Santhet: Jurnal Sejarah, Pendidikan Dan Humaniora
Vol. 9, No.5 Oktober 2025
Available online at https://ejournal.unibabwi.ac.id/index.php/santhet DOI:10.36526/js.v3i2.6068

Research Article e-ISSN: 2541-6130 p-ISSN: 2541-2523

ECONOMIC LOSS OF ONLINE MOTORCYCLE TAXI DRIVERS DUE TO ACCOUNT CLONING: A CASE STUDY OF TOMOHON CITY

Kerugian Ekonomi Pengemudi Ojek Online Akibat Kloning Akun: Studi Kasus Kota Tomohon

Lenda Lumentah[1a] Jola Silvana Kalangi[2b] Julita Inggrinne Nelwan[3c] Royke Max Suot[4d] Rieneke Kalalo[5e] Sjerly Maria Lumi[6f] Welky Karauwan[7g] James Edward Lalira[8h](*)

[1,2,3,4,5,6,7,8]Universitas Kristen Indonesia Tomohon

[a]*lendalumentahmajeza@gmail.com*
[b]*joulakalangi64@gmail.com*
[c]*barbienelwan@gmail.com*
[d]*roymax272@gmail.com*
[e]*rinrykekalalo2@gmail.com*
[f]*sjerlymarialumi99@gmail.com*
[g]*welkykarauwan@fkipukit.ac.id*
[h]*jameslalira@gmail.com*

(*) jameslalira@gmail.com
jameslalira@gmail.com

How to Cite: **James Edward Lalira**. (2025). Economic Loss of Online Motorcycle Taxi Drivers Due to Account Cloning: A Case Study of Tomohon City. doi: 10.36526/js.v3i2.6068

Received : 15-08-2025
Revised : 23-09-2025
Accepted: 08-10-2025

Keywords:
Economics and Human Resources,
Driver Losses,
Online Motorcycle Taxi,
Account Cloning,
Tomohon

Abstract
This study aims to analyze the economic losses suffered by online motorcycle taxi drivers in Tomohon City due to account cloning, a growing form of digital exploitation in Indonesia's gig economy. The research examines financial, operational, and psychological impacts, evaluates platform security measures, and assesses the erosion of consumer trust. A mixed-methods approach was employed, combining quantitative surveys with 50 drivers and qualitative in-depth interviews with drivers, customers, and platform representatives. Data were collected through structured questionnaires, participatory observation, and thematic analysis. Quantitative data were analyzed using descriptive statistics to measure income decline and additional costs, while qualitative data were interpreted through thematic content analysis to understand lived experiences and systemic vulnerabilities.Findings reveal that 44% of income reduction is directly linked to account-related disruptions, with affected drivers losing between IDR 500,000 and 1,000,000. Additional recovery costs further strain their financial stability. Psychologically, 76% reported moderate to high anxiety, and 64% stated that the threat of cloning negatively affects work motivation. Consumer trust is compromised, as 80% of drivers acknowledge reputational damage due to service inconsistencies caused by cloned accounts. Despite high awareness of cloning (82%), only 40% implement preventive measures, and 70% perceive platform responses as inadequate. The discussion highlights that account cloning is a systemic issue rooted in weak platform governance and low digital literacy. The absence of compensation mechanisms exacerbates worker vulnerability. This study recommends mandatory implementation of advanced security protocols, integrated digital literacy programs, and a formal gig worker protection framework including rapid reporting and financial compensation. These measures are essential for building a fairer and more sustainable digital transportation ecosystem.

INTRODUCTION

The rise of the digital economy in Indonesia has significantly transformed urban transportation systems, particularly through the proliferation of online motorcycle taxi (ojek online) services. These digital platforms not only enhance mobility access, but also serve as a livelihood source for millions of daily wage workers across the country. In medium-sized cities, such as Tomohon, online ojeks have become increasingly embedded within the local economic ecosystem. However, this rapid growth has not been matched by adequate protective mechanisms for the drivers. An emerging threat is account cloning, in which the identity of legitimate drivers is illegally replicated by unauthorised parties. This practice enables perpetrators to intercept ride requests without consent, thereby distorting income distribution. As a result, genuine drivers experience a sharp decline in the daily order volume. This condition not only causes financial harm, but also erodes their sense of security and trust in the platform.

Although Tomohon is not a major metropolitan area, there has been a notable increase in online ojek use in recent years. Field data indicate a growing number of registered drivers, particularly since 2021, coinciding with the rising transportation demand and broader technology adoption among residents. However, reports from driver communities revealed sudden and unexplained losses in ride requests. Many drivers reported remaining active on the app but received no service requests for hours. This pattern recurs unevenly, suggesting external interference in the order allocation algorithm. It is strongly suspected that this phenomenon is linked to account cloning, unauthorised use of personal data, and devices belonging to legitimate drivers. This practice allows offenders to operate two accounts simultaneously: one under the authentic driver's identity, and another cloned account running in parallel. Consequently, the platform's algorithm can be deceived into assigning orders to the illegitimate accounts.

The impact of account cloning extends beyond economic dimensions and affects psychological and social well-being (Bonetti et al. 2023; Moldes & Ku 2020; Dwivedi et al. 2023). Drivers who fall victims often suffer stress due to income instability, especially because they rely on daily earnings to meet their basic needs (Amoadu et al. 2023; Nanjunda 2021). Preliminary interviews revealed that some drivers feel "haunted" because of the constant possibility of their accounts being cloned. Moreover, customers may be adversely affected, potentially receiving services from unverified individuals, which introduces safety risk. The platform's lack of transparency in handling cloning-related complaints further deepened distrust. There is no clear reporting mechanism and customer service responses are frequently inadequate. If left unaddressed, this practice could destabilise the digital ecosystem and undermine public confidence in app-based business models. Therefore, this study aimed to empirically uncover the resulting losses and provide data-driven recommendations.

Existing studies on online ojek have primarily focused on legal aspects, particularly from Islamic or civil law perspectives. Researchers have examined practices such as account leasing, pledging, selling, and assessing compliance with religious norms and corporate policies. For instance, Wulandari (2022) and Nanda Kukuh (2020) analyze account transactions through the lens of Islamic commercial jurisprudence (fikih muamalah), arguing that such practices violate the principles of honesty and business integrity (Nanda, 2020; Wulandari, 2022). However, these approaches remain largely normative and fail to quantify the actual economic losses experienced by the drivers. They did not address the technical aspects of account cloning, such as how data are compromised or how platform security systems are breached. Consequently, the findings of such studies offer limited applicability for developing digital security frameworks or worker protection policies.

Other studies have explored intra-driver competition, such as strategies for selecting pickup locations or optimising operational hours to maximise ride requests. Akbar et al. (2023) investigated competitive behaviors among drivers in Samarinda, but did not consider external threats such as account cloning. Their study assumed a level-playing field among drivers, whereas cloned accounts introduced structural inequities. Additionally, several academic studies have examined the legal protection for drivers against consumer misconduct, such as fake orders or payment fraud. Other researchers highlight aspects of consumer law but do not investigate internal digital crimes, such as account manipulation (Mahendra & Luhfitasari, 2022; Sukmayanti & Sudirga, 2022). They also failed to assess the effectiveness of two-step verification or authentication systems designed to prevent unauthorised access. Thus, there is a significant gap in the literature on digital security and account exploitation.

Some studies have assessed customer satisfaction (Oktarisa & Nanda, 2019) or safety-riding behaviour (Nusa et al., 2021); however, their focus does not extend to integrity or system security. Research on account pledging agreements by Syalamuddin et al. (2022) and Faizin (2020) remains confined to contractual laws, rather than cybersecurity. No prior study has specifically measured income reduction due to account cloning or analyzed suspicious activity patterns within the system (Mustika & Savirani, 2021; Sandbukt, 2021; Wahyudi et al., 2023). The current state of knowledge reveals a fragmented body of literature that does not comprehensively address account cloning from an economic, technological, or policy perspective. No existing research integrates quantitative data on financial losses with in-depth qualitative insights from victims. This study fills that gap by employing an integrated mixed-methods approach, focusing on the economic impact and targeting an under-researched local context, Tomohon City.

This study offers originality by empirically identifying and mapping the direct economic losses incurred by drivers due to account cloning, a gap unaddressed in studies on medium-sized Indonesian cities. Unlike previous normative or legal approaches, this study employs a comparative quantitative descriptive analysis to measure income changes before and after suspected cloning incidents. It further integrates qualitative data from interviews with drivers, customers, and platform representatives to understand the mechanisms and underlying causes of cloning. Another key contribution lies in its focus on Tomohon as a case study, which offers unique insights into digital economies in non-metropolitan regions. This study also formulates concrete policy recommendations applicable to both platforms and regulators. Thus, it not only bridges a critical literature gap but also delivers evidence-based solutions to pressing real-world issues.

Account cloning poses a serious threat to fairness in the digital economy, particularly for daily wage workers who are dependent on consistent earnings (Nowak, 2022; Ramizo, 2021). Without intervention, this phenomenon may evolve into systematic exploitation, undermining trust in digital platforms. Drivers who lose ride requests because of cloned accounts suffer direct financial losses, including forgone income and unrecovered operational costs. Over time, this can trigger social instability and reduce public participation in the digital economy. Additionally, consumer confidence is compromised when services are delivered by unverified individuals, which increases safety risks. If unaddressed, the overall reputation of the digital transportation industry may suffer, especially in emerging markets such as Tomohon, where trust in app-based services is still being established.

From a policy standpoint, the findings of this research align closely with the National Research Master Plan (RIRN), particularly under the theme of Economy and Human Resources, with emphasis on gig worker protection. The results can inform stricter digital security regulations, including two factor authentication, monitoring of suspicious activities, and compensation schemes for cloning victims. The study also supports Key Performance Indicators (IKU) for higher education institutions by contributing to public policy innovation. This urgency is further reinforced by technological demands, as cybersecurity must be prioritized in digital transformation. Without secure, inclusive, and transparent systems, a digital ecosystem cannot be sustainable. Hence, this study responds to the urgent need for data-driven solutions to protect digital workers from technological exploitation.

This study aims to analyze the economic impact of account cloning on the income of online drivers of ojek in Tomohon City, focusing on income reduction, increased operational costs, and psychological consequences. It seeks to identify patterns of suspicious account activity and evaluate the effectiveness of platform security systems in preventing cloning. Furthermore, this research aims to uncover enabling factors both technological and behavioral that facilitate cloning. It also explores how this practice affects consumer trust in online ojek services. Based on these findings, mitigation strategies were formulated for adoption by drivers, platforms, and regulatory bodies. The ultimate goal is to provide practical policy recommendations to foster a fairer, safer, and more sustainable digital transportation ecosystem.

The findings have significant academic, practical, and policy implications. Academically, this study enriches the literature on digital economies and cybersecurity in Indonesia, particularly in non-metropolitan areas. For ojek online platforms, the results can guide improvements in the early detection of suspicious accounts and strengthen driver protection mechanisms. Recommendations such as two-factor authentication, login alerts from new devices, and responsive reporting systems can be implemented directly. For regulators, this study provides a scientific basis for crafting policies that protect gig workers from digital crimes. Socially, it promotes a fairer system in which drivers are safeguarded from exploitation. Economically, it contributes to stabilizing the daily earnings of informal workers. Technologically, this encourages innovation in digital security for application-based services.

METHOD

This study employed a mixed-methods approach (Asad et al., 2022; Gupta et al., 2024) within a case study design to comprehensively examine the economic impact of account cloning on online motorcycle taxi drivers in Tomohon City. The integration of qualitative and quantitative data allows for a nuanced understanding of both measurable financial losses and the lived experiences of the affected drivers. Data collection was conducted through structured surveys, in-depth interviews, and participatory observation to ensure methodological triangulation. The case study framework was selected to enable a focused investigation of a specific phenomenon within its real-life context, particularly in an emerging urban setting where digital labor dynamics are rapidly evolving. Research activities are centered on selected subdistricts of Tomohon known for high ojek online activity and reported incidents of account misuse. Site selection was based on preliminary evidence of cloning cases and socioeconomic diversity among drivers. This design facilitates contextual depth while maintaining analytical precision. As such, the methodology is well suited to uncover the multifaceted consequences of digital exploitation in localized gig economies.

The research population included all registered ojek online drivers in Tomohon City, alongside key stakeholders such as customers, platform representatives, and local regulators. A sample of 50 inDrive drivers was selected through simple random sampling for the quantitative component, ensuring statistical representativeness for income and operational cost analysis. For qualitative data, purposive sampling was applied to identify 20 drivers who had experienced or reported account cloning. The selection criteria emphasize direct exposure to the phenomenon and the ability to provide rich, reflective narratives. Semi-structured interviews were conducted to explore drivers’ perceptions of security, financial impacts, and psychological stress related to unauthorized account use. Structured field surveys were administered using a validated questionnaire to measure economic indicators, including daily income, order frequency, and operational expenditures. Participatory observation is conducted during peak service hours to document interaction patterns, order allocation behaviors, and potential anomalies in platform functionality. This multi-source data strategy enhances both internal validity and contextual authenticity.

Data collection was executed in three sequential phases: preparation, field implementation, and cross-verification. The preparatory phase included instrument development, pilot testing of survey tools, and training of research assistants to ensure procedural consistency. Secondary data were gathered from official reports, academic publications, and publicly available platform policies related to digital security and driver rights. During field implementation, primary data were collected through face-to-face interviews and direct survey administration, with strict adherence to research ethics and participant confidentiality. All interviews were audio-recorded with informed consent and transcribed verbatim for thematic analysis. Cross verification or data triangulation is performed by comparing findings from surveys, interviews, and observations to identify convergent and divergent patterns. The collected data were systematically categorized by source, theme, and reliability level. This structured approach ensures data integrity, minimizes bias, and supports robust interpretation. Methodological transparency strengthens the credibility of the findings for academic and policy audiences.

Data analysis was conducted separately for quantitative and qualitative components before being integrated into a unified interpretation. Quantitative data were analyzed using comparative descriptive statistics to identify shifts in driver income before and after suspected cloning incidents. Measures such as mean, standard deviation, and paired t-tests were applied to assess the magnitude and significance of economic losses. Qualitative data were analyzed through thematic content analysis to identify recurring narratives, underlying motives, and coping strategies among affected drivers. NVivo software was utilized to code and manage textual data systematically, enabling the precise tracking of emergent themes. The integration of both datasets is achieved through joint display mapping, where quantitative trends are interpreted along with qualitative insights to form a cohesive narrative. Policy recommendations are formulated through iterative discussions among research team members grounded in empirical evidence and contextual feasibility. This analytical process ensures that the findings are not only descriptive but also prescriptive, offering actionable solutions for platform operators, regulators, and driver communities.

RESULT AND DISCUSSION

Result

A. Quantitative Data

1. Demographic and Professional Profile of Drivers

The study involved 50 ojek online drivers actively operating in Tomohon City, offering a representative snapshot of the local digital labor force. Nearly all participants were male (94%), aligning with the gender composition commonly observed in Indonesia’s ride-hailing industry. The majority of respondents fell within the 20–30 age range (60%), reflecting a workforce that is not only young but also familiar with digital platforms. Approximately 40% had been engaged in app-based driving for more than three years, indicating a sustained reliance on platform-generated income. The most frequently used platforms were inDrive (80%) and Grab (20%), illustrating a fragmented yet competitive digital ecosystem. This multi-app usage pattern suggests a strategic effort by drivers to optimize order acquisition across different systems. Most respondents reported working daily, with earnings directly dependent on the volume of completed trips. Demographic and operational consistency across respondents strengthens the internal validity of the findings for urban gig economy research.

2. General Experiences and Economic Vulnerabilities

An overwhelming 86% of drivers reported a recent decline in income, highlighting the financial volatility inherent in platform-based work. Of these, 72% linked the drop to intensified competition among drivers, whereas 58% pointed to technical malfunctions in the application as a contributing factor. Significantly, 44% explicitly associated reduced earnings with account-related disruptions, including unauthorized access and temporary suspension. External factors, such as adverse weather and personal health issues, were acknowledged but less frequently cited as primary causes. A striking 88% affirmed that the number of ride requests received had a significant influence on their daily earnings, reinforcing the precariousness of gig employment. Two-thirds (68%) noted shifts in competitive dynamics in recent years, particularly the emergence of algorithmic advantages and unethical practices. When asked about the main drivers of competition, over half (52%) identified "unhealthy practices like account cloning" as a major concern. This reveals that drivers perceive cloning not just as a security flaw, but also as a systemic distortion in the fairness of income distribution.

3. Awareness and Direct Experience with Account Cloning

A notable 82% of respondents were familiar with the concept of "account cloning," confirming a high level of awareness within the driver community. Among them, 66% considered the practice either common or widespread in Tomohon’s ojek online network. Six out of ten drivers either experienced cloning firsthand or knew someone close to them who had been affected. The most frequently reported consequences were financial loss (74%), account deactivation (56%), and unauthorized use of personal information (32%). Many drivers described receiving alerts about logins from unfamiliar devices as a clear sign of compromised account integrity. Despite these risks, only 40% indicated that they had implemented preventive measures, such as two-factor authentication or routine password updates. In response to suspicious activities, the most common actions were contacting customer support (68%) or resetting passwords (54%), although few felt their concerns were adequately addressed. The persistence of such incidents indicates that current platform mechanisms fail to provide timely or effective resolutions.

4. Financial and Psychological Impact of Cloning

Drivers facing account-related disruptions estimated monthly income losses between IDR 500,000 and IDR 1,000,000, with more than half (52%) falling within the range of IDR 1, 000, 000–2, 000, 000. Beyond lost earnings, 48% incurred additional expenses, such as travel to service centers or data purchases, to resolve account issues, averaging IDR 300,000–500,000 monthly. These combined financial burdens represent severe strain, particularly for drivers operating with minimal profit margins. On a psychological level, 76% expressed moderate to high anxiety about the possibility of future cloning incidents. This anxiety translated into reduced work motivation, with 64% stating that the threat of cloning negatively influences daily operations. Approximately 40% reported receiving complaints from passengers because of inconsistent services or rating anomalies linked to cloned accounts. While most attempted to clarify the situation, many felt powerless without formal platform acknowledgment or support. Furthermore, 80% of the respondents recognized that consumer trust in their reliability had diminished, posing a long-term threat to their professional reputation.

5. Perceived Inadequacy of Platform and Policy Responses

Only 30% of the drivers felt that the platforms had provided sufficient guidance on preventing account cloning, exposing a significant gap in digital safety education. Regarding security practices, 54% reported using two-factor authentication and 42% regularly updated passwords, indicating partial but inconsistent adherence to protective protocols. Despite these individual efforts, 70% believed that institutional safeguards, both technical and legal, were insufficient or entirely absent. The lack of an immediate reporting channel or real-time monitoring system has repeatedly been highlighted as a critical barrier to swift resolution. Drivers proposed several improvements, including an enhanced security infrastructure (78%), ongoing digital literacy programs (66%), and enforceable penalties for offenders (72%). A rapid incident reporting tool was strongly desired (64%), underscoring the need for responsive support systems. An overwhelming 88% of the respondents agreed that research outcomes should guide policy reforms to protect digital workers. This consensus reflects a clear demand for regulatory and platform-level interventions to combat digital exploitation in the transportation sector.

B. Qualitative Data

The qualitative data table reveals five core themes that emerged from the drivers' experiences with account cloning, illustrating the multidimensional nature of digital exploitation in the gig economy. The themes of Digital Trauma and Powerlessness reflect the loss of autonomy over a digital identity that has become essential to livelihoods, resulting in feelings of helplessness and chronic stress. Victims suffer not only financial loss but also reputational damage when services are delivered by cloned accounts, creating structural injustice within algorithm-based rating systems. This indicates that account security is not merely a technical issue but a matter of worker dignity and economic fairness. Theme-independent adaptation strategies highlight drivers' self-initiated efforts to protect their accounts, such as regularly changing passwords or deactivating apps. However, these strategies are often ineffective because of limited digital literacy and absence of institutional support from platforms. The reliance on individual initiatives reveals a systemic failure to provide proactive protection. Consequently, digital resilience cannot be built solely from the bottom-up, but requires structured institutional intervention.

The theme Erosion of Consumer Trust demonstrates that account cloning harms not only drivers, but also undermines consumer confidence in the entire digital service ecosystem. When customers receive services from individuals who do not match the profile displayed in the app, they feel deceived even though the legitimate driver is the actual victim. This misalignment creates a communication gap between the parties that are adversely affected. The resulting decline in trust in the verification system reflects broader institutional distrust that threatens the sustainability of platform-based business models. Theme Cloning Mechanisms and Technological Vulnerabilities uncover technical loopholes, such as the sale of second-hand devices without proper data wiping that are exploited by perpetrators to gain unauthorised access to genuine accounts. This practice shows that cloning often stems not from advanced technical skills but from the exploitation of user negligence and lack of awareness. The final theme, Unresponsive Platform Response, highlights the slow account recovery process and the absence of financial compensation, which exacerbates economic and psychological harm. Without clear accountability mechanisms, platforms continue to evade responsibility, deepening the imbalance in digital labour relations.

Table: Qualitative Data

Theme	Academic Interpretations
Digital Trauma and Powerlessness	Loss of control over account and digital identity
	Unfair reputational damage
Independent Adaptation Strategies	Preventive efforts without institutional support
	Technology adoption without full understanding
Erosion of Consumer Trust	Miscommunication between victims and customers
	Declining trust in system transparency
Cloning Mechanisms and Technological Vulnerabilities	Exploitation of second-hand devices without data reset
	Temporary competitive advantage for perpetrators
Unresponsive Platform Response	Slow and non-transparent account recovery process
	Absence of financial compensation

Discussion

Quantitative Findings

The finding that 94% of the drivers were male reflects the gendered nature of app-based transportation work in Indonesia, a sector historically dominated by men. This imbalance is not merely demographic, but also contributes to disparities in access to digital training and technical support. Female workers in this field may face compounded barriers owing to social norms and limited platform safeguards. This aligns with Murtadlo and Sulhan’s (2023)research on digital economic inclusion, which highlights the uneven distribution of digital transformation benefits. When systems are designed without considering user diversity, marginalized groups become more vulnerable to exploitation. In the context of account cloning, gender inequality can exacerbate susceptibility, owing to restricted access to security education. Therefore, responses to digital threats should incorporate broader social dimensions. Without such inclusivity, worker protection will benefit only a privileged segment of the gig workforce.

The predominance of drivers aged 20–30 years indicates that the ojek online workforce is primarily composed of young, tech-savvy individuals who may lack digital security awareness. While they are proficient in using applications, many do not understand risks such as account cloning or data theft. Their reliance on daily income makes them particularly vulnerable to prolonged system disruptions. Salistia et al.,(2023) emphasize human capital capacity in digital innovation but do not address digital security literacy. The gap between technical skills and security awareness creates exploitable vulnerability in cloning perpetrators. Platforms often assume that users understand associated risks, despite evidence to the contrary. Thus, this demographic profile is not merely descriptive but indicative of structural vulnerability. Interventions must target this age group with accessible integrated digital safety education.

The finding that 40% of respondents have been active for over three years suggests that online ojek is no longer a temporary job but a long-term livelihood. This sustained dependence increases systemic risk when disruptions, such as account cloning, occur. Drivers who have invested time and resources in the platform ecosystem become more susceptible to significant losses when access is compromised. This supports the argument that the digital economy has created a new economic civilization requiring mature regulation (Beaumier et al., 2020; Tarakanov et al., 2019). When gig work becomes functionally permanent, legal and technical protection must evolve accordingly. Systems designed for temporary workers cannot safeguard workers that are fully dependent on algorithms. Without adequate protection, the microeconomic stability of these workers remains a perpetual risk. Hence, the duration of engagement is a critical indicator for assessing the need for formal worker safeguards.

The high rate of income decline (86%) reveals the intrinsic volatility of app-based economic models, which fail to guarantee stability, even for experienced workers. Intense competition (72%) and technical issues (58%) create dual pressure, which worsens uncertainty. Other research shows that competition is often based on system access rather than service quality (Rahmayati, 2021; Syapsan, 2019). Account cloning represents an extreme form of this imbalance, where perpetrators gain an advantage without effort. When algorithmic systems cannot distinguish between legitimate and cloned accounts, fair competition collapses. In this context, income loss is not merely a market fluctuation, but a result of systemic distortion. Therefore, interventions should be both technical and regulatory in nature. Without structural reforms, inequity persists.

The claim that 44% of income decline is directly linked to account issues indicates that cloning is not a marginal threat but a primary cause of economic loss. This figure shows that account security is central to income stability, comparable to external factors, such as weather or health. This contrasts with prior studies that focused on legal or ethical aspects, such as Wulandari's (2022) analysis of account leasing from an Islamic economic perspective. Normative approaches do not measure the real economic harm experienced by workers. In contrast, these data show that losses are tangible and measurable, demanding empirical policy responses. Account cloning must be understood not only as a technical breach but also as a form of economic exploitation. Without recognizing this economic dimension, the proposed solutions will remain superficial.

The high awareness of the term "account cloning" (82%) indicates that the phenomenon has become part of everyday discourse among drivers. However, awareness does not always translate into preventive action, as only 40% of the respondents reported implementing proactive security measures. This reflects a knowledge-action gap in digital literacy, where understanding does not lead to safe behavior. Studies on digital cultural transformation show that technology adoption is often instrumental, lacking deep comprehension (Bozkus, 2023; Moldes & Ku, 2020). Drivers use apps to earn income and not to understand their risks. In this context, digital security education must be integrated into the platform ecosystem and not delivered sporadically. Notifications, tutorials, and threat simulations can become part of the user experience. Without such integration, awareness remains passive knowledge that fails to protect workers.

The significant financial impact, with over half of the affected drivers losing IDR 1–2 million monthly, shows that account cloning is not just a technical issue, but also a threat to livelihood sustainability. Such losses can undermine the fulfilment of basic needs, especially for daily wage earners without savings. Additional costs, such as travel to service offices (48%), unfairly increase economic burdens. Research on legal protection for drivers facing fake orders reveals a similar pattern: losses are both direct and secondary (Fauzan & Permana, 2022; Wahyudi et al., 2023). In cloning cases, losses are multidimensional: financial, operational, and reputational. A system that fails to prevent or compensate for such losses violates the principles of distributive justice. As the party controlling the algorithm, the platform must be accountable for the damage caused by its failures.

The widespread psychological impact, with 76% reporting anxiety and 64% reduced work motivation, shows that account cloning undermines drivers' holistic well-being. Chronic stress due to income uncertainty can affect mental health and service quality. When workers feel digitally unsafe, they cannot deliver optimal services. This aligns with Oktarisa and Nanda's (2019) findings on the link between trust and rider productivity. However, their study does not address external digital threats such as cloning, which amplifies stress beyond typical gig work volatility. Well-being on digital platforms must, therefore, include digital safety as a core component of occupational health. The erosion of consumer trust, reported by 80%, further illustrates the spillover effects of cloning, where individual reputational damage undermines the entire service network.

The decline in consumer trust (80%) due to service inconsistency shows that account cloning harms not only drivers but also damages the system's overall reputation. When customers receive poor service from a cloned account, they blame the legitimate driver, eroding their hard-earned trust. This creates a spillover effect, where one violation harms multiple parties. Mahendra and Luhfitasari highlight consumer protection but do not examine how worker violations also harm consumers. Worker integrity and consumer trust are interdependent in digital ecosystems. Without accountability for cloning, trust in the platform continues to erode. Thus, account security is foundational to systemic trust (Mahendra and Luhfitasari, 2022). Platforms must view security not as a cost but as an investment in long-term reputation.

The perception of inadequate platform response by 70% of the respondents reveals institutional failure in protecting gig workers. The absence of fast reporting and compensation mechanisms indicates weak corporate social responsibility. Faizin's study on account leasing shows that platforms often evade responsibility by classifying violations as individual issues. However, these data show that violations are systemic and require systemic responses (Faizin, 2020). Platforms must not act merely as intermediaries but also as duty-bearers in the ecosystems they create. Government regulation should compel platforms to provide minimum protection, such as digital insurance or compensation funds. Without such measures, workers will remain victims of structured digital exploitation. Thus, discussions on digital security must be linked to fair platform governance.

Qualitative Findings

The reported experience of digital trauma reveals a loss of autonomy over digital identity, which has become a primary livelihood tool for drivers. When an account is cloned, drivers lose not only income, but also control over their professional representation of consumers. This phenomenon reflects digital disempowerment, whereby gig workers lose access to their work tools without swift recovery. In many cases, victims feel "silently robbed" because of the absence of notifications or warnings from the platform. This intensifies feelings of helplessness and erodes trust in the system intended to protect them. These findings show that digital security is not merely a technical issue but also a matter of worker dignity. Workers remain vulnerable to systematic exploitation, without adequate protection. Therefore, account security must be recognized as a fundamental right in the digital economy.

Unfair reputational damage becomes an additional burden for victims, as they receive negative reviews for services they did not provide. Sudden rating drops damage long-term reputation despite the driver's innocence. This highlights flaws in algorithm-based rating systems that cannot distinguish between real and cloned accounts. This injustice disrupts fairness in the digital ecosystem, where reputation is key social capital. Customers who give low ratings are unaware that they are evaluating the perpetrator, not the victim. This creates cross-mistrust between workers and consumers. Without a clarification mechanism, a legitimate driver's reputation remains tarnished. Therefore, rating systems must be updated to account for potential cloning.

Drivers' self-initiated preventive efforts, such as turning off the app or regularly changing passwords, demonstrate self-regulation in a work environment that fails to protect them. However, reliance on individual strategies reveals platform failures in providing proactive security systems. Many drivers do not understand how two-factor authentication and security apps operate, rendering their protection suboptimal. This indicates the need for structured, ongoing digital literacy programs from platforms. Security education must be part of onboarding and continuous training. Without this, workers will continue to rely on personal improvisation, which is not always effective. Thus, prevention must be a shared responsibility and not an individual burden.

The adoption of technology without full understanding shows that while drivers use advanced devices, they often do not grasp the associated risks. Many install antivirus software without knowing whether it truly protects them. This reflects the wide digital literacy gap between technology use and security awareness. Platforms often assume that users understand digital risks, although reality proves otherwise. Provided education is often generic and noncontextual. Therefore, interventions must be specifically designed for non-technical workers using simple language and relevant examples. Otherwise, the training will remain ineffective. Digital resilience must be built from the ground and not imposed from above.

The miscommunication between victims and customers shows that account cloning creates a gap between digital identity and real-world services. Customers feel deceived when the displayed profile does not match that of the arriving driver. However, the driver involved is a victim, not a perpetrator. This inconsistency undermines social contracts in platform-based economies. Consumers begin developing their own verification methods, such as noting physical traits, which indicate lost trust in the system. This reflects institutional distrust in the digital ecosystem. Trust cannot be rebuilt without transparency and accountability. Therefore, platforms must act as active mediators rather than passive observers.

Account cloning is often enabled by the exploitation of second-hand devices that are not properly reset. Perpetrators using used phones still logged into drivers' accounts, allowing them to operate the two accounts simultaneously. This practice reveals the technological vulnerabilities systematically exploited by certain actors. User ignorance about data sanitization contributes to this problem. Therefore, education on data sanitization must be expanded, not only for workers but also for second-hand device sellers. In addition, platforms should implement facial verification or geolocation to prevent logins from new devices. Without such measures, technological loopholes could continue to be exploited. Security must start upstream and not just be addressed after violations occur.

The platform's slow and non-transparent response reveals a failure in accountability mechanisms. Recovery processes that take days without procedural clarity worsen the economic and psychological harm. The absence of financial compensation reflects the lack of a formal protection framework for gig workers. Platforms avoid this by classifying cloning as an individual issue. However, the data show that this is a systemic violation. Therefore, government regulations require platforms to provide compensation schemes and rapid reporting. Without this, workers will remain victims of structured digital exploitation. Digital justice can only be achieved if platforms are held accountable for the systems that they control.

CONCLUSION

This study confirms that account cloning poses a serious threat to the economic sustainability of online motorcycle taxi drivers in Tomohon City, extending far beyond mere technical malfunctions. The practice directly causes significant income loss, with affected drivers reporting average monthly financial damages reaching millions of Indonesian Rupiah, alongside additional costs incurred during account recovery. The impact is not limited to financial loss but extends into the psychological realm, where victims experience high levels of anxiety, reduced work motivation, and a profound sense of insecurity regarding their digital identity. These findings indicate that account cloning has created structural inequity within the digital ecosystem in which a supposedly fair system is exploited for selective gain without accountability.

Qualitative insights reveal that victims of account cloning endure digital trauma because of the loss of control over their livelihood-dependent accounts. Many drivers feel inadequately protected by platforms, particularly because of delayed, non-transparent responses, and the absence of compensation mechanisms. The lack of real-time monitoring and instant reporting further exacerbates their vulnerability. While some drivers have taken preventive measures, such as changing passwords or enabling two-factor authentication, these individual efforts are often insufficient because of limited digital literacy. This highlights that reliance on personal initiatives cannot address a systemic issue that demands collective and institutional intervention.

This research successfully addresses its core objectives by comprehensively revealing the economic losses, psychological burdens, and reputational distortions experienced by drivers due to account cloning. The mixed-methods approach enabled the integration of measurable quantitative data with in-depth qualitative narratives, providing a holistic understanding not previously captured in the existing literature. Unlike prior studies that focus on legal or ethical dimensions, this study shifts the focus to tangible economic harm and the need for fair platform governance. By positioning drivers as vulnerable subjects within digital exploitation, this study reframes account cloning from a technical violation to a matter of economic justice.

Looking ahead, these findings offer a foundation for developing gig worker protection policies for both platforms and regulators. Minimum digital security standards should be mandated, including facial verification, anomaly detection, and instant reporting systems. Furthermore, structured digital literacy programs should be integrated into the platform ecosystem to enhance driver resilience. This study also opens avenues for future research, such as comparative studies across regions or experimental interventions to assess the effectiveness of security measures. Thus, while rooted in a local case, the implications of this research hold potential for broader national applications, contributing to the development of a more equitable and sustainable digital transportation ecosystem.

-spasi-

DAFTAR PUSTAKA

Akbar, S. A., Nasir, B., & Situmorang, L. (2023). Strategi Kompetisi Pengemudi Ojek Online Kelurahan Sempaja Selatan Dalam Menghadapi Persaingan Sesama Pengemudi Ojek Online Di Kota Samarinda. *EJournal Pembangunan Sosial*, *1*, 30–45.

Amoadu, M., Ansah, E. W., & Sarfo, J. O. (2023). Psychosocial work factors, road traffic accidents and risky driving behaviours in low-and middle-income countries: a scoping review. *IATSS Research*, *47*(2), 240–250.

Asad, M. M., Naz, A., Churi, P., Guerrero, A. J. M., & Salameh, A. A. (2022). Mix method approach of measuring VR as a pedagogical tool to enhance experimental learning: Motivation from literature survey of previous study. *Education Research International*, *2022*(1), 8262304.

Beaumier, G., Kalomeni, K., Campbell-Verduyn, M., Lenglet, M., Natile, S., Papin, M., Rodima-Taylor, D., Silve, A., & Zhang, F. (2020). Global regulations for a digital economy: Between new and old challenges. *Global Policy*, *11*(4), 515–522.

Bonetti, G., Donato, K., Medori, M. C., Dhuli, K., Henehan, G., Brown, R., Sieving, P., Sykora, P., Marks, R., & Falsini, B. (2023). Human Cloning: Biology, Ethics, and Social Implications. *La Clinica Terapeutica*, *174*(6).

Bozkus, K. (2023). Organizational culture change and technology: Navigating the digital transformation. In *Organizational Culture-Cultural Change and Technology*. IntechOpen.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., Koohang, A., Ribeiro-Navarrete, S., Belei, N., & Balakrishnan, J. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers*, *25*(5), 2071–2114.

Faizin, I. (2020). *Tinjauan Ijarah Terhadap Praktik Sewa-Menyewa Akun Ojek Online Oleh Anggota Komunitas Ponorogo Ojek Online Singo Aloon-Aloon Independen Di Kabupaten Ponorogo*. IAIN Ponorogo.

Fauzan, D. A., & Permana, Y. S. (2022). Legal Protection For Online Transportation Drivers In The

Case Of Fictional Order In Indonesia. *LEGAL BRIEF*, *11*(3), 1800–1805.

Gupta, O. J., Yadav, S., Srivastava, M. K., Darda, P., & Mishra, V. (2024). Understanding the intention to use metaverse in healthcare utilizing a mix method approach. *International Journal of Healthcare Management*, *17*(2), 318–329.

Mahendra, R. A., & Luhfitasari, R. (2022). Perlindungan Hukum Terhadap Konsumen Akibat Praktik Jual Beli Akun Pengemudi Ojek Online Di Kota Balikpapan. *Journal de Facto*, *8*(2), 145–160.

Moldes, O., & Ku, L. (2020). Materialistic cues make us miserable: A meta-analysis of the experimental evidence for the effects of materialism on individual and societal well-being. *Psychology & Marketing*, *37*(10), 1396–1419.

Murtadlo, K., & Sulhan, M. (2023). Ekonomi Digital dan Inklusi Keuangan Terhadap Pemulihan Ekonomi Nasional. *Jurnal Nusantara Aplikasi Manajemen Bisnis*, *8*(1), 90–104.

Mustika, W., & Savirani, A. (2021). 'Ghost accounts','Joki accounts' and 'account therapy': everyday resistance among ride-hailing motorcycle drivers in Yogyakarta, Indonesia. *The Copenhagen Journal of Asian Studies*, *39*(1).

NANDA KUKUH WICAKSONO, W. I. C. (2020). *TINJAUAN HUKUM ISLAM TENTANG GADAI AKUN OJEK ONLINE*. UIN Raden Intan Lampung.

Nanjunda, D. C. (2021). Impact of socio-economic profiles on public health crisis of road traffic accidents: A qualitative study from South India. *Clinical Epidemiology and Global Health*, *9*, 7–11.

Nowak, S. L. (2022). *Provincializing Platform Capitalism: Digitization and Informality in Jakarta's Motorbike Taxi Industry*. University of California, Los Angeles.

Nusa, S. T., Febriyanty, D., & Rusdy, M. D. R. (2021). Faktor-Faktor yang Berhubungan dengan Perilaku Safety Riding pada Komunitas Ojek Online di Kota Bekasi. *J Kesehat Masy*, *2*(2), 95–102.

Oktarisa, F., & Nanda, C. A. (2019). Amanah dan Kepuasan Konsumen dalam Memprediksi Produktivitas Rider Ojek Online. *JSSH (Jurnal Sains Sosial Dan Humaniora)*, *3*(1), 27–35.

Rahmayati, R. (2021). Competition Strategy In The Islamic Banking Industry: An Empirical Review. *International Journal Of Business, Economics, And Social Development*, *2*(2), 65–71.

Ramizo, G. (2021). *Ubering while poor: the socio-political implications of digital platforms in underdeveloped contexts*. University of Oxford.

Salistia, F., Riyanto, R., Junaedi, D., & Amalia, R. S. (2023). Ekosistem SDM dan inovasi ekonomi digital di Indonesia. *Sci-Tech Journal*, *2*(1), 11–31.

Sandbukt, S. (2021). *Top-Up with Driver: Digital Money, Transactional Aspirations, and Peerhood in Yogyakarta, Indonesia*. IT-Universitetet i København.

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.

SYALAMUDDIN, M., & others. (2022). *TINJAUAN YURIDIS PERJANJIAN GADAI AKUN OJEK ONLINE PERSPEKTIF HUKUM PERDATA INDONESIA.*

Syapsan. (2019). The effect of service quality, innovation towards competitive advantages and sustainable economic growth: Marketing mix strategy as mediating variable. *Benchmarking: An International Journal*, *26*(4), 1336–1356.

Tarakanov, V. V, Inshakova, A. O., & Dolinskaya, V. V. (2019). Information society, digital economy and law. In *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT* (pp. 3–15). Springer.

Wahyudi, E., Darmawan, D., & Hardyansah, R. (2023). Legal Protection for Online Ojek Drivers Who are Victims of Fictitious Order. *Bulletin of Science, Technology and Society*, *2*(2), 37–43.

Wulandari, W. (2022). *TINJAUAN HUKUM EKONOMI SYARIAH TERHADAP PRAKTEK SEWA MENYEWA AKUN OJEK ONLINE MAXIM (Studi Kasus di Kota Bengkulu)*. Universitas Islam Negeri Fatmawati Sukarno.