Journal of Cyber Law and Information Security
Volume 1, Number 2, 2022

E-Commerce Fraud and Consumer Protection in Indonesia: Evaluating the Effectiveness and Limitations of Existing Legal Safeguards

Vania Anindya[1*]

[1] Universitas Pakuan, Bogor, Indonesia

Abstract

Article history:
Received: July 26, 2022
Revised: August 13, 2022
Accepted: October 17, 2022
Published: December 30, 2022

Keywords:
Consumer Protection, Digital Fraud, E-Commerce, Electronic Transactions, Platform Responsibility.

Identifier:
Zera Open
Page: 115-135
https://zeraopen.com/journal/jclis

E-commerce growth in Indonesia has expanded consumer access to digital markets, but it has also increased exposure to fraud, including fake sellers, non-delivery of goods, misleading advertisements, off-platform payment redirection, and data-related risks. This study examines two main questions: how effective Indonesia's existing legal safeguards are in protecting consumers from e-commerce fraud, and why the consumer protection framework must be re-evaluated in response to evolving digital risks. Using a normative legal approach, the article analyzes consumer protection law, electronic transaction regulation, electronic system obligations, and rules on trading through electronic systems. The discussion shows that Indonesian law already provides a relevant legal foundation through recognition of consumer rights, electronic contracts, electronic evidence, business obligations, and complaint mechanisms. However, these safeguards remain limited in practical enforcement, seller traceability, platform accountability, preventive supervision, and accessible dispute resolution. The study finds that consumer protection must be strengthened through clearer platform responsibility, stronger system supervision, faster remedies, and closer integration between consumer protection and information security.

*Corresponding author:
(Vania Anindya)

1. Introduction

The rapid expansion of e-commerce has transformed consumer transactions in Indonesia from conventional face-to-face exchanges into electronic interactions mediated by digital platforms, websites, marketplaces, and payment systems. This transformation has improved market access, reduced transaction barriers, and enabled consumers to compare goods and services more efficiently. However, the same digital environment has also created legal vulnerabilities because parties often transact without physical contact, direct verification of seller identity, or full certainty regarding product quality, delivery, and refund mechanisms. In this context, consumer protection is not merely a matter of private contract enforcement, but also a question of whether the legal framework can ensure fairness, accountability, and legal certainty in electronic commerce.

Indonesian positive law already provides several safeguards relevant to e-commerce fraud. Law Number 8 of 1999 concerning Consumer Protection establishes consumer rights, business actor obligations, prohibition of misleading information, and mechanisms for dispute resolution. Law Number 19 of 2016, which amended the Electronic Information and Transactions Law, strengthens the legal recognition of electronic information, electronic contracts, and electronic evidence. Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operation also requires electronic system operators to maintain secure and reliable systems, while Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems further regulates business obligations in online trade. Normatively, these instruments show that Indonesia has

not left e-commerce transactions outside the scope of law. Yet, the continuing occurrence of online fraud indicates that the existence of legal norms does not automatically guarantee effective protection in practice.

Previous legal studies show that the main challenge lies in the gap between formal regulation and practical enforcement. Erlinawati and Nugrahaningsih (2017) argue that the Consumer Protection Law can be applied to online business, but its effectiveness is influenced by consumer awareness, business compliance, and institutional enforcement. Setyawati et al. (2017) also emphasize that electronic transaction agreements often place consumers in a weaker bargaining position because contractual terms are commonly prepared unilaterally by business actors. This condition becomes more problematic when consumers are required to pay first, while the seller controls product information, delivery certainty, and post-transaction remedies.

The problem is also linked to the legal character of electronic contracts. Atikah (2018) explains that online sale and purchase transactions remain legally binding when they fulfill general contractual requirements, but their electronic format raises difficulties in proving consent, verifying identity, and ensuring that consumers receive accurate information. Sommaliagustina (2018) similarly notes that e-commerce is vulnerable to default, especially when goods are not delivered, do not match descriptions, or when sellers cannot easily be traced. Ranto (2019) further distinguishes preventive and repressive consumer protection, showing that Indonesian law provides both forms of protection, although the repressive mechanism often becomes less meaningful when consumers face complex

procedures, low claim values, or unclear responsibility among sellers and platform providers.

These weaknesses are reflected in public cases. The Grab Toko case, for example, involved consumers who paid for electronic goods but did not receive the promised products, causing significant losses and highlighting the risks of deceptive online stores using attractive prices and digital promotion. CNN Indonesia reported that the case affected hundreds of consumers and caused losses estimated at Rp17 billion (CNN Indonesia, 2021a). Online fraud reports also showed that fraudulent selling remained one of the most frequent complaint categories in digital transactions (CNN Indonesia, 2021b). In addition, the Tokopedia data breach incident illustrated that consumer harm in e-commerce is not limited to non-delivery or fake goods, but also includes information security risks that may expose users to further fraud (CNN Indonesia, 2020).

The urgency of studying this issue lies in the fact that e-commerce fraud tests the capacity of Indonesian law to respond to digital transactions that are fast, cross-regional, and often anonymous. Moha et al. (2020) highlight the importance of electronic system operator registration because it can help consumers identify legitimate business actors and support government supervision. Astari et al. (2020) also stress that supervision is essential to ensure that e-commerce business activities do not undermine consumer rights. Therefore, this article adopts a normative legal approach to evaluate the effectiveness and limitations of existing legal safeguards in protecting Indonesian consumers from e-commerce fraud. The discussion is guided by two research questions: how effective are Indonesia's existing legal safeguards in

protecting consumers from e-commerce fraud? and why is the re-evaluation of Indonesia's consumer protection framework urgent in addressing the evolving risks of e-commerce fraud?

2. Research Methods

This study uses a normative legal research method to examine the effectiveness and limitations of Indonesia's existing legal safeguards in protecting consumers from e-commerce fraud. A normative approach is appropriate because the focus of the study is not to measure consumer experiences empirically, but to analyze legal norms, regulatory structures, and doctrinal principles that govern electronic commerce, consumer rights, business obligations, and electronic transaction security. Through this approach, the article evaluates whether the current legal framework provides sufficient protection against fraudulent practices in digital trade and whether its regulatory design remains adequate in responding to the evolving risks of e-commerce transactions.

The research applies statutory, conceptual, and analytical approaches. The statutory approach is used to examine relevant Indonesian legal instruments, particularly Law Number 8 of 1999 concerning Consumer Protection, Law Number 19 of 2016 concerning the amendment to the Electronic Information and Transactions Law, Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operation, and Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems. These regulations are analyzed to identify the rights, obligations, prohibitions, liabilities,

and dispute resolution mechanisms available for consumers and business actors in e-commerce transactions. The conceptual approach is used to clarify key legal concepts such as consumer protection, electronic contracts, misleading information, platform responsibility, legal certainty, and preventive and repressive protection. Meanwhile, the analytical approach is applied to assess the gap between the normative content of the law and the practical challenges arising from fraud in online transactions.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include statutes and government regulations related to consumer protection and electronic commerce. Secondary legal materials include peer-reviewed journal articles, scholarly legal studies, and reputable academic discussions on e-commerce, electronic transactions, consumer vulnerability, and digital fraud. Reputable news reports are used only as supporting materials to illustrate selected fraud cases and public complaints, not as the main basis for legal interpretation. Tertiary materials, such as legal dictionaries and official institutional explanations, are used where necessary to support conceptual clarification.

The collected materials are analyzed qualitatively through descriptive and prescriptive legal analysis. Descriptive analysis is used to explain the scope and structure of the existing safeguards, while prescriptive analysis is used to evaluate whether those safeguards are adequate and what improvements may be necessary. The analysis is organized according to the two research questions: first, the effectiveness of Indonesia's legal safeguards in protecting consumers from e-

commerce fraud; and second, the urgency of re-evaluating the consumer protection framework in response to evolving digital fraud risks.

3. Results and Discussion

3.1. How Effective Are Indonesia's Existing Legal Safeguards in Protecting Consumers from E-Commerce Fraud?

Indonesia's existing legal safeguards provide an important normative foundation for protecting consumers from e-commerce fraud, but their effectiveness remains partial. From a statutory perspective, consumer protection in e-commerce is supported by several legal instruments, particularly Law Number 8 of 1999 concerning Consumer Protection, Law Number 19 of 2016 concerning the amendment to the Electronic Information and Transactions Law, Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operation, and Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems. These regulations collectively recognize consumer rights, business actor obligations, electronic contracts, electronic evidence, electronic system reliability, and obligations in online trade. Therefore, the issue is not the complete absence of regulation, but whether the available legal safeguards are sufficiently operational, accessible, and enforceable in the specific context of e-commerce fraud.

Law Number 8 of 1999 concerning Consumer Protection remains the primary legal basis for consumer rights in Indonesia. It recognizes the consumer's right to comfort, security, and safety in consuming goods or services; the right to correct,

clear, and honest information; the right to be heard; the right to advocacy and dispute settlement; and the right to compensation when goods or services are not as agreed. In e-commerce fraud cases, these rights are highly relevant because fraud usually begins with an imbalance of information. Consumers rely on product descriptions, seller identity, digital advertisements, payment instructions, and marketplace mechanisms. When a seller provides false information, fails to deliver goods, sends goods that do not match the description, or disappears after receiving payment, the consumer's right to information and right to compensation are directly violated. Erlinawati and Nugrahaningsih (2017) argue that the Consumer Protection Law can be applied to online business activities because the relationship between consumers and business actors still exists even when the transaction occurs electronically. This means that online transactions should not reduce the legal position of consumers.

However, the effectiveness of the Consumer Protection Law is limited by the fact that it was enacted before the rapid development of marketplace-based transactions. The law was designed mainly for conventional consumer transactions, where the identity of the business actor, the place of transaction, and the route for complaint are relatively easier to identify. In contrast, e-commerce transactions may involve several parties, including the seller, marketplace provider, payment service provider, courier, and electronic system operator. This multi-actor structure complicates responsibility. When fraud occurs, consumers often face uncertainty about whether the seller, platform, or another intermediary should be held responsible. Rahmana and Suparto (2019) explain that consumers in e-commerce

often bear a greater risk than business actors because online transactions commonly use standard-form contracts and consumers are placed in a passive position. This weak bargaining position reduces the practical effectiveness of legal safeguards even when consumer rights are formally recognized.

The Electronic Information and Transactions Law also contributes to consumer protection by recognizing electronic information, electronic documents, and electronic contracts as valid legal instruments. This is important because proof in e-commerce fraud cases often depends on screenshots, chat records, invoices, transfer receipts, transaction histories, and platform notifications. Atikah (2018) notes that online sale and purchase transactions remain legally binding as long as they fulfill general contractual requirements. Therefore, electronic form does not invalidate the agreement. Handriani (2020) further explains that consumer protection in online sale and purchase agreements must be understood through the relationship between contractual validity, consumer rights, and the responsibility of business actors to provide goods according to the information promised. This provides a legal basis for consumers to claim that a transaction existed and that the seller breached the agreement. Nevertheless, evidentiary recognition alone does not fully solve the enforcement problem. Consumers may have proof of payment or proof of communication, but they may still struggle to identify the seller, locate the responsible party, or pursue remedies when the value of the loss is relatively small compared with the cost and complexity of legal action.

Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems strengthens consumer protection by requiring business actors in

electronic trade to provide clear identity, accurate information, complaint services, and mechanisms for resolving consumer problems. This regulation is more specific to e-commerce than the Consumer Protection Law and therefore has stronger relevance to online fraud. It addresses the need for transparency in digital trade and requires business actors to support consumer complaint mechanisms. Moha et al. (2020) emphasize that registration of electronic system operators is important because it supports supervision and helps consumers identify legitimate business actors. In this sense, the regulation has preventive value: it seeks to reduce fraud before it occurs by making online business actors more visible, accountable, and traceable.

However, the practical effectiveness of this safeguard depends on supervision, compliance, and enforcement. If sellers can easily create accounts, use false identities, move between platforms, or communicate with consumers outside official marketplace channels, the preventive function of the regulation becomes weaker. Sommaliagustina (2018) notes that e-commerce transactions are vulnerable to default, including goods not being sent or goods not matching what was promised. These forms of default often overlap with fraud when the seller intentionally misleads consumers from the beginning. In such cases, the distinction between civil breach of contract and criminal fraud may become blurred. This creates a further limitation because consumers may be uncertain whether to pursue a civil claim, submit a complaint to a marketplace, report to consumer dispute institutions, or file a criminal report.

Marketplace responsibility is one of the most important issues in evaluating the effectiveness of existing safeguards. Marketplaces are not always the direct sellers, but they provide the digital infrastructure where transactions occur. They manage seller registration, product display, payment flows, complaint channels, rating systems, and sometimes escrow mechanisms. Winarsih and Oktaviarni (2021) found that marketplace providers are responsible for providing complaint facilities, following up consumer problems, mediating between sellers and consumers, and ensuring the operation of their electronic systems, although this responsibility has not been implemented optimally. This finding is important because it shows that platform responsibility exists, but its practical reach is still limited. If the marketplace only acts after a complaint is submitted, protection becomes reactive rather than preventive.

In the Grab Toko case, consumers were reportedly attracted by offers of electronic goods at unusually low prices, paid for the products, but did not receive them. The case illustrates a serious weakness in preventive consumer protection because the fraudulent scheme was able to operate long enough to cause substantial losses. Although consumers could theoretically rely on consumer protection law, electronic transaction law, and criminal law, the harm had already occurred. The case shows that effectiveness cannot be measured only by whether legal rules exist, but also by whether those rules can prevent deception, detect suspicious business behavior, stop fraudulent actors early, and provide quick remedies to affected consumers. Ranto (2019) distinguishes preventive and repressive protection and suggests that both are necessary. In the context of e-commerce fraud, preventive

protection includes transparency, seller verification, platform monitoring, and secure payment systems, while repressive protection includes compensation, dispute settlement, administrative sanctions, and criminal enforcement.

The Tokopedia data breach incident also expands the meaning of consumer protection in e-commerce. Fraud risk is not limited to fake goods or non-delivery. When consumer data is exposed, fraudsters may use personal information for phishing, impersonation, account takeover, or further scams. Government Regulation Number 71 of 2019 requires electronic system operators to maintain secure and reliable systems, but data security incidents show that regulatory obligations must be matched by technical compliance and strong supervision. Astari et al. (2020) argue that supervision is necessary to ensure that e-commerce business activities do not harm consumer rights. In this regard, legal effectiveness depends on the state's ability to supervise electronic system operators, impose sanctions, and ensure that digital platforms maintain adequate security standards.

Therefore, Indonesia's existing legal safeguards are normatively relevant and partially effective. They provide legal recognition of consumer rights, electronic contracts, electronic evidence, business obligations, complaint mechanisms, and platform responsibility. Yet, their limitations appear in enforcement, platform accountability, consumer access to remedies, seller traceability, and the speed of regulatory response. The legal framework can protect consumers after fraud occurs, but it is less effective in preventing fraud before harm arises. This means that the current safeguards function more strongly as a formal legal basis than as a fully effective protective system.

3.2. Why Is the Re-Evaluation of Indonesia's Consumer Protection Framework Urgent in Addressing the Evolving Risks of E-Commerce Fraud?

The re-evaluation of Indonesia's consumer protection framework is urgent because e-commerce fraud evolves more quickly than traditional legal enforcement mechanisms. Digital fraud is adaptive. Fraudsters can use fake stores, manipulated reviews, false discounts, social media advertisements, phishing links, impersonated customer service accounts, and payment redirection schemes. These practices exploit consumer trust and the speed of online transactions. While the existing legal framework recognizes consumer rights and business obligations, it does not always provide sufficiently detailed mechanisms for addressing the specific operational risks of platform-based commerce. As a result, the law may remain formally valid but practically insufficient.

One reason re-evaluation is necessary is the changing structure of e-commerce itself. Earlier consumer protection models assumed a relatively direct relationship between consumer and business actor. Modern e-commerce, however, often involves platform intermediaries. Consumers may believe they are protected because they transact through a recognizable marketplace, even though the seller is a separate third party. This creates a legal expectation gap. Consumers expect the platform to guarantee safety, while platforms may limit their responsibility through terms and conditions. Setyawati et al. (2017) argue that electronic transaction agreements often place consumers in a weaker position because contractual terms are commonly determined by business actors. This issue becomes more significant

in marketplace transactions where consumers rarely read or negotiate standard terms, and where limitation-of-liability clauses may reduce platform responsibility.

Re-evaluation is also urgent because consumer harm in e-commerce is often small in individual value but large in cumulative impact. A single consumer may suffer a loss that is not economically worth litigating, but many consumers may experience similar losses across platforms. This creates an access-to-justice problem. Formal remedies through court proceedings may be too costly, slow, and complex for ordinary e-commerce disputes. Consumer dispute settlement mechanisms exist, but they may not always be well integrated with digital platforms or online evidence systems. Setiantoro et al. (2018) argue that consumer protection in e-commerce requires stronger preventive protection and more effective dispute settlement mechanisms, including non-litigation and online dispute resolution. This is especially relevant because e-commerce disputes are digital in nature and therefore need remedies that are also fast, accessible, and digitally compatible.

Another urgency arises from the blurred boundary between civil, administrative, and criminal responsibility. When goods are not delivered, the case may be treated as breach of contract. When the seller intentionally deceives the buyer, it may become fraud. When the platform fails to supervise its system or allows misleading content to continue, administrative responsibility may also be relevant. This overlap can create confusion for consumers and enforcement bodies. If the legal framework does not clearly allocate responsibility among sellers, platforms, and system operators, consumer protection becomes fragmented. Ranto (2019) emphasizes that consumer protection must include both preventive and repressive

dimensions. However, in practice, consumers may move from marketplace complaint channels to police reports to consumer institutions without receiving a clear or timely remedy.

The increasing importance of personal data and information security also makes re-evaluation necessary. E-commerce fraud is now closely connected with data misuse. Personal data, phone numbers, addresses, transaction histories, and account credentials can become tools for further fraud. Although the article focuses on the pre-Personal Data Protection Law period, Government Regulation Number 71 of 2019 already required electronic system operators to ensure system reliability and security. Still, incidents involving user data show that general security obligations may not be enough without clear standards, strong audits, breach notification duties, and effective sanctions. The risk is not only financial loss from one transaction, but repeated exposure to scams, phishing, and impersonation. Therefore, consumer protection must be understood as part of information security governance.

Re-evaluation is also needed because the growth of digital trade increases dependency on consumer trust. E-commerce can only function sustainably when consumers believe that sellers are identifiable, payments are secure, products are accurately described, complaints are handled fairly, and fraudulent actors can be removed quickly. If legal safeguards are perceived as weak, consumers may become reluctant to transact online or may depend only on platform reputation rather than legal certainty. Astari et al. (2020) stress the importance of supervision in ensuring that e-commerce activities do not harm consumer rights. Supervision is not merely a bureaucratic function. It is a mechanism for maintaining trust in the digital market.

A further reason for re-evaluation is the need to clarify platform responsibility. Marketplaces occupy a strategic position because they are closer to transaction data than regulators or courts. They can detect suspicious seller behavior, unusual transaction patterns, repeated complaints, fake reviews, and misleading product listings. Therefore, platform responsibility should not be limited to providing complaint channels after consumers suffer losses. It should include stronger preventive obligations, such as seller verification, proactive monitoring of high-risk products or suspicious pricing, transparent refund procedures, and cooperation with law enforcement. Winarsih and Oktaviarni (2021) show that marketplace responsibility includes complaint handling and system operation, but implementation remains less than optimal. This supports the argument that regulatory strengthening should move from general responsibility toward clearer operational standards.

The normative evaluation also shows that the current framework should better integrate consumer protection with digital literacy. Legal safeguards cannot operate effectively if consumers do not understand how to identify fraud, use official complaint mechanisms, preserve electronic evidence, and avoid off-platform transactions. However, consumer education should not be used to shift responsibility away from business actors or platforms. The law must balance consumer caution with institutional accountability. Erlinawati and Nugrahaningsih (2017) emphasize that implementation of consumer protection in online business is affected by awareness and enforcement. Thus, strengthening the framework requires both legal reform and practical education.

In light of these considerations, the re-evaluation of Indonesia's consumer protection framework is urgent for three main reasons. First, e-commerce fraud has become more complex, involving not only non-delivery of goods but also misleading digital promotion, fake sellers, identity concealment, and data-related risks. Second, the existing legal framework still leaves practical gaps in enforcement, dispute resolution, and platform responsibility. Third, consumer trust in digital markets depends on legal safeguards that are preventive, responsive, and technologically relevant. The law must therefore evolve from merely recognizing consumer rights to ensuring that those rights can be exercised effectively in the digital marketplace.

Overall, the results of this normative analysis indicate that Indonesia already has a legal foundation for protecting consumers from e-commerce fraud, but the framework requires strengthening. The Consumer Protection Law, Electronic Information and Transactions Law, and regulations on electronic systems and online trade provide essential rules, yet they must be supported by clearer platform obligations, faster dispute resolution, stronger supervision, reliable seller verification, and better integration between consumer protection and information security. Without such re-evaluation, legal protection may remain formal rather than functional, leaving consumers exposed to fraud risks that continue to develop alongside the expansion of e-commerce.

4. Conclusion

This study concludes that Indonesia's existing legal safeguards provide a relevant but still limited foundation for protecting consumers from e-commerce

fraud. Law Number 8 of 1999 concerning Consumer Protection remains important because it recognizes basic consumer rights, including the right to safety, accurate information, complaint mechanisms, and compensation. The Electronic Information and Transactions Law also supports consumer protection by recognizing electronic information, electronic documents, and electronic contracts as legally valid instruments. In addition, Government Regulation Number 71 of 2019 and Government Regulation Number 80 of 2019 strengthen the regulatory basis for electronic system reliability, business identity, information transparency, complaint services, and obligations in online trade. Normatively, these instruments show that e-commerce transactions are not outside the reach of Indonesian law. However, the effectiveness of these safeguards remains partial because the available rules are stronger as a formal legal basis than as a fully operational mechanism for preventing fraud.

In practice, consumers may still face difficulties in identifying fraudulent sellers, proving bad faith, locating responsible parties, and obtaining quick remedies. E-commerce fraud often involves multiple actors, including sellers, platforms, payment service providers, couriers, and electronic system operators, which may create uncertainty regarding liability. Although marketplace providers have an important role in transaction safety, their responsibility is often implemented reactively through complaint handling rather than proactively through seller verification, suspicious transaction monitoring, and early fraud prevention. The findings also show that re-evaluating Indonesia's consumer protection framework is urgent because e-commerce fraud continues to evolve alongside digital trade. Fraud

is no longer limited to non-delivery of goods, but may also involve misleading advertisements, fake stores, false discounts, impersonation, phishing, off-platform payment redirection, and misuse of consumer data. This development requires consumer protection to be integrated with information security, platform governance, and accessible digital dispute resolution.

Therefore, strengthening the current framework should focus on several key areas. Platform responsibility should be clarified through stricter obligations for seller verification, transparent complaint handling, refund mechanisms, and cooperation with law enforcement. Dispute resolution should also become faster, cheaper, and more compatible with digital evidence and low-value online claims. In addition, supervision of electronic system operators must be improved to ensure compliance with security, transparency, and accountability obligations. Consumer education remains important, but it should not shift responsibility away from business actors and platforms that have greater control over digital transaction systems. Overall, Indonesian law has established an important foundation for consumer protection in e-commerce, but it must be re-evaluated and strengthened so that legal protection does not remain merely formal, but becomes practical, preventive, and responsive to the changing risks of digital fraud.

References

Astari, A. A. M. A. R. L., Budiartha, I. N. P., & Ujianti, N. M. P. (2020). Pengawasan terhadap transaksi bisnis e-commerce dalam mewujudkan perlindungan konsumen. *Jurnal Konstruksi Hukum, 1*(1), 38–43.

Atikah, I. (2018). Pengaturan hukum transaksi jual beli online (e-commerce) di era teknologi. *Muamalatuna, 10*(2), 1–27.

CNN Indonesia. (2020, May 3). Kronologi lengkap 91 juta akun Tokopedia bocor dan dijual. *CNN Indonesia*. Retrieved Apr 2, 2022 from https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

CNN Indonesia. (2021a, January 15). Kronologi Grab Toko tipu 980 orang dan rugikan Rp17 M. *CNN Indonesia*. Retrieved March 13, 2022 from https://www.cnnindonesia.com/ekonomi/20210115135836-92-594181/kronologi-grab-toko-tipu-980-orang-dan-rugikan-rp17-m

CNN Indonesia. (2021b, October 15). Kominfo catat kasus penipuan online terbanyak: Jualan online. *CNN Indonesia*. Retrieved March 8, 2022 from https://www.cnnindonesia.com/teknologi/20211015085350-185-708099/kominfo-catat-kasus-penipuan-online-terbanyak-jualan-online

Erlinawati, M., & Nugrahaningsih, W. (2017). Implementasi Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen terhadap bisnis online. *Jurnal Serambi Hukum, 11*(1).

Handriani, A. (2020). Perlindungan konsumen dalam perjanjian transaksi jual beli online. *Pamulang Law Review, 3*(2), 127–138.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2021, August 19). *Siaran pers No. 293/HM/KOMINFO/08/2021 tentang waspada jerat penipuan online, Kominfo tunjukkan 5 modus pelaku dan langkah pelindungan data.* https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-293-

hm-kominfo-08-2021-tentang-waspada-jerat-penipuan-online-kominfo-tunjukkan-5-modus-pelaku-dan-langkah-pelindungan-data

Moha, M. R., Sukarmi, S., & Kusumadara, A. (2020). Urgensi pendaftaran penyelenggara sistem elektronik bagi pelaku usaha e-commerce. *Jambura Law Review, 2*(2), 101–119.

Rahmana, D. M., & Suparto, S. (2019). Consumer protection and responsibility of business actors in electronic transactions (e-commerce). *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan, 2*(2), 213–225.

Ranto, R. (2019). Tinjauan yuridis perlindungan hukum terhadap konsumen dalam transaksi jual beli melalui media elektronik. *Jurnal Ilmu Hukum: Alethea, 2*(2), 145–164.

Setiantoro, A., Putri, F. D., Novitarani, A., & Njatrijani, R. (2018). Urgensi perlindungan hukum konsumen dan penyelesaian sengketa e-commerce di era Masyarakat Ekonomi ASEAN. *Jurnal RechtsVinding: Media Pembinaan Hukum Nasional, 7*(1), 1–17.

Setyawati, D. A., Ali, D., & Rasyid, M. N. (2017). Perlindungan bagi hak konsumen dan tanggung jawab pelaku usaha dalam perjanjian transaksi elektronik. *Syiah Kuala Law Journal, 1*(3), 46–64.

Sommaliagustina, D. (2018). Perlindungan hukum terhadap konsumen e-commerce di Indonesia. *Journal Equitable, 3*(2), 47–58.

Winarsih, I., & Oktaviarni, F. (2021). Tanggung jawab penyedia layanan aplikasi marketplace terhadap konsumen dalam transaksi jual beli online di Provinsi Jambi. *Zaaken: Journal of Civil and Business Law, 2*(2), 349–367.