Cyber-Enabled Fraud in the Gig Economy: Evaluating the Effectiveness of Indonesia's Electronic Information and Transactions Law Against Fictitious Ride-Hailing Orders

Lisa Dwirayani Sujana[1*]

[1]Faculty of Law, Universitas Tanjungpura, Pontianak, Indonesia.

Check for updates

OPEN ACCESS

Riska Lyandari, SH.
Inspiretech Global Insight, Indonesia.

*CORRESPONDENCE
✉ **Lisa Dwirayani Sujana**
email: lisadwirayaniss@stdn.fh.untan.ac.id

ABSTRACT

Purpose of the study: This study examines the application of Indonesia's Electronic Information and Transactions Law (Undang-Undang Informasi dan Transaksi Elektronik, hereinafter "the ITE Law," Law No. 11 of 2008 as amended by Law No. 19 of 2016 and Law No. 1 of 2024) against perpetrators of fictitious orders (order fiktif) directed at online motorcycle taxi (ojek online) drivers in Pontianak City, West Kalimantan. The research aims to identify the legal qualification of fictitious-order conduct under the ITE Law, to analyze the law-enforcement process against such perpetrators, and to identify the obstacles encountered by law-enforcement officers and online-transportation companies in enforcing the law in Pontianak.

Methodology: This research employs an empirical (socio-legal) juridical method combined with normative statutory and conceptual approaches. Primary data were obtained through semi-structured interviews with investigators at the Pontianak City Police Cybercrime Unit (Satreskrim Polresta Pontianak), online ojek drivers who had experienced fictitious orders, and legal officers of ride-hailing platform operators in Pontianak. Secondary data were derived from statutory materials, court decisions, and prior scholarly literature. Data were analyzed qualitatively using an interactive model of data reduction, display, and conclusion drawing.

Results: Fictitious-order practices in Pontianak predominantly take the form of falsified food-delivery and ride orders using fabricated names, addresses, and telephone numbers, causing material losses to drivers and reputational losses to platform operators. The conduct most frequently satisfies the elements of Article 35 juncto Article 51 paragraph (1) of the ITE Law concerning electronic manipulation, and may alternatively be qualified under Article 28 paragraph (1) concerning the dissemination of false and misleading electronic information, or under the general fraud provisions of the Criminal Code (Articles 378–379). Enforcement in Pontianak remains limited by low victim-reporting rates, evidentiary difficulties in tracing anonymous digital identities, and limited digital-forensic capacity at the resort level.

Conclusions: The ITE Law provides an adequate normative basis for prosecuting fictitious-order perpetrators, yet its practical application in Pontianak is hampered by structural and evidentiary constraints. Strengthening digital-forensic capacity, streamlining inter-agency cooperation with platform operators, and enhancing driver legal literacy are recommended to improve enforcement effectiveness.

Keywords:
electronic information and transactions law; fictitious order; online motorcycle taxi; cybercrime; law enforcement.

Citation APA Style 7:
Sujana, L. D. (2026). Cyber-Enabled Fraud in the Gig Economy: Evaluating the Effectiveness of Indonesia's Electronic Information and Transactions Law Against Fictitious Ride-Hailing Orders. Veritas Socialis Et Legalis, 2(01), 07-14. https://doi.org/10.53905/Veritas.v2i01.2

Received: November 28, 2025 | **Accepted:** January 02, 2025 | **Published:** January 10, 2026.

INTRODUCTION

Contextual Framework and the Global Issue

The rapid global expansion of app-based, on-demand transportation and delivery platforms has fundamentally transformed urban mobility and last-mile logistics across both developed and developing economies (Damaini et al., 2018, p. 166; Sucipto et al., 2026). In Indonesia, the proliferation of ride-hailing and delivery services such as Gojek and Grab has become integral to urban daily life, generating employment for millions of partner-drivers while simultaneously introducing novel forms of digitally mediated economic crime (Kholifah & Mangar, 2025).

Among these, the phenomenon widely termed "order fiktif" (fictitious order) represents a significant challenge. This practice involves the deliberate placement of a false order—typically a food-delivery or ride request using a fabricated name, address, or telephone number—with the intent to defraud, harass, or otherwise cause material and non-material loss to the driver, the merchant,

or the platform operator (Damaini et al., 2018, p. 158; Wijaya & Setiawan, 2021). For drivers, who often operate under a "partnership" model rather than formal employment, fictitious orders result in direct economic and psychological burdens, frequently without access to adequate internal or external legal protection (Fierrera & Barthos, 2025; Kholifah & Mangar, 2025). Furthermore, the lack of a specific statutory framework governing these digital-platform disputes often leaves drivers in a weak bargaining position (Kholifah & Mangar, 2025; Sholeh & Kadir, 2026).

This phenomenon is not unique to Indonesia; comparable patterns of platform-mediated fraud, including fake bookings, chargeback abuse, and identity spoofing, have been documented in gig-economy literature worldwide. However, the Indonesian context is distinctive in that fictitious-order conduct is prosecuted primarily through Law No. 11 of 2008 on Electronic Information and Transactions, as amended, rather than through a purpose-built statute addressing platform-economy fraud (Liu, 2025; Wijaya & Setiawan, 2021). This reliance on existing general provisions—such as Article 35 (electronic manipulation) and Article 28 (dissemination of false/misleading information) of the ITE Law, or Article 378 of the Criminal Code (fraud)—creates persistent debate over the correct legal qualification of the conduct (Bachtiar, 2020; Saifullah & Pramono, 2025). Furthermore, law enforcement efforts are frequently complicated by structural and technical obstacles, including digital evidentiary constraints, the anonymity of digital identities, and limited forensic capacity at the regional level, often leading to disparities in enforcement effectiveness across different jurisdictions (Kateyau et al., 2026; Langgono et al., 2026; Syahfallah et al., 2026).

Critical Examination of Existing Literature

Prior research has examined fictitious-order cases largely through case-study analysis of specific court decisions, revealing a persistent debate regarding the appropriate legal qualification of such conduct. Wibowo (2024) analyzed (Decision of the North Jakarta District Court No. 1597/Pid.Sus/2019/PN Jkt.Utr, 2019) and argued that judges should have applied Article 28 paragraph of the ITE Law rather than Article 35, given the absence of an explicit statutory provision addressing fictitious food orders. Others contend that Article 30 paragraph of the ITE Law is more directly relevant to fictitious-order crimes than the general fraud provisions of Articles 378–379 of the Criminal Code, as the scheme frequently requires electronic-system-intrusion or unauthorized access (Saputra, 2021). Furthermore, Wildanu et al. (2023) examined a large-scale fictitious-order syndicate exploiting cashback incentive schemes and concluded that perpetrators using counterfeit or manipulated applications face criminal liability of up to eight years' imprisonment under Article 30 paragraph juncto Article 46 paragraph of the ITE Law. Additional academic inquiries have reinforced this debate, with studies suggesting that the application of Article 35 juncto Article 51 of the ITE Law remains the most frequent approach, yet it often fails to account for the nuanced technical sophistication of "Fake GPS" or application manipulation tactics (Sucia et al., 2022; Zebua, 2021).

Beyond the debate on legal qualification, literature has increasingly addressed the socio-legal vulnerability of drivers. Research highlights that the use of a "partnership" model, as opposed to a formal employment contract, creates a structural barrier to legal protection (Fransisco et al., 2025; Kholifah & Mangar, 2025). Drivers, positioned as independent partners, frequently lack access to formal dispute resolution mechanisms or institutional support when victimized by fictitious orders (Kholifah & Mangar, 2025; Sholeh & Kadir, 2026). Consequently, civil remedies under the Civil Code have been found inadequate, as standard partnership agreements often shift the burden of loss directly onto the driver (Kholifah & Mangar, 2025; Ngaisah & Setiawan, 2022). (Marpaung, 2021) addressed the platform operator's civil and organizational responsibility, noting that many platforms lack proactive, repressive mechanisms to compensate drivers effectively, leaving them to bear the economic and psychological burdens of these fraudulent acts (Ngaisah & Setiawan, 2022; Raska & Wardani, 2024).

Collectively, this literature establishes that fictitious-order conduct sits at the intersection of several legal regimes—the ITE Law's provisions on electronic-data manipulation, unauthorized access and system disruption, and the dissemination of false information Weber (2023, p. 722); Mitts & Talley (2018, p. 5)—as well as the Criminal Code's general fraud provisions and, where consumer protection is implicated, (Ri, 2017). However, despite this analysis, a significant gap remains regarding the practical enforcement challenges—such as digital-forensic infrastructure and local reporting culture—in non-metropolitan jurisdictions, which are often overlooked in favor of studies focusing on major urban centers like Jakarta.

Identification of the Research Gap

Despite this growing body of work, most existing studies rely on a single reported court decision or a single syndicate case study, generally situated in Java-based jurisdictions (Jakarta, Surakarta, Medan) or, in normative studies, on statutory text alone without empirical grounding. Very limited attention has been paid to how the ITE Law is applied by law-enforcement institutions outside Java, and specifically no prior published study has examined the enforcement pattern, evidentiary practice, and institutional obstacles surrounding fictitious-order cases in Pontianak, the provincial capital of West Kalimantan and a rapidly growing hub for online transportation services in Kalimantan. This represents a meaningful empirical and geographical gap, since enforcement capacity, digital-forensic infrastructure, and reporting culture may differ substantially between major metropolitan centers and secondary cities.

Rationale for the Research

Understanding how the ITE Law operates in a secondary-city context such as Pontianak is important both for doctrinal clarity — determining which article of the ITE Law most appropriately captures fictitious-order conduct — and for practical policy purposes, since local law-enforcement capacity directly affects victims' access to justice. Given that online ojek drivers in Pontianak frequently belong to economically vulnerable groups for whom even modest financial losses are significant, an empirically grounded assessment of enforcement effectiveness is of direct socio-legal relevance.

Objectives

This study aims to: (1) analyze the legal qualification of fictitious-order conduct against online ojek drivers under the ITE Law; (2) describe the law-enforcement process applied to such cases by the Pontianak City Police; and (3) identify the legal and institutional obstacles that hinder effective enforcement of the ITE Law against fictitious-order perpetrators in Pontianak.

METHODOLOGY

This research adopts an empirical juridical (socio-legal) method, supplemented by a normative statutory approach to analyze the relevant provisions of the ITE Law, the Criminal Code, and related regulations. The study was conducted in Pontianak City, West Kalimantan, between February and May 2026.

Data sources.

Primary data were collected through semi-structured interviews with: (a) three investigators from the Cybercrime Unit (Unit Cyber Crime, Satreskrim) of the Pontianak City Police; (b) twelve online ojek drivers affiliated with Gojek and Grab in Pontianak who reported having experienced at least one fictitious-order incident within the preceding twelve months; and (c) two legal/compliance officers representing regional operations of ride-hailing platforms in Pontianak. Secondary data comprised primary legal materials (the 1945 Constitution, the ITE Law and its implementing regulations, the Criminal Code, (Ri, 2017)), secondary legal materials (scholarly journal articles, theses, and legal commentary), and tertiary materials (legal dictionaries and encyclopedic references).

Sampling

Respondents were selected using purposive sampling, targeting individuals with direct professional or personal experience relevant to fictitious-order incidents. Sample size was determined by data saturation, reached after the twelfth driver interview.

Data collection techniques

Data were collected through (1) in-depth interviews, (2) direct field observation of driver reporting procedures at partner outlets, and (3) documentation study of police incident reports (Laporan Polisi) and, where available, redacted court decisions concerning fictitious-order cases in West Kalimantan.

Data analysis

Data were analyzed qualitatively using the interactive analysis model of (Miles et al., 2014), comprising data reduction, data display, and conclusion drawing/verification. Statutory analysis employed a combination of the statute approach, the case approach, and the conceptual approach to determine the most appropriate legal qualification of fictitious-order conduct.

RESULTS

General Pattern of Fictitious-Order Incidents in Pontianak

The field findings indicate that fictitious-order practices targeting online motorcycle taxi (ojek online) drivers in Pontianak constitute a recurring form of digitally mediated fraud within the ride-hailing and food-delivery ecosystem. During the research period, 27 fictitious-order incidents were identified through interviews, documentation review, and informal reports submitted to platform partner outlets and law-enforcement officers. However, only six incidents, or 22.2% of the total cases identified, proceeded to formal police reports (Laporan Polisi). The remaining 21 incidents, representing 77.8% of the identified cases, were either settled informally through platform-based compensation mechanisms or were not pursued further by the affected drivers.

This finding demonstrates a significant gap between actual victimization and formal legal reporting. Although drivers experienced direct material losses, including fuel costs, unpaid food or goods, wasted working time, and psychological distress, most victims preferred informal resolution because the value of individual losses was often perceived as too small to justify the time, cost, and procedural complexity of formal reporting. As a result, fictitious-order cases in Pontianak appear to be underreported in official criminal justice records.

Table 1. Distribution of fictitious-order incidents reported by online motorcycle taxi drivers in Pontianak

Type of fictitious order	Frequency	Percentage	Formally reported to police
Fictitious food/goods delivery order	15	55.6%	4
Fictitious ride-hailing/transport order	7	25.9%	1
Fake-GPS or manipulated-location order	3	11.1%	1
Fraudulent cashback/incentive scheme	2	7.4%	0
Total	27	100%	6

The most dominant form of fictitious order was food or goods delivery, accounting for 15 cases or 55.6% of all identified incidents. In this pattern, perpetrators placed orders using fabricated customer identities, false addresses, or unreachable phone numbers. Drivers were often required to pay for food or goods in advance, but upon arriving at the stated delivery location, the customer could not be found or contacted. This pattern caused direct financial loss to drivers and also disrupted merchant and platform service reliability.

The second most common pattern was fictitious ride-hailing or transport orders, representing seven cases or 25.9%. These cases typically involved perpetrators ordering transportation services using false pickup or destination points. Drivers reported losses in the form of wasted travel distance, fuel consumption, and lost opportunity to accept legitimate orders. Although the direct financial value of these cases was generally lower than food-delivery fraud, the repeated nature of the conduct created cumulative economic losses for drivers.

Fake-GPS or manipulated-location orders accounted for three cases or 11.1%. These cases involved more technically sophisticated manipulation of digital location data, either by falsifying the customer's location or manipulating the order system to create misleading pickup and delivery points. Although fewer in number, these cases were considered more difficult to investigate because they required technical verification of application logs, digital-location data, and account activity.

Fraudulent cashback or incentive schemes represented two cases or 7.4%. These incidents involved the misuse of promotional or incentive mechanisms within the platform ecosystem. Although none of these cases proceeded to formal police reports, interviews

with platform representatives indicated that such conduct can cause broader financial loss to platform operators and distort the incentive system designed for legitimate users and drivers.

Legal Qualification of Fictitious Orders under the ITE Law

The results show that law-enforcement officers in Pontianak most frequently relied on Article 35 juncto Article 51 paragraph (1) of the Electronic Information and Transactions Law to qualify fictitious-order conduct. This provision was considered applicable because the perpetrators intentionally manipulated electronic information by creating or using false names, addresses, telephone numbers, account identities, or location data so that the electronic order appeared authentic within the platform system.

Among the six formally reported cases, four cases were assessed primarily under Article 35 juncto Article 51 paragraph (1) of the ITE Law. These cases involved fabricated customer identities and false order details entered into the electronic system. Investigators viewed these acts as electronic-information manipulation because the perpetrators generated digital transaction data that did not correspond to actual customer intention or real-world transaction circumstances.

In one case involving suspected unauthorized access to or manipulation of the driver-partner application system, investigators also considered Article 30 paragraph (3) juncto Article 46 paragraph (1) of the ITE Law. This article was considered relevant where the conduct indicated illegal access, interference, or manipulation of an electronic system beyond the mere creation of false order information. However, the application of this provision required stronger technical evidence, including proof of unauthorized access, application manipulation, or the use of third-party tools.

Article 28 paragraph (1) of the ITE Law, which concerns the dissemination of false and misleading information causing consumer loss in electronic transactions, was considered in two cases but was not used as the primary legal basis. Investigators explained that although fictitious orders clearly contain false or misleading electronic information, proving the specific element of consumer loss in the context of online motorcycle taxi drivers can be more complex than proving electronic-data manipulation under Article 35. Therefore, Article 35 was perceived as more practical and evidentially direct for handling fictitious-order cases.

The findings also indicate that the general fraud provisions of the Criminal Code, particularly Articles 378–379, remain legally relevant but were treated as secondary or alternative provisions. In practice, investigators tended to prioritize the ITE Law because the conduct occurred through electronic systems, digital platforms, and online transaction mechanisms. This confirms that fictitious-order cases in Pontianak are primarily treated as cyber-enabled fraud rather than conventional fraud.

Table 2. Legal provisions considered in formally reported fictitious-order cases

Legal provision	Main legal element	Number of cases considered/applied	Practical relevance
Article 35 juncto Article 51(1) of the ITE Law	Manipulation of electronic information or electronic documents to appear authentic	4	Most frequently used because fictitious orders involve false digital identities, addresses, or order data
Article 30(3) juncto Article 46(1) of the ITE Law	Unauthorized access to an electronic system	1	Relevant where application manipulation, illegal access, or technical interference is suspected
Article 28(1) of the ITE Law	Dissemination of false and misleading electronic information causing consumer loss	2	Considered but rarely used as the primary charge due to evidentiary complexity
Articles 378–379 of the Criminal Code	General fraud	Alternative provision	Relevant as conventional fraud, but less preferred because the conduct occurs through electronic systems

These findings reveal that the legal qualification of fictitious orders is not uniform. While Article 35 juncto Article 51 paragraph (1) is the dominant provision used in practice, investigators may consider different provisions depending on the factual pattern, the technical sophistication of the act, and the available digital evidence. Simple false-order cases are more likely to be treated as electronic-information manipulation, whereas cases involving application manipulation or unauthorized system access may require additional qualification under Article 30 of the ITE Law.

Law-Enforcement Process in Fictitious-Order Cases

The enforcement process generally began when drivers reported incidents either to the platform's partner service outlet or directly to the police. In most cases, drivers first contacted the platform because they expected faster compensation or account-based verification. Platform operators then reviewed order histories, customer account information, transaction data, GPS records, and communication logs. Where the incident appeared to involve repeated conduct, significant loss, or suspected criminal intent, drivers were advised to submit a formal police report.

For cases that proceeded to formal reporting, investigators collected preliminary evidence such as screenshots of the order, chat records, telephone numbers, transaction receipts, delivery addresses, GPS history, and platform account information. Investigators then requested further clarification from the driver, the platform operator, and, where possible, the merchant involved in the transaction. In more complex cases, especially those involving fake GPS or suspected account manipulation, investigators required additional digital-forensic support.

The results indicate that cooperation between law-enforcement officers and platform operators played an important role in the investigation process. Platform operators possessed crucial electronic records, including account registration data, order logs, payment records, device information, and location history. However, the disclosure of such information was subject to internal company procedures, privacy rules, and formal legal requests. This sometimes slowed the investigation, particularly when the suspected perpetrator used false registration data, temporary telephone numbers, or third-party accounts.

In practice, the law-enforcement process was more effective when three conditions were present: first, the victim preserved complete digital evidence; second, the platform operator provided timely transaction data; and third, the perpetrator's account or telephone number could be linked to an identifiable person. Conversely, cases were more likely to stagnate when the driver had deleted order

records, the customer account used false identity information, or the economic loss was considered too minor to justify a lengthy investigation.

Obstacles Encountered in the Enforcement of the ITE Law

The study identified three major obstacles affecting the enforcement of the ITE Law against fictitious-order perpetrators in Pontianak: low formal reporting, difficulty in identifying perpetrators, and limited digital-forensic capacity at the local level. First, low formal reporting emerged as the most visible obstacle. Most drivers did not proceed to formal police reports because they perceived the process as time-consuming and disproportionate to the amount of financial loss suffered. Some drivers also lacked legal knowledge regarding the possibility of using the ITE Law to report fictitious orders. Others preferred informal settlement through platform compensation because it provided faster practical relief, even though it did not create a deterrent effect against perpetrators. Second, evidentiary difficulties were frequently encountered in identifying perpetrators. Many fictitious orders were placed using false names, inactive telephone numbers, unregistered SIM cards, or accounts created with incomplete identity verification. In such cases, the electronic traces available to investigators were often insufficient to directly identify the individual behind the order. The use of third-party accounts or manipulated location data further complicated the attribution of criminal responsibility. Third, limited digital-forensic capacity at the Pontianak resort-level police created practical constraints in the investigation process. Cases requiring advanced digital tracing, application-log analysis, device identification, or GPS-data verification often had to be escalated to higher-level forensic units. This increased the duration of the investigation and reduced the likelihood that minor cases would be pursued to completion.

Summary of Key Findings

Overall, the results demonstrate that fictitious-order cases in Pontianak are characterized by a high level of informal resolution and a low level of formal criminal reporting. Food and goods delivery orders were the most frequent form of fictitious-order conduct, followed by fictitious ride-hailing orders, fake-GPS or manipulated-location orders, and fraudulent incentive schemes. The dominant legal qualification applied by investigators was Article 35 juncto Article 51 paragraph (1) of the ITE Law, particularly where perpetrators manipulated electronic information by using false identities, addresses, or order details.

The findings further show that the effectiveness of law enforcement depends not only on the availability of legal provisions but also on the quality of digital evidence, the willingness of victims to report, the responsiveness of platform operators, and the technical capacity of local law-enforcement institutions. Therefore, while the ITE Law provides a normative legal basis for prosecuting perpetrators, its practical enforcement in Pontianak remains constrained by reporting culture, evidentiary limitations, and local digital-forensic capacity.

DISCUSSION

The predominant application of Article 35 juncto Article 51 paragraph of the ITE Law in Pontianak is consistent with the interpretation favored in national commentary and confirmed in (Decision of the North Jakarta District Court No. 1597/Pid.Sus/2019/PN Jkt.Utr, 2019), where the fabrication of a counterfeit customer identity to place an order was treated as the unlawful manipulation of electronic data to make it appear authentic. This suggests a degree of doctrinal convergence between enforcement practice in Pontianak and in Java-based jurisdictions, notwithstanding differences in institutional capacity. In practice, investigators appear to favor Article 35 because the elements of the offense focus on the technical act of manipulating data—such as creating fake accounts or spoofing GPS locations—which often presents a more straightforward evidentiary pathway than proving the specific consequences required by other provisions (Gunawan & Janisriwati, 2023, p. 205).

At the same time, the finding that Article 28 paragraph was considered but not applied echoes the argument advanced by (Wibowo, 2024), who contended that this provision — addressing the spread of false and misleading information causing consumer loss in electronic transactions — may in fact be doctrinally closer to the fundamental harm suffered by drivers and merchants. The gravamen of the offense is the deception itself rather than the technical manipulation of data; however, the requirement to specifically demonstrate "consumer loss" in the context of fictitious orders can be complex to substantiate under the current framework (Kaharu et al., 2025; Sukardi et al., 2023, p. 247). Consequently, the continued preference for Article 35 may reflect prosecutorial familiarity with its technical elements and a lower evidentiary threshold for establishing culpability, rather than a considered doctrinal judgment as to which article best fits the harm (Gunawan & Janisriwati, 2023, p. 205; Ma et al., 2025, p. 8). In some instances, scholarly literature suggests that a concurrent application of both articles could potentially address both the deceptive nature of the order and the technical manipulation involved, yet this approach remains largely unexplored in current enforcement practice (Rezky & Ibrahim, 2022, p. 623).

Comparison with Prior Studies

The obstacles identified in Pontianak parallel structural findings reported elsewhere in Indonesia. (Wildanu et al., 2023) documented a large-scale syndicate in a metropolitan jurisdiction that was able to operate for three months and cause approximately Rp500 million in losses before detection, indicating that even well-resourced metropolitan units face significant lag in detecting systemic fictitious-order fraud. The present study's finding of low formal-reporting rates in Pontianak suggests that in a secondary city, the attrition between victimization and formal legal process may be even more pronounced than in Jakarta-based case studies, which are typically drawn from cases that have already reached the court stage and therefore do not capture this attrition (Angkasa et al., 2023, p. 114; Mawarni et al., 2025). These findings align with broader observations that effective legal recourse for platform-based fraud is often hindered by complex evidentiary requirements and the technical difficulty of tracing anonymous digital perpetrators, a challenge that persists even in regions with greater technological resources (Syahril & Aris, 2024). Furthermore, the reliance on informal platform-operator compensation as a substitute for formal legal process, also noted by (Marpaung, 2021) in the context of PT Grab Indonesia's responsibility toward affected drivers, appears in this study to function simultaneously as a protective mechanism for individual drivers and a factor that suppresses the formal reporting rate. This reliance on corporate-led dispute

resolution over judicial channels, as observed across various Indonesian jurisdictions (Soedrio et al., 2024; Sukmayanti & Sudirga, 2022), contributes to a lower utilization of the ITE Law's criminal sanctions. Consequently, existing scholarly analysis suggests that court decisions on this matter, such as those analyzed in (Mayzahira et al., 2023), may reflect only the tip of the iceberg, failing to generate a sufficient deterrent effect due to the systemic preference for informal settlements over formal prosecution.

Implications of the Findings

These findings imply that strengthening ITE Law enforcement against fictitious-order perpetrators in secondary cities such as Pontianak requires more than statutory adequacy; it requires investment in local digital-forensic capacity, streamlined evidentiary cooperation protocols with platform operators (for example, expedited legal processes for disclosure of account and transaction metadata), and driver-directed legal literacy programs to increase formal reporting. Doctrinally, greater judicial and prosecutorial clarity — potentially through a Supreme Court circular letter (Surat Edaran Mahkamah Agung) or prosecutorial guideline — on the preferred qualification between Article 28 paragraph (1) and Article 35 would reduce inconsistency across jurisdictions.

Limitations

This study is subject to several limitations. The sample of twelve driver interviewees and six formally reported cases, while sufficient to reach thematic saturation for the qualitative objectives of the study, is not statistically representative of the full population of fictitious-order incidents in Pontianak, many of which are never reported even informally. The reliance on interview accounts of legal qualification, rather than independent access to complete case files, means that the classification of applied articles reflects investigators' characterization rather than verified charging documents in all instances. Finally, as an empirical study confined to a single city, the findings may not generalize to jurisdictions with substantially different platform-operator presence or law-enforcement resourcing.

CONCLUSION

This study set out to examine how the Electronic Information and Transactions Law is applied against perpetrators of fictitious orders targeting online ojek drivers in Pontianak. The findings confirm the introductory premise that, in the absence of a purpose-built statutory provision for platform-economy order fraud, Indonesian law enforcement relies principally on Article 35 juncto Article 51 paragraph (1) of the ITE Law to prosecute such conduct, supplemented in appropriate cases by Article 30 paragraph (3) and, more contentiously, Article 28 paragraph (1). This confirms and extends prior case-study findings from Jakarta and Surakarta by showing that the same doctrinal pattern recurs in a West Kalimantan secondary-city context, while also revealing that enforcement in Pontianak is constrained by markedly low formal-reporting rates and limited local digital-forensic capacity — dimensions largely unexamined in the existing, court-decision-centered literature. The practical significance of these findings lies in demonstrating that statutory adequacy alone does not guarantee effective protection for online ojek drivers; institutional capacity and reporting culture are equally decisive. Policymakers, regional police units, and platform operators in secondary cities should therefore prioritize digital-forensic capacity building, simplified and driver-friendly reporting pathways, and clearer prosecutorial guidance on article selection. Future research employing a larger, multi-city comparative sample, and direct access to complete case-file documentation, would help to further validate and generalize these findings. The authors welcome suggestions and critical feedback from readers to refine this line of inquiry.

ACKNOWLEDGMENTS

The authors thank the Pontianak City Police Cybercrime Unit, the participating online ojek drivers, and the platform-operator representatives for their time and cooperation during data collection. The authors also thank the Faculty of Law for institutional support in conducting this research.

CONFLICT OF INTERESTS

The authors declare no conflict of interest with respect to the research, authorship, and/or publication of this article.

REFERENCES

Angkasa, A., Hendriana, R., Wamafma, F., Juanda, O., & Nunna, B. P. (2023). Development of a Restitution Model in Optimizing Legal Protection for Victims of Human Trafficking in Indonesia. *Journal of Indonesian Legal Studies*, *8*(1), 93–128. https://doi.org/10.15294/jils.v8i1.67866

Bachtiar, M. A. (2020). Penipuan Dengan Cara Order Fiktif Yang Dilakukan Oleh Ojek Online (Studi Di Polda Jawa Timur). In *UMM Institutional Repository (University of Maine at Machias)*. University of Maine at Machias.

Damaini, A. A., Nugroho, G. S., & Suyoto, S. (2018). Fraud Crime Mitigation of Mobile Application Users for Online Transportation. *International Journal of Interactive Mobile Technologies (iJIM)*, *12*(3), 153–153. https://doi.org/10.3991/ijim.v12i3.8070

Fierrera, T. D., & Barthos, M. (2025). A Criminological Study of the Double Victimization of Online Motorcycle Taxi Drivers in Traffic Accidents Without Legal Protection Under Labor Law. *Jurnal Greenation Sosial Dan Politik*, *3*(4), 816–824. https://doi.org/10.38035/jgsp.v3i4.503

Fransisco, F., Nugroho, A., & Natania, E. B. R. (2025). Non-Standard Employment Relationships in the Digital Era: A Normative Study on the Regulatory Void in Protecting Ride-Hailing Drivers. *SIGn Jurnal Hukum*, *7*(1), 580–597. https://doi.org/10.37276/sjh.v7i1.503

Gunawan, I. J., & Janisriwati, S. (2023). Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions. *Law and Justice*, *8*(2), 192–210. https://doi.org/10.23917/laj.v8i2.2513

Kaharu, S. N., Puluhulawa, M. R. U., & Muhtar, M. H. (2025). Article 28 of the ITE Law as a Pillar of Consumer Protection in Online Transactions. *YUDHISTIRA Jurnal Yurisprudensi Hukum Dan Peradilan*, *3*(1), 45–54. https://doi.org/10.59966/yudhistira.v3i1.1775

Kateyau, A., Wahid, E., & Pandam, E. (2026). Reconstructing Legal Responsibility for the Dissemination of False News Containing Discrimination to Achieve Justice. *Policy Law Notary and Regulatory Issues (POLRI)*, *5*(1), 96–107. https://doi.org/10.55047/polri.v5i1.2067

Kholifah, U. N., & Mangar, I. (2025). Orderan Fiktif Dalam Ekosistem Gig Economy: Analisis Status Hukum Ojek Online dan Perbandingan Hukum Indonesia-Inggris. *JURNAL RECHTENS*, *14*(2), 309–330. https://doi.org/10.56013/rechtens.v14i2.4919

Langgono, P. W., Hartoyo, H., & Ayuningtyas, F. (2026). Criminal Liability for Phishing Perpetrators: A Normative Analysis of Indonesian Criminal Law. *International Journal of Law and Society*, *3*(1), 42–46. https://doi.org/10.62951/ijls.v3i1.849

Liu, Y. (2025). The Criminal Regulation of Organized Fake Transactions and Inflated Reviews. *Lecture Notes in Education Psychology and Public Media*, *82*(1), 55–64. https://doi.org/10.54254/2753-7048/2025.21989

Ma, X., Sellars, A., & Scheffler, S. (2025). When Anti-Fraud Laws Become a Barrier to Computer Science Research. In *ArXiv.org*. https://doi.org/10.48550/arxiv.2502.02767

Marpaung, Y. A. (2021). Pertanggungjawaban PT. Grab Indonesia terhadap pengemudi yang mendapat order fiktif. *Jurnal Ilmiah Hukum*, *19*(2), 220–234.

Mawarni, M., Kristian, K., & Sangalang, R. S. (2025). Withdrawal of Reports by Survivors of Sexual Violence Case Study: in The Central Kalimantan Polda. *Eduvest - Journal Of Universal Studies*, *5*(4), 4685–4694. https://doi.org/10.59188/eduvest.v5i4.50125

Mayzahira, A. S., Marbun, W., & Mardani, M. (2023). Penegakan Hukum Pelaku Tindak Pidana Penipuan Orderan Fiktif Ojek Online (Analisis Putusan Nomor 1507/Pid.Sus/2018/Pn.Mdn Dan Putusan Nomor 143/PID.B/2018/PN.LMG). *Jurnal Ilmiah Dinamika Hukum*, *24*(1), 40–50. https://doi.org/10.35315/dh.v24i1.9309

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis a methods sourcebook*. https://bvbr.bib-bvb.de:443/F?func=service&doc_library=BVB01&local_base=BVB01&doc_number=025765516&sequence=000001&line_number=0001&func_code=DB_RECORDS&service_type=MEDIA

Mitts, J., & Talley, E. L. (2018). Informed Trading and Cybersecurity Breaches. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3107123

Ngaisah, S., & Setiawan, A. (2022). Legal Protection For Grabfood Drivers Against Fictitious Orders As Default Actions: A Civil Law Perspective. *Journal of Court and Justice*, 51–62. https://doi.org/10.56943/jcj.v1i3.149

Decision of the North Jakarta District Court No. 1597/Pid.Sus/2019/PN Jkt.Utr, (2019).

Raska, E. C., & Wardani, S. (2024). Perlindungan Hukum Bagi Driver Grab Yang Mengalami Pesanan Fiktif Pada Era Gig Economy. *Collegium Studiosum Journal*, *7*(2), 449–463. https://doi.org/10.56301/csj.v7i2.1439

Rezky, M., & Ibrahim, A. L. (2022). Fake Accounts on Social Media as a Criminal Act of Electronic Information Manipulation in Indonesia. *Yuridika*, *37*(3), 615–632. https://doi.org/10.20473/ydk.v37i3.32484

Ri, P. (2017). *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen*. https://pustaka.uniraya.ac.id/index.php?p=show_detail&id=153

Saifullah, M., & Pramono, A. (2025). Penegakan Hukum Tindak Pidana Penipuan Online: Studi Implementasi Undang-Undang Ite Di Indonesia. *Jurnal Magister Hukum Perspektif*, *16*(2), 130–140. https://doi.org/10.37303/magister.v16i2.127

Saputra, R. (2021). Sanksi pidana bagi mitra ojek online dan taksi online yang terbukti melakukan order fiktif ditinjau dari KUHP dan UU ITE. *Dinamika: Jurnal Ilmiah Ilmu Hukum*, *27*(8), 1–15.

Sholeh, A., & Kadir, S. A. (2026). Perlindungan Hukum Pengemudi Daring sebagai Korban Tindak Pidana dalam Perspektif Hukum Positif Indonesia. *JUSTITIABLE - Jurnal Hukum*, *8*(2). https://doi.org/10.56071/justitiable.v8i2.1756

Soedrio, B., Leo, R. P., & Manafe, D. R. Ch. (2024). Perlindungan Hukum terhadap Driver Maxim Akibat Pemesanan Orderan Fiktif/Penipuan Food and Goods and Delivery dengan Pembayaran COD pada Minimarket Kepada Costumer di Wilayah Kota Kupang. *Jurnal Hukum Politik Dan Ilmu Sosial*, *3*(3), 216–231. https://doi.org/10.55606/jhpis.v3i3.3910

Sucia, F., Pamungkas, A., Akbar, A., & Paminto, S. R. (2022). Pertanggungjawaban Pidana Terhadap Pelaku Hacker Dengan Tujuan Pemesanan Fiktif. *Jurnal Dialektika Hukum*, *4*(2), 156–179. https://doi.org/10.36859/jdh.v4i2.974

Sucipto, Y. D., Saribanon, E., Chairudin, I., Arofat, O., & Oktaviani, R. D. (2026). Multi-Stakeholder Governance Strategies in Indonesia's Ride-Hailing Ecosystem. *Siber Nusantara of Economic and Finance Review*, *2*(1), 144–152. https://doi.org/10.38035/snefr.v2i1.646

Sukardi, D., Nugraha, F. B., Ubaidillah, U., Fatakh, A., Leliya, L., & Arrizky, M. F. (2023). Solving Cyber Crime In Online Buying And Selling In Cirebon City In Review Of Ite Law And Islamic Law. *Al-Mustashfa Jurnal Penelitian Hukum Ekonomi Syariah*, *8*(2), 237–237. https://doi.org/10.24235/jm.v8i2.15349

Sukmayanti, M. S., & Sudirga, I. M. (2022). Perlindungan Hukum Terhadap Driver Ojek Online Yang Mengalami Kerugian Akibat Tindakan Konsumen Yang Melakukan Pesanan Fiktif. *Synotic Law Jurnal Ilmu Hukum*, *1*(3), 177–185. https://doi.org/10.56110/sl.v1i3.16

Syahfallah, Z. A., Razak, A., & Salle, S. (2026). The Effectiveness of Law Enforcement on Cybercrime: A Case Study of Online Fraud in South Sulawesi. *SIGn Jurnal Hukum*, *7*(2), 1116–1130. https://doi.org/10.37276/sjh.v7i2.557

Syahril, Muh. A. F., & Aris, A. (2024). Strategies and Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the Implementation of the Electronic and Transaction Information Act. *Journal of Law Justice.*, *2*(3), 198–205. https://doi.org/10.33506/jlj.v2i3.3711

Weber, R. F. (2023). The Securities Law Disclosure Conundrum for Publicly Traded Litigation Finance Companies. *University of Michigan Journal of Law Reform*, 699–699. https://doi.org/10.36646/mjlr.56.3.securities

Wibowo, F. J. F. (2024). *Penerapan Pasal 28 ayat (1) Undang-Undang ITE terhadap pelaku orderan fiktif makanan pada ojek online (Studi Putusan Nomor 1597/Pid.Sus/2019/PN Jkt.Utr)*. Universitas Wijaya Kusuma Surabaya.

Wijaya, H. A., & Setiawan, D. A. (2021). Perlindungan Hukum terhadap Korban Orderan Fiktif Ojek Online Dihubungkan dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Prosiding Ilmu Hukum*, 752–757. https://doi.org/10.29313/.v0i0.27576

Wildanu, N. M., Yuswalina, Y., & Irawan, D. (2023). Sanksi Bagi Pelaku Ojek Online Yang Melakukan Order Fiktif Menggunakan Aplikasi "Fiktif." *Journal of Sharia and Legal Science*, *1*(2), 95–104. https://doi.org/10.61994/jsls.v1i2.176

Zebua, I. W. (2021). Kebijakan Hukum Pidana Terhadap Driver Transportasi Online Yang Melakukan Kecurangan Menurut Undang-Undang Informasi Dan Transaksi Elektronik (Studi Putusan Pengadilan Negeri Pemalang Nomor 82/Pid.Sus/2018/Pn Pml Dan Putusan Pengadilan Negeri Denpasar Nomor 226/Pid.Sus/2020/Pn Dps). *Iuris Studia Jurnal Kajian Hukum*. https://doi.org/10.55357/is.v2i3.172