Eduvest – Journal of Universal Studies
Volume 4 Number 12, December, 2024
p- ISSN 2775-3735- e-ISSN 2775-3727

THE VULNERABILITY OF E-COMMERCE AS A CRIME MEANS OF MONEY LAUNDERING

Danang Tri Hartono[1], Dominikus Rato[2], Bayu Dwi Anggono[3]
Univesitas Jember, Indonesia [1,2,3]
Email: hartonodanang@gmail.com

ABSTRACT

Technological advances in the field of the internet and its supporting ecosystem have changed human lives. The way humans communicate, transact, trade and play games has changed massively. Along with the progress of the internet ecosystem, it has led to the emergence of trading platforms, both webservices and smartphone applications. Developments that change how people trade and pay for trade transactions cause vulnerabilities that can be used by criminals or to commit criminal acts. Criminal acts of fraud, unauthorized use of personal data, bribery through e-commerce media, and money laundering are criminal acts that have emerged along with the rampant use of e-commerce. Various methods of money laundering can be done using e-commerce media. One of the mitigations that can be done by the Government is to classify e-commerce media as a Reporting Party in the anti-money laundering regime.

KEYWORDS *E-commerce, Money Laundering Modes, Technological advances*

INTRODUCTION

The development of information technology has caused the digital world to move very quickly, thus affecting various aspects of human life. The digital world affects how humans communicate, transact, trade and seek information and entertainment. In the non-digital era, humans trade by meeting face-to-face with buyers and bringing goods to be sold. In the non-digital era, humans physically bring money that will be used for transactions, as well as meet to bargain. The digital world has changed everything. People trade to make trades simply through digital platforms, without the limitations of space and time. People from the North Pole can buy goods from Indonesia with just one app in hand. The internet and digital worlds have changed everything.

The development of information technology in Indonesia has been nauseous since 1967, when the Indonesian Government allowed the entry of computer technology from abroad (Andyni & Kurniasari, 2021). At that time, computers were still a very luxurious item. Its use is still limited in government agencies or companies that are already very large. In the 1990s in Indonesia, more sophisticated

How to cite: Danang Tri Hartono, et al. (2024). The Vulnerability of E-Commerce As A Crime Means of Money Laundering. *Journal Eduvest. 4*(12): 12251-12263
E-ISSN: 2775-3727

and more compact Personal Computers began to enter Indonesia. Various new operating systems are also starting to emerge. In this era, the Pentium II computer from Intel Corporation began to be popular in Indonesia. This type of computer is slowly starting to replace the functions of the typewriter. Significant changes occurred in the 2000s. Pentium III computers with CPU stands are starting to gain popularity (Geriadi et al., 2023). At the beginning of this era, Windows 98 was still quite popular before it was finally displaced by Windows XP. In 2002, the Pentium IV began to appear. It was from this moment that a turning point occurred and improvements in computer specifications continued to occur. Computer capabilities have been increasingly used since the emergence of the use of cellular phones that have computer-like capabilities. This has further accelerated the growth of the use of cellular phones since the advent of the internet. Indonesia's internet users in the early 2000s were only around 2 million. It experienced a significant increase in 2011 with the number of users reaching 43 million people. Internet users in Indonesia in 2021 have increased significantly, reaching 202.6 million. There was an increase of around 15.5 percent from the beginning of 2020. This development was further accelerated by the occurrence of the covid 19 pandemic. With the pandemic causing people to have to practice social distancing, digital development is accelerating (Astohar et al., 2022). This also causes a shift in the behavior of some people who mostly make purchases in shopping centers, shifting to online shopping through e-commerce platforms.

Based on Statista research data, by 2030, Indonesia's e-commerce market is predicted to generate around 160 billion US dollars in online retail sales, up from 58 billion US dollars, in 2022. By 2030, Indonesia is expected to account for more than 42 percent of the Southeast Asian e-commerce market likely due to the growth of the middle class and increasing access to the internet. Other emerging markets including Malaysia, the Philippines, Thailand, and Vietnam are also growing rapidly (Rani & Desiyanti, 2024). The development of the internet and the digital world has given rise to new innovations related to trading platforms or so-called ecommerce. The development of platforms that change how people trade and transact has given rise to new crime phenomena. These crimes can be in the form of fraud or money laundering.

Money laundering is basically disguising the proceeds of criminal acts to look like legal funds. The mode or typology of money laundering continues to change along with the development of technology, financial instruments and their supporting ecosystems. The international anti-money laundering community that is a member of the Financial Action Task Force (FATF) continues to conduct studies and updates related to the development of this typology. However, international policies or standards will always lag behind what is done by the perpetrators of criminal acts. Anticipating the development of information technology, the government has issued Law Number 11 of 2008 concerning Information and Electronic Transactions which has been perfected through Law Number 19 of 2016. Meanwhile, in terms of anti-money laundering, Indonesia already has Law number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (Amrin et al., 2022).

In this paper, the author will discuss ecommerce that can be used as a means of committing criminal acts, including money laundering. According to Muchsin, legal protection is an activity to protect individuals by harmonizing the relationship between values or principles that are embodied in attitudes and actions in creating order in life among fellow humans. With the emergence of e-commerce and its supporting ecosystem, it must be legally ensured that the media has been able to protect citizens from crimes that arise. The government should continue to conduct studies and observe the development of the financial industry to protect Indonesia from money laundering crimes.

RESEARCH METHOD

E-commerce and Crime

1) E-commerce Development

E-commerce is basically a buying and selling platform, which brings together sellers and buyers in one technology platform. What is traded in e-commerce can be in the form of goods or services. Before the advent of e-commerce, people bought and sold on the spot physically, but with e-commerce platforms people met virtually by viewing the goods sold virtually and completing transactions electronically (Salsabella, 2022). Judging from this, it can be concluded that the development of e-commerce platforms cannot be separated from the development of the payment system itself.

E-commerce or electronic commerce, also known as e-business, refers to the transaction of goods and services through electronic communication. Although the general public has become familiar with e-commerce in just the last decade, e-commerce has actually been around for more than 30 years. There are two basic types of e-commerce: business-to-business (B2B) and business-to-consumer (B2C). In B2B, companies conduct business with suppliers, distributors, and other partners through electronic networks. In B2C, companies sell products and services to consumers. Although B2C is better known to the general public, B2B is the form that actually dominates e-commerce in terms of revenue. (History of E-commerce, University of Missouri, 2006)

The evolution of e-commerce has been studied and followed up by several researchers and stakeholders in the field. The advancement of Information Technology, more precisely related to the development of the Internet, since the 1990s has increased rapidly. According to (Albertin, 2012) the evolution of e-commerce can be divided into four phases. In the first phase, organizations use the Internet function for the process of disseminating information about their products and services. It was the initial stimulus for the development of e-commerce. Still according to the author, the second stage, is to receive orders and send information and instructions on the utilization of their products and services. In this phase, it was first used for supervision and carrying out logistics distribution within the company (Safira & Dewi, 2019).

The third phase of evolution, according to (Albertin, 2012) is the distribution of products and services using Information Technology (IT). In this phase, several products began to be commercialized digitally, such as music and software. For the latter comes the phase that consolidates e-commerce, with interaction between

sellers and consumers, no longer transmitting data or delivering products and services only. With the advancement of IT and the widespread use of the Internet, such interactions allow simple internet users to become potential consumers, using e-commerce. This enables a true revolution in how to commercialize products, services, and information, bringing more convenience and a wide variety of offers and choices to consumers, but also to sellers.

2) Crime in the World of E-commerce

a) Crimes related to the Platform

An e-commerce platform is basically a medium where sellers and buyers meet. In the platform provided by the organizer, sellers can upload photos of goods and/or descriptions of the goods sold along with the prices offered on the platform. Meanwhile, buyers can enter the platform and search for the goods or services needed and then place orders and payments. What can be categorized as a crime in terms of platforms is a crime that is organized in such a way that it involves the ecommerce platform itself (Sensuse et al., 2020).

Crimes that arise in terms of platforms can be categorized into at least 2 types, namely:

i) Customer data protection

Upon entering the platform, both the seller and the buyer are required to enter personal data into the available platform. Personal data, in practice, can be worth money and sold to other parties. So there are legal consequences if there is a leak of personal data, whether it is done intentionally or unintentionally.

ii) Use of fake websites

Fake websites are usually used by criminal actors to commit fraud. With a fake website, the website publisher tries to attract buyers, but basically there is not 1 item that with good intentions will be sold by the website owner.

b) Crimes related to the use of the platform

Users of the e-commerce platform can be seen from the seller and buyer side. The crime that usually occurs is the sale of counterfeit goods (fraud). In addition, e-commerce platforms can be used for bribery, where sellers send goods to the party to be bribed without any prior payment. In addition, there are criminal acts through e-commerce platforms related to transactions. Related to transactions using e-commerce, it is prone to crimes in the form of business email compromise, falsification of transaction proofs, and sending funds without the delivery of goods.

RESULT AND DISCUSSION

Ecommerce Vulnerabilities Related to Money Laundering Crimes

Money laundering is an activity to disguise the origin of wealth derived from a criminal act (illegal funds) so that it can be used for both legitimate activities (legal funds) and illegal activities. In short, money laundering is the process of making unauthorized money appear to be money obtained from legitimate activities. When a crime generates large profits, the perpetrator will try to find a way to enjoy the funds by disguising their origins, including to cover up who the people involved in the activity are. The perpetrators of criminal acts do various

things to be able to disguise the source of funds, by changing the form, transferring, exchanging, buying, and bringing to other jurisdictions through various instruments that are unlikely to attract attention. Criminal acts that are the source of money laundering crimes, also known as original criminal acts, have been regulated in Article 2 of Law number 8 of 2010. These criminal acts can be in the form of: corruption, illicit arms trafficking, narcotics trafficking, smuggling of goods, and various other criminal acts related to criminal organizations, embezzlement, insider trading, and various fraud schemes using computers (Rumata & Sastrosubroto, 2017).

Established in 1989, the Financial Action Task Force (FATF) is an intergovernmental body that is a member of the G7 industrialized countries (Group of Seven) that aims to establish and develop international standards on anti-money laundering and countering the financing of terrorism programs. One of the early breakthroughs of the FATF was to socialize that money laundering and terrorism financing are not only limited to cash transactions but can be through a wide variety of other financial instruments. Through several disclosures of the typology of money laundering and terrorism financing, the FATF shows that the crime of money laundering and terrorism financing can actually be carried out through various means, financial institutions or business entities. The 2000 United Nations Convention on Transnational Organized Crime, also known as the "Palermo Convention," states that every country must have adequate rules to criminalize money laundering, trace the flow of funds, freeze transactions, conduct seizures and be willing to cooperate with law enforcement officials in other countries.

1) Ecommerce is not a reporting party

In general, the typology of money laundering is carried out through 3 stages, namely placement, layering and integration. In order to be able to prevent and identify these practices, in the anti-money laundering regime, it has been regulated that every financial institution, provider of goods and services including the profession (accountants, lawyers, notaries, and financial planners) to identify financial transactions using their services that are categorized as suspicious transactions, cash transactions, and other transactions based on the law must be reported.

The development of e-commerce as a buying and selling platform in the current era of digitalization is able to answer human needs. In the digital era that can be accessed anywhere and anytime. Making the digital era without looking at the territorial boundaries of a country jurisdiction (*borderless*). This is certainly a loophole that can be exploited by criminals. Especially e-commerce as a buying and selling platform has become a forum for crime. There are various types of goods that can be traded from cheap goods to luxury goods and from a nominal value of hundreds of rupiah to billions of rupiah. Crimes that are rampant are carried out such as fraud, narcotics trafficking, criminal transactions to money laundering. As the number of e-commerce users and the volume of financial transactions increase, it can disguise criminal activities committed by criminals (Simanjuntak, 2019).

E-commerce is one of the sectors that is very active in financial transactions. However, e-commerce platforms are not classified as direct reporting parties to the

Financial Transaction Reporting and Analysis Center (PPATK). Based on Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (hereinafter referred to as the Anti-Money Laundering Law) in Article 17 paragraph (1) concerning the Reporting Party, there are two (2) types of reporting parties, namely Financial Service Providers (hereinafter referred to as PJK) such as banks, financing companies, insurance companies to money transfer businesses and Goods and Services Providers (hereinafter referred to as PBJ) such as property companies, Motor vehicle traders, precious metals. This is because e-commerce platforms are only an intermediary between sellers and buyers. E-commerce today focuses more on providing buying and selling transaction facilities in offering convenience and convenience of transactions (Yildiz & Koçan, 2018). In positive law in Indonesia, regulations on e-commerce are explicitly contained in Government Regulation of the Republic of Indonesia Number 80 of 2019 concerning Trade Through Electronic Systems. In this regulation, e-commerce platforms are known as Electronic System Trade Organizers (hereinafter abbreviated as PPMSE). In detail the regulations regulate on:

a) The party that conducts PMSE;
b) Requirements in PMSE;
c) PMSE Maintenance;
d) Obligations of Business Actors;
e) Proof of PMSE transactions;
f) Electronic Advertising;
g) Electronic Bidding, Electronic Acceptance and Electronic Confirmation;
h) electronic contracts;
i) Protection of personal data;
j) Payments in PMSE;
k) Delivery of goods and services in PMSE;
l) Exchange of goods or services and cancellation of purchases in PMSE;
m) Dispute resolution in PMSE; and
n) Coaching and Supervision.

In the PPMSE rules, there is an obligation to store PMSE data and information related to financial transactions for a minimum period of 10 (ten) years. The financial transaction information can be used as evidence of valid transactions and can be used as evidence in the trial. However, in this regulation, PPMSE does not have the obligation to actively report financial transactions to relevant institutions, only limited to submitting statistical data information periodically to relevant government institutions.

2) Ecommerce transactions cut off the flow of funds

The ease of accessing e-commerce platforms in buying and selling has an impact on increasing users and transaction volume. This has a positive impact on improving the country's economy, economic growth and development of a country. One of the main factors driving the rapid growth of e-commerce is the ease of making payments. A variety of innovative payment methods have been developed to provide a seamless online shopping experience for consumers. Various payment

methods are provided by e-commerce, namely: credit cards, e-wallets, bank transfers, cash *on delivery*, and installments.

In addition to having a positive impact, e-commerce also has a negative impact as a container for illegal transactions mentioned above. Criminals use e-commerce as a diversion of financial transactions, especially in money laundering crimes. Criminals use e-commerce as a diversion or disguise the flow of funds obtained from the proceeds *of crime*. The ease of various payments provided by e-commerce operators has become a new modus operandi in the criminal process.

The Royal United Service Institute (RUSI) in its study published in January 2020, stated that fictitious transactions between users of e-commerce platforms can be used for money laundering purposes. For example, Alice is in America while Bob is on the island of Bali. Alice wants to send money from the crime to Bob, so Alice can buy the goods sold by Bob. Then Alice will send funds through financial instruments available on the ecommerce platform. Furthermore, the ecommerce platform will forward the payment to Bob's account. However, Bob did not deliver the actual goods to Alice, so the transfer of funds from Alice to Bob had taken place perfectly. In 2015, in the United States, there was a case of terrorism financing through e-commerce media. A U.S. citizen has received $1,200 from a member of Daesh (ISIS), through PayPal under the pretext of selling printers through ebay. For this, the perpetrator was found guilty by a United States court in 2018 and sentenced to 20 years in prison. A similar case also occurred against a company that was involved in an omission in Slovenia called Sis d.o.o. that sold soft frames in the Aple Store. Sis d.o.o. turned out to be owned by a narcotics kingpin who sold steroid-type narcotics. For this case, Aplle has been sanctioned by OFAC in the amount of USD 466,912 for making transfers to people subject to financial sanctions.

Banking is the largest industry in conducting financial transactions. Banking financial products such as deposits, loans, and fund transfer facilities both domestically and abroad are the most transacted instruments by financial service users. Traditionally, buying and selling transactions through banking can be described as follows:

Figure 1. The Transaction Mechanism

In the mechanism mentioned above, the transaction occurs after the buyer sends funds from his account to the buyer's account as a seller and the goods have

been delivered by B to A. With a transaction using an ecommerce platform, the transaction mechanism is as follows:

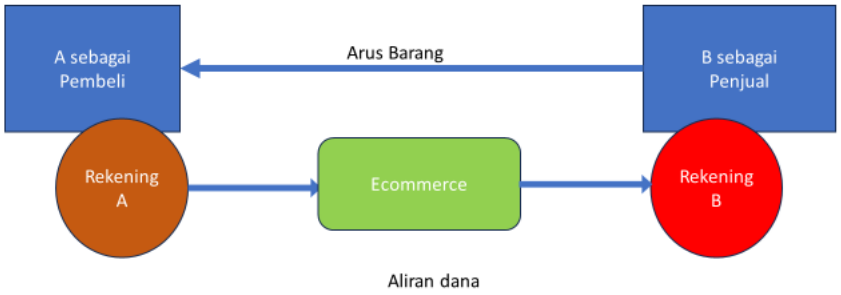

Figure 2. the flow of the transaction

From the flow of the transaction, in terms of financial transactions, in the mutation of account A will see transactions from account A to an e-commerce account and in the mutation of account B there will be incoming funds from the ecommerce account. This will break the transaction between A and B.

Some of the typologies of money laundering that may occur include the following:

1. If A is a narcotics dealer who owns a hotel, then narcotics buyers can book hotels through travel applications (such as booking.com, traveloka, tiket.com, etc.). However, the hotel bookers did not actually come and stay at the hotel. The tjuan of hotel bookings is solely to make narcotics payments. In terms of financial transactions, it will be seen from the mutation of the narcotics buyer's account the money goes out to the travel application, while from the narcotics dealer account it will be seen that money comes in from the payment application platform.
2. Bribery transactions can also be carried out by the bribery making ticket and accommodation reservations on behalf of the person to be bribed.
3. Bribery transactions can also be carried out through ecommerce platforms by carrying out buying and selling activities without using actual goods.

The typology of money laundering transactions through e-commerce platforms will become even more complex with the existence of payment gateways and aggregator solutions. Payment gateways in the arrangement by Bank Indonesia are categorized as Payment Initiation and Acquiring Services (PIAS). According to Article 4 of PBI No.23/6/PBI/2021 concerning Payment Service Providers (PJP),

PIAS activities include the forwarding of payment transactions including: 1. forwarding orders or instructions for the transfer of funds through tools, media, and/or a set of procedures with certain methods or uses of technology in payment transactions; and/or 2. Forwarding payment transaction data in the form of instrument data, nominal payment transaction data, and other payment transaction data. In addition, in forwarding payment transactions, PJP may store data on the source of funds and/or access to the source of funds, process payment transactions, acquire, override payments, and forward funds to providers of goods and/or services.

With the existence of these new instruments, it will cause a longer chain of financial transactions from the source of funds to the final recipient of funds. The transaction can be described as follows:

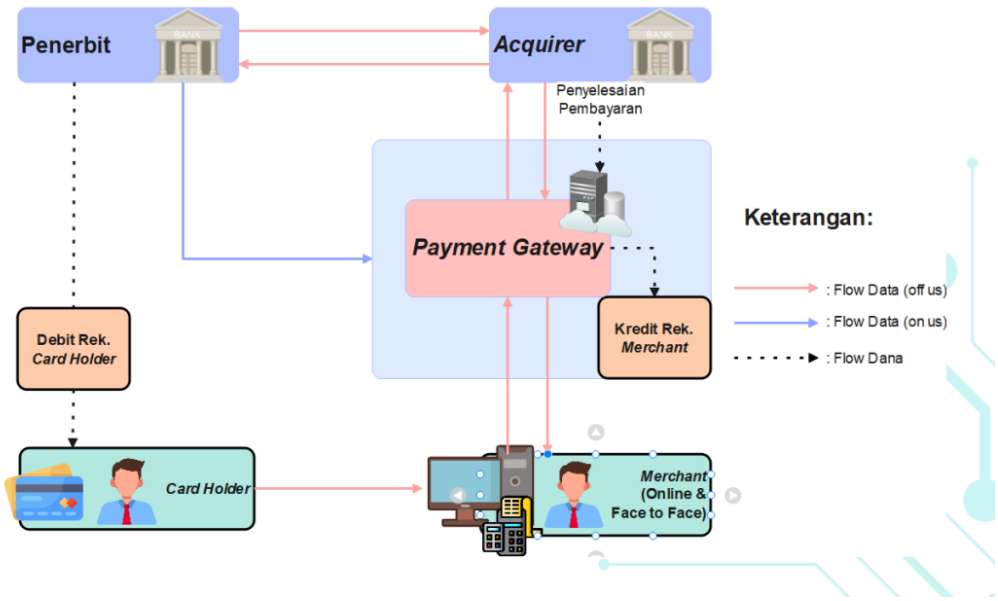

Figure 3. the description of the transaction

From the description of the transaction, it can be seen that the flow of funds will be even longer because it involves the payment gateway as the party that collects transaction data between e-commerce customers and makes the payment stement.

Early detection, the targeted crime of money laundering is carried out by the Reporting Parties as stipulated in Article 17 of Law No. 8 of 2010. In this article, it is stipulated that the Reporting Party consists of Financial Service Providers, Goods and Services Providers and other Reporting Parties that will be regulated in government regulations. In Government Regulation number 61 of 2021 concerning Reporting Parties in the Prevention and Eradication of Money Laundering Crimes, new Reporting Parties have been added in the financial services sector in addition to those regulated in Article 17 of Law number 8 of 2010. The new Complainants include: venture capital companies; infrastructure finance companies; microfinance institutions; export finance institutions; information technology-based money

lending service providers; crowdfunding service providers through information technology-based stock offerings; and information technology-based Financial Transaction service providers. From the addition of the new reporting parties, it can be seen that the addition of new reporting parties has not been able to reach the companies involved in the disconnection of financial transaction funds.

This is certainly used by criminals as a loophole in disguising financial flows to cut off the flow of funds. In countering this, e-commerce platforms should ideally participate in mitigation to anticipate transactions carried out by implementing recognizing service users or *Know Your Customer* (KYC) or *customer due diligence* (CDD) and *Enhanced Due Diligence* (EDD). The application of this principle is carried out to improve transaction security and prevent illegal transactions. This KYC principle is carried out by means of identity verification, phone number verification, address verification, and biometric verification. In the financial service provider sector, the obligation to apply the principle of recognizing service users is regulated in Article 18 of the Anti-Corruption Law. In number (5) there are at least 3 categories of service user principles applied, including:

a) Identification of service users;
b) Verification of service users; and
c) Monitoring of service user transactions.

The Financial Service Provider Reporter in carrying out its obligations applies the KYC principle and reports any suspicious financial transactions to PPATK. There are supervisory and regulatory agencies to carry out supervision of the compliance of financial service providers. The absence of KYC/CDD and EDD procedures on e-commerce platforms and their supporting ecosystems has led to money laundering loopholes that have not been identified by stakeholders. Therefore, it is necessary to pay serious attention from the government to create a legal instrument that can be applied to fill the legal void (*rechtsvacuum*) in resolving this problem.

3) Fraud through e-commerce

ESET in its survey published on November 22, 2021 in Asia Pacific, found several interesting facts. One of them is that three out of four (59 percent) respondents surveyed in Indonesia indicated that they had encountered potentially fraudulent activities online. Another fact found is that 67 percent in Asia Pacific found various online scams in the last 12 months. The most common types are shopping scams in e-commerce (21 percent), social media (18 percent), and investment scams (15 percent). Meanwhile, in Indonesia, the most common types of fraud are e-commerce shopping (19 percent), social media (16 percent), and online investment (9 percent). (ESET cybersecurity survey amongst internet users in APAC reveals large gap between threat awareness and taking action)

The Law on ITE has not regulated a special delicacy regarding Fraud. However, based on Article 45A paragraph (1) Law 19/2016, any person who deliberately and without the right spreads false and misleading news that results in consumer losses in electronic transactions as referred to in Article 28 paragraph (1)

of the ITE Law shall be sentenced to a maximum of 6 years in prison and/or a maximum fine of IDR 1 billion.

To determine whether a person violates Article 28 paragraph (1) of the ITE Law or not, there are several implementation guidelines that must be considered as follows:

i) The criminal offense in Article 28 paragraph (1) of the ITE Law is not a criminal offense against the act of spreading false news (hoaxes) in general, but the act of spreading false news in the context of electronic transactions such as online trade transactions;
ii) News or false information is transmitted through messaging application services, online broadcasting, websites/social media, marketplaces, advertisements, and/or other transaction services through electronic systems;
iii) The form of electronic transaction can be in the form of an engagement between business actors/sellers and consumers or buyers;
iv) Article 28 paragraph (1) of the ITE Law cannot be imposed on parties who commit defaults and/or experience force majeur;
v) Article 28 paragraph (1) of the ITE Law is a material offense, so consumer losses as a result of fake news must be calculated and determined in value.

4) Corruption

Although there has never been a case of corruption using e-commerce that has been declared ineffective, technically e-commerce can be used as a means to commit bribery. To bribe state administrators, a briber can do the following, among others:

a) Buying luxury goods that can be in the form of gold, bags, watches, etc. with the address of the delivery of goods is the address of the person to be bribed.
b) Buying tour packages through e-commerce and those who travel are the ones who will be bribed.
c) State organizers open stores in e-commerce and sell high-value goods at high prices. Furthermore, the briber purchased the goods but the goods were not delivered by the PN.

Technically, these transactions break the transaction between the briber and the person to be bribed. In banking records, it can be seen that funds are sent from the briber to the e-commerce account and not to the account of the person to be bribed. Regarding this incident, according to the author, the ITE Law has not been able to reach him so that the Law on Corruption can be used in the case.

5) Money Laundering Crimes

The prevention and eradication of money laundering has been regulated in Law No. 8 of 2010 concerning the prevention and eradication of anti-money laundering. In its development, the crime of money laundering is increasingly complex, crossing *jurisdictional boundaries* and using increasingly farious modes, utilizing institutions outside the financial system, and has even penetrated into various sectors. In general, the crime of money laundering can be carried out in

several stages, including *placement* or placement of funds from criminal acts in the financial system, *layering* or disguising the transaction of funds resulting from criminal acts in various financial instruments and the third is *integration*, which is the final process of money laundering where the perpetrator tries to enjoy the funds from the proceeds of criminal acts to assets that are visible from legitimate sources.

The use of ecommerce in the context of money laundering can be categorized as happening perfectly. This can happen because *the placement*, *layering* and *integration* processes occur at one time in a series of transactions. For this reason, e-commerce platforms must have an independent mechanism to be able to identify crimes that arise, including money laundering crimes. One of the important things is that ecommerce platforms must be able to identify offers on the platform with abnormal prices. Some of the questions that must be answered related to money laundering using ecommerce platforms are: Whether the platform can identify abnormal amounts, prices and sales and whether the platform can identify whether the goods are actually delivered from the auctions that have been made.

CONCLUSION

The development of the internet and the digital world has given rise to new innovations related to trading platforms or so-called ecommerce. The development of these platforms has changed how people trade and transact so that new crime phenomena have arisen. These crimes can be in the form of bribery, fraud or money laundering. Based on the rules of law and transaction settlement schemes on e-commerce platforms, it can be seen that e-commerce is prone to being used as a means of money laundering. Several cases of using e-commerce platforms for money laundering and terrorism financing have occurred in several countries, and it is likely to have occurred in Indonesia.

There needs to be a rule that requires e-commerce platforms to settle their transactions through financial institutions which based on the rules have been required as a party that is obliged to carry out CDD and EDD related to AML PPT. If in the context of the effectiveness and efficiency of transactions to accelerate national economic growth, the settlement of transactions must still use companies that are not required to carry out CDD and EDD, then it is natural for the relevant institution to review the existence of new reporting parties related to AML PPT in the settlement of e-commerce business transactions.

REFERENCES

Amrin, E., Rismawati, R., Goso, G., & Asriany, A. (2022). Studi Komparasi Layanan Fintech Dalam Meningkatkan Keuangan Inklusif Pada Umkm Di Kota Palopo. *Ecobisma (Jurnal Ekonomi, Bisnis Dan Manajemen)*, *9*(2), 114–125.

Andyni, N., & Kurniasari, F. (2021). Pengaruh literasi dan efikasi diri terhadap inklusi keuangan pada penggunaan layanan pembayaran digital shopee pay di jabodetabek. *Jurnal Manajemen*, *16*(1), 128–140.

Azalia, B. N., & Susanti, S. (2021) Shopee Sumbang Omzet Terbesar untuk

UMKM Saat Pandemi. CNBC Indonesia. https://www.cnbcindonesia.com/entrepreneur/20210504103920-2242959/shopee-sumbang-omzet-terbesar-untuk-UMKM-saat-pandemi

Aoril 2022. Perlindungan hukum terhadap konsumen online, Hukum Online, 25v

Astohar, A., Praptitorini, M. D., & Shobandiyah, S. (2022). Pengaruh literasi keuangan dan layanan keuangan berbasis teknologi terhadap inklusi keuangan (Studi kasus pada UMKM di Kabupaten Demak). *The Academy Of Management and Business*, *1*(2), 69–79.

Danu Wicaksana, Bina Nusantara, 2016. Intruduction to e-commerce in Indonesia and challenges within,

Geriadi, M. A. D., Sawitri, N. P. Y. R., Wijaya, B. A., & Putri, I. G. A. P. T. (2023). Pengaruh Literasi Keuangan Terhadap Inklusi Keuangan Melalui Financial Technology. *Jurnal Studi Manajemen Dan Bisnis*, *10*(2), 178–187.

Rani, G. M., & Desiyanti, R. (2024). Pengaruh Literasi Keuangan, Inklusi Keuangan dan Digital Payment Terhadap Kinerja UMKM Makanan & Minuman di Kota Padang. *EKOMABIS: Jurnal Ekonomi Manajemen Bisnis*, *5*(02), 161–174.

Rumata, V. M., & Sastrosubroto, A. S. (2017). The Indonesian e-commerce governance challenges in addressing the penetration of global user generated commerce platforms. *2017 International Conference on Computer, Control, Informatics and Its Applications (IC3INA)*, 7–11.

Safira, N., & Dewi, A. S. (2019). Peran modal sosial sebagai mediator literasi keuangan dan inklusi keuangan di Kota Padang. *Jurnal Mitra Manajemen*, *3*(1), 29–43.

Salsabella, O. (2022). Pengaruh literasi keuangan dan financial technology terhadap inklusi keuangan. *Bandung Conference Series: Business and Management*, *2*(1), 703–711.

Sensuse, D. I., Sipahutar, R. J., Jamra, R. K., & Suryono, R. R. (2020). Challenges and recommended solutions for change management in Indonesian E-Commerce. *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, 250–255.

Simanjuntak, P. (2019). Indonesias policy on ecommerce regulation and its challenges. *Bulletin of Social Informatics Theory and Application*, *3*(2), 69–74.

Yildiz, E., & KOÇAN, M. (2018). Impact of Product Innovation and Product Quality on Brand Loyalty: An Empirical Study on Smartphone Users. *ICPESS 2018 PROCEEDINGS Volume 2: Ecomonic Studies*, *51*.