch, Y., & Wood, S. (2021). The scams among us: Who falls prey and why. Current Directions in Psychological Science, 30(3), 260–266.

[7] Brenner, L., Meyll, T., Stolper, O., & Walter, A. (2020). Consumer fraud victimization and financial well-being. Journal of Economic Psychology, 76, 102243.

[8] Ueno, D., Arakawa, M., Fujii, Y., Amano, S., Kato, Y., Matsuoka, T., & Narumoto, J. (2022). Psychosocial characteristics of victims of special fraud among Japanese older adults: A cross-sectional study using scam vulnerability scale. Frontiers in Psychology, 13, 960442.

[9] Sarriá, E., Recio, P., Rico, A., Díaz-Olalla, M., Sanz-Barbero, B., Ayala, A., & Zunzunegui, M. V. (2019). Financial fraud, mental health, and quality of life: A study on the population of the city of Madrid, Spain. International Journal of Environmental Research and Public Health, 16(18), 3276.

[10] Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted love: A systematic literature review of online romance scam research. Interacting with Computers, 35(6), 773–788.

[11] Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. IEEE Access, 9, 44928–44949.

[12] Su, Y., Shih, C. H., & Yang, T. J. O. (2024). Investment fraud cases study in Chinese context of instant messaging software. Procedia Computer Science, 246, 391–402.

[13] Ministry of Justice. (2025). Statistics on telecom and online fraud cases handled by district prosecutors' offices (June 2021–June 2025). Ministry of Justice, Taiwan.

[14] Ministry of Justice, R.O.C. (Taiwan). (2025). Statistical data on telecommunication and online fraud cases investigated, proportion of new cases, concluded investigations, and finalized convictions. Ministry of Justice Statistical Information Network.