RESEARCH ARTICLE

Online Buying and Selling Fraud in Indonesia and Its Criminal Law Enforcement

Asif Lutfiyana
Data Privacy Research Center, Indonesia
✉ asiflutfiyana97@gmail.com

OPEN ACCESS

Citation: Lutfiyana, A. (2021). Online Buying and Selling Fraud in Indonesia and Its Criminal Law Enforcement. *Law Research Review Quarterly, 7*(1), 53-68. https://doi.org/10.15294/lrrq.v7i1.43192

Submitted : September 7, 2020
Revised : January 15, 2021
Accepted : February 2, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

The development of technology and information is quite fast, especially on the internet. Through the internet, everyone can access and find all information around the world quickly and easily. The internet spurs the emergence of creativity in all fields, especially in business. So that there emerged online businesses that provided various kinds of human needs, ranging from food, clothing, property, and other needs. Online business is very useful to reduce costs and time during the buying and selling process. In contrast to conventional business, which requires producers and consumers to meet in person, so it requires a lot of money and time. This research aims to analyse and examine the fraud case of online transactions in Indonesia and its law enforcement. The research emphasized and found that in every facility that is offered by an online business, there is always an opening for crime to emerge. Therefore, the government established a regulation, namely Law Number 11 of 2008 concerning Electronic Information and Transactions as the legal umbrella for cybercrime. However, this regulation still needs to be reviewed because it still has weaknesses in ensnaring cybercrime. Where the development of technology and information is increasingly complex. So, it requires flexible regulations on technological developments.

Keywords: *Online Transactions; Fraud; Criminal Law*

1. INTRODUCTION

The rapid development of information and communication technology needs to be considered. Even though it makes it easy for the community, sometimes that convenience can be misused as a tool to commit crimes. Crime in the field of technology itself is often referred to as cyber crime or cyber crime or in foreign languages it is known as cybercrime. Pornography, embezzlement, data theft, illegal access to a system (hacking), bank account burglary, internet system tampering (cracking), theft of credit card numbers (carding), provision of misleading information, illegal transactions of goods, are some of the frequent examples of cybercrime. happened and harmed many parties (Suyanto, 2005: 48; Fitri, Syukur, & Justisa, 2019).

The United Nations as an institution that has one of the main objectives of maintaining world peace and security, has issued a resolution No. 55/63 on December 4, 2001, in which it was agreed that all countries must work together to anticipate and fight crimes that misuse information technology.

The technology offered by computers, especially the internet, is very supportive in all fields. Especially for those who are innovative and have a business spirit, of course they will benefit greatly from the internet. With the internet network, they can open a shop without spending money, only need to create an attractive buying and selling website plus some promos and quality goods.

Online business trends or what is often known as online shops are now mushrooming, almost all types of necessities are in the online shop. any need can be fulfilled by simply clicking on the picture and transferring money. But as consumers we need to be careful, if we are easily lulled by advertisements that place products at low prices, don't be easily tempted because there are so many irresponsible people out there under the guise of a business creating fake

accounts to deceive consumers. When consumers transfer money to the seller's account, but in the end the goods ordered are not received by the buyer, even if the bad accounts are sometimes untraceable.

Humans are social creatures who cannot live alone, requiring the role of others in fulfilling their needs (Waluyo & Feryanto, 2008: 73). Human needs are getting more and more complex every day, various methods are used to fulfill them. Law was created as something related to the minimum provisions needed to bring about public order through government stipulations (Rosidawati & Santoso, 2013: 35; Prabowo, 2012; Setiawan & Achyar, 2013). The rise of cybercrima encourages the government to move quickly in dealing with the response. However, in Indonesia, cybercrime has only been regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions. Indonesia needs a legal umbrella in fighting cybercrime. Because we know that now technology is growing rapidly and there are also many humans who are not wise in managing it.

2. METHOD

The research method is used as a tool to help and answer problems in the main research through procedures and techniques using research steps, using normative research methods, by describing the science of law in the dogmatic layer of law. The type of method used in this paper is normative legal research methods, from secondary legal materials, existing literature, as well as writings in the form of theses and articles, also taking from primary legal material, namely related laws, and the Criminal Code.

3. RESULT AND DISCUSSION

A. Cybercrime: The Capture of Indonesia

The problem of cyber crime that is carried out through the internet media often occurs in Indonesia. By law, this crime is not a simple crime as it is generally,

because the tools used are computers and the internet. An informal data indicates that Indonesia is the third largest "*hacker*" country in the world. Meanwhile, for Indonesia, the "*hacker*" city was first occupied by Semaranng, then Yogyakarta (Ariyadi, 2008; Amelia, 2016).

Cyber crime is known by two terms, namely "*cybercrime*" and "*computer related crime*" which are contained in two UN conference documents regarding The Treatment of Offender in Havana, Cuba in 1990 and in Vienna, Austria in 2000. The term cyber crime itself divided into 2, namely first cybercrime in a narrow sense called a computer crime. Second, ciber crime in a broad sense is called computer related crime.

The term cyber crime in the UN X / 2000 conference in Vienna, Austria includes crimes committed:

1) By using the means of a computer system or network (by means of a computer system or network)
2) In a computer system or network (in a computer system or network) and
3) Against a computer system or network (ageinst a computer system or network)

From the above explanation, it can be concluded that the narrow meaning of cyber crime is aimed at a computer system or network. Meanwhile, in a broad sense, cyber crime includes all new forms of crime shown to computers, computer networks and their use as well as traditional forms of crime which are now being committed using or with the help of computer devices (computer related crimes) (Tianotak, 2011: 2; Karo & Sebastian, 2019).

The problems faced in the law of information and telecommunications, especially the problem of cyber crime, are very broad, because they are no longer limited by the territory of a country and can be accessed anytime and anywhere. Actually, if we look again, cyber crime is similar to crime in general, namely as a

crime and a motivation to harm others with different tactics through computers and the internet.

To better understand cyber crime, here are some forms of action, as explained by Juju & Sulianta (2010: 75), as follows:

1) Carding
   Carding is shopping using someone else's credit card, usually by stealing data on the Internet, the perpetrator is the carder.
2) Hacking
   Hacking is the activity of breaking into other people's computer programs, including on a website. There are two types of hackers, first black hackers (crackers) and there are so-called white hackers. What black hackers do is usually damage and steal from other people's web or systems. While white hackers usually tell the admin or website account owner that their website has a security hole that can be broken into.
3) Cracking
   Cracking is a hacking activity with malicious motives. Another name is the black hat hacker. If hackers only peek at security holes, here crackers are more daring to destroy the security of other people's computers and focus on enjoying the results.
4) Defacing
   Defacing is the activity of destroying website pages with an improper appearance. What is being done is solely seeking personal satisfaction, fun, revenge, political elements, and other crimes
5) Spamming
   Spamming is the act of sending e-mail that the recipient does not want, it can also be through the comment box or guest book of a site. Spamming is also often referred to as bulk email or junk e-mail, aka junk, while the sender is referred to as a spammer. An example of the event most frequently experienced by the community is the lucky draw

message sent via email and SMS (Short Message Service), although many people have been deceived.

6) Phishing
   Phishing is an activity to lure internet users to want to provide personal data information and passwords on a fake website. Usually occurs in online banking users.
7) Malware
   Malware is a "*malicious*" program in the form of viruses, worms, trojans, horses, adware, browsers, hijackers, and many more which are infected into an application, so that when someone runs the program it can damage the infected software or operating system.
8) Hijacking
   Hijacking or in Indonesian can be interpreted as piracy which is defined as one of the crimes of piracy of other people's work. The most common crime is software piracy (Saragih & Siahaan, 2016: 23).

B. E-Commerce: Potential Fraud

With the existence of information and communication science, especially the internet, the marketing and sales process can be carried out at any time without being bound by space and time. The power of e-commerce allows geophysical barriers to disappear (Pradana, 2015: 36). The ability of the internet to be able to transmit data in various forms such as text, video, animated images, sound, and others, many business people take advantage of this technology by creating websites to promote their business. All levels of society who are familiar with internet technology are already familiar with this online buying and selling activity.

The activity of buying and selling online in English is called electronic commerce (e-commerce). Can be defined as the application and application of e-business

(e-business) related to commercial transactions, such as: electronic funds transfer, SCM (supply chain management), e-marketing (emarketing), or online marketing (online marketing), online transaction processing, electronic data interchange (EDI), product promotion and others (Jauhari, 2010: 159).

The global definition of e-Commerce is all forms of trading transactions of goods or services that are carried out electronically (Jauhari, 2010: 159). In general, e-Commerce is a package in the form of technology, applications and business processes that connect companies, consumers and communities through electronic transactions and trade in goods, services and information that are carried out electronically. Another definition of E-commerce is the process of buying, selling, transferring, or exchanging products, services, or information through computer networks via the internet (Kozinets, et.al, 2010: 71). Compared to conventional business principles, e-commerce is certainly more efficient. All processes are carried out electronically, starting from suppliers, distributors, partners, consumers, can be done faster, more intensively, and can be more cost effective in transportation.

C. E-Commerce Scams

The types of cybercrime are quite diverse, as previously discussed. What often happens when buying and selling online is usually fraud. The modes range from email phishing, scam investment websites, money games, online buying and selling and many more.

In online buying and selling scams, scammers can disguise themselves as sellers and buyers. When playing the role of a buyer, scammers will ask for their goods to be shipped first, but recently this rarely happens. If the fraudster plays the role of a seller, he will usually offer goods at a lower price than the original price. Then, if the buyer has started transferring

money to the seller's account, a few moments later the seller will run away and block the buyer's account so that he cannot hold him accountable. There is another possibility, namely that the seller still sends the ordered item, but it is different or not in accordance with what was ordered.

The risk of online shopping is very high, so this can reduce consumer confidence in shopping online. The risks that are quite worried about are credit card fraud, unsuitable goods, quality of goods, delivery of goods and consumer personal data. different from conventional trading where sellers and buyers meet directly in carrying out transactions.

In order to avoid online buying and selling scams, you should be more careful and do not be tempted by cheap prices. In addition, we also need to know the mode of this type of fraud. Krisianto (2014) highlighted are some tips for avoiding online crimes, as follows:

1) Be selective in receiving information
   Even though the internet is a repository of information. However, not all the information we get from the internet is not always true.
2) Be selective in providing information
   Do not be easy to believe with people who are first known on the internet. And avoid disseminating information that you yourself have doubts about its correctness.
3) Consult with more experienced people
   Can ask the cyber crime expert or join discussions in online forums.
4) Up to date anti Virus
   Make sure your computer has an antivirus that is up to date. In order to prevent the spread of computer viruses that are accidentally installed.

D. Legal Arrangements against Cybercrime in Indonesia

The development of information technology, including the internet, presents challenges for policy

makers. The law is required to adapt to social changes that occur. The rapid development of internet use invites crime to occur.

It is easy for someone to create a fake identity to surf the internet, carry out electronic transactions anywhere, making it difficult for legal officials to determine the true identity and location of the perpetrator. No matter how strong the e-commerce system is, there is a risk of crime in the form of fraud, credit card hijacking (carding), illegal transfer of funds from certain accounts (Liddy & Sturgeon, 1988: 21).

Prior to the enactment of the ITE Law as a form of active government role. Law enforcement officers use the Criminal Code in ensnaring cyber crime cases. The provisions contained in the Criminal Code concerning cyber crime are still global. Teguh Arifiady categorized several things specifically regulated in the Criminal Code and arranged according to the level of intensity of the case (Sumenge, 2011: 105), namely:

1) The provisions relating to the theft offense in Article 362 of the Criminal Code
2) Provisions relating to the destruction / destruction of goods are contained in Article 406 of the Criminal Code
3) Offenses regarding pornography are contained in Article 282 of the Criminal Code
4) The offense regarding fraud is contained in Article 378 of the Criminal Code
5) Provisions relating to the act of entering or crossing another person's territory,
6) Crimes regarding embezzlement are contained in Article 372 of the Criminal Code & 374 of the Criminal Code
7) Crimes against public order are contained in Article 154 of the Criminal Code
8) Offenses regarding insult are contained in Article 311 of the Criminal Code.
9) The offense regarding letter forgery is contained in Article 263 of the Criminal Code

10) Provisions regarding secret leakage are contained in Article 112 of the Criminal Code, Article 113 of the Criminal Code, & Article 114 of the Criminal Code
11) Offenses regarding gambling are contained in Article 303 of the Criminal Code

Criminal acts regulated in the ITE Law are regulated in CHAPTER VII concerning prohibited acts which can be categorized into several groups, namely:

1) Criminal acts related to illegal activities.
2) Criminal acts related to interference.
3) Criminal acts facilitate acts prohibited by Article 34 of the ITE Law.
4) The criminal act of falsifying information or electronic documents is contained in Article 34 of the ITE Law.
5) Additional criminal acts are contained in Article 36 of the ITE Law.
6) Emphasis on criminal threats in Article 52 of the ITE Law.

Regarding the crime of fraud, the ITE Law regulates the crime of illegal access (Article 30), and interference to computer systems (Article 32). As well as regulating additional criminal acts in Article 36 which states that *"... intentionally and without rights or against the law commits an act as referred to in Article 27 to Article 34 which results in losses to other people*".

Previously also regulated in Article 378 of the Criminal Code which reads: "*Anyone who with the intention of benefiting himself or another person unlawfully, by using a false name or fake dignity, with trickery, or a series of lies, moves others to hand over something to him , or in order to give a debt or write off a credit, he will be punished for fraud with a maximum imprisonment of four years*".

However, the Criminal Code is still regulated in general, which is intended for conventional crimes. Meanwhile, fraud in the ITE Law has a narrower scope.

However, Law Number 11 of 2008 concerning Electronic Information and Transactions or which is

often abbreviated as the ITE Law, still has weaknesses, including:

1) The General Provisions Chapter does not clearly describe the explanation of crimes using computers.
2) The ITE Law still uses a pragmatic-political approach, instead of using a public policy approach that involves more groups, so it is not surprising that the ITE Law only regulates the use of technology that has been so widely used in various aspects of human life (Sugiswati, 2011: 62).
3) Provisions concerning the implementation of evil acts or punishable actions such as negligence and mistakes have not been included in the ITE Law, such as the matters regulated in book I of the Criminal Code are not in the ITE Law.
4) The ITE Law also does not regulate the expiration of the crime of hacking. All these criminal activities are regulated in the Chapter concerning what actions are prohibited.

The birth of the ITE Law has not been accompanied by regulations governing its formal law. The existing legal instruments in Indonesia are inadequate to ensnare cybercrime in general and hacking crimes in particular (Sugiswati, 2011: 163; Karo & Sebastian, 2019). As an effort to combat cyber crime, the following steps need to be taken (Sobri, Emigawaty, & Damayanti, 2017: 230), among others:

1) Modernizing the national criminal law and its procedural law.
2) Improve the national computer network security system according to international standards.
3) Increase the understanding and expertise of law enforcement officials regarding efforts to prevent, investigate, and prosecute cases related to cyber crime.
4) Increase citizen awareness about the problem of cyber crime and the importance of preventing these crimes from occurring.

5) Increasing cooperation between countries, be it bilateral, regional and multilateral, in efforts to deal with cybercrime.

E. Factors for the Emergence of Cybercrime

The emergence of cases of law violation through the internet media can be motivated by several factors, including:

1) The economic condition of the community, the level of community needs is increasing while the employment opportunities are also decreasing. This encourages the crime rate to increase. Crime is a portrait of the concrete relation of the development of community life which directly or indirectly has sued the condition of society (Ismail, 2009: 243).
2) The interests of business, politics, culture, religion and so on can become motives, reasons and arguments that make a person and a group of people fall for cyber crime.
3) The Indonesian legal system still provides loopholes and weaknesses in the supervision system for these crimes. So that many criminal acts cannot be ensnared by law.

4. CONCLUSION

Finally, this research highlighted and concluded that cybercrime is not a simple crime as it is in general, because the media used are computers and the internet. However, it can also be said to be similar to conventional crimes, namely both crimes and harming others. The internet makes it easier for businesses, especially online businesses (e-commerce), because it removes geophysical barriers. Various online fraud modes range from e-mail phishing, scam investment websites, money games, online buying and selling and many more. Furthermore, concerning protection against cyber crime is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions and several articles in the Criminal Code.

Especially the criminal act of fraud can be charged under Article 36 of the ITE Law and Article 378 of the Criminal Code.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Amelia, T. N. (2016). Fraud in online transaction: case of Instagram. *Journal of Advanced Management Science Vol*, *4*(4), 347-350. doi: 10.12720/joams.4.4.347-350.

Fitri, F. A., Syukur, M., & Justisa, G. (2019). Do The Fraud Triangle Components Motivate Fraud In Indonesia?. *Australasian Accounting, Business and Finance Journal*, *13*(4), 63-72. http://dx.doi.org/10.14453/aabfj.v13i4.5.

Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal Inovasi*, *6*(3), 242-247. https://ejurnal.ung.ac.id/index.php/JIN/article/view/815.

Jauhari, J. (2010). Upaya pengembangan usaha kecil dan menengah (UKM) dengan memanfaatkan e-commerce. *Jurnal Sistem Informasi*, *2*(1), 1-12.

Juju, D., & Sulianta, F. (2013). *Hitam Putih Facebook*. Jakarta: Elex Media Komputindo.

Karo, R. K., & Sebastian, A. (2019). Juridical analysis on the criminal act of online shop fraud in Indonesia. *Lentera Hukum*, *6*(1), 1-14. https://doi.org/10.19184/ejlh.v6i1.9567.

Kozinets, R. V., De Valck, K., Wojnicki, A. C., & Wilner, S. J. (2010). Networked narratives: Understanding word-of-mouth marketing in online

communities. *Journal of marketing*, *74*(2), 71-89. https://doi.org/10.1509/jm.74.2.71

Krisianto, A. (2011). *Internet Untuk Pemuda: Panduan Menggunakan Internet Secara Produktif*. Jakarta: Elex Media Komputindo.

Liddy, C., & Sturgeon, A. (1998). Seamless secured transactions. *Information Management & Computer Security*, *6*(1), 21-27. https://doi.org/10.1108/09685229810207416.

Prabowo, H. Y. (2012). A better credit card fraud prevention strategy for Indonesia. *Journal of Money Laundering Control*, *15*(3), 267-293. https://doi.org/10.1108/13685201211238034.

Pradana, M. (2015). Klasifikasi jenis-jenis bisnis e-commerce di Indonesia. *Neo-Bis*, *9*(2), 32-40. https://doi.org/10.21107/nbs.v9i2.1271.

Rosidawati, I., & Santoso, E. (2017). Pelanggaran Internet Marketing Pada Kegiatan E-Commerce Dikaitkan dengan Etika Bisnis. *Jurnal Hukum & Pembangunan*, *43*(1), 27-53. http://dx.doi.org/10.21143/jhp.vol43.no1.1507.

Saragih, Y. M., & Siahaan, A. P. U. (2016). Cyber Crime Prevention Strategy in Indonesia. *SSRG Int. J. Humanit. Soc. Sci*, *3*(6), 22-26.

Setiawan, R., & Achyar, A. (2013). Effects of Perceived Trust and Perceived Price on Customers' Intention to Buy in Online Store in Indonesia. *ASEAN Marketing Journal*, *4*(1), 26-36. https://doi/org/10.21002/amj.v4i1.2029.

Sobri, M., & Damayanti, N. R. (2017). *Pengantar Teknologi Informasi-Konsep dan Teori*. Yogyakarta: Penerbit Andi.

Sugiswati, B. (2011). Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi di Era Informasi. *Perspektif*, *16*(1), 59-72. http://dx.doi.org/10.30742/perspektif.v16i1.70.

Sumenge, M. (2013). Penipuan Menggunakan Media Internet Berupa Jual-Beli Online. *Lex Crimen*, *2*(4), 102-112.

https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/3093/2637.

Suyanto, M. (2003). *Multimedia Alat untuk Meningkatkan Keunggulan Bersaing*. Yogyakarta: Penerbit Andi.

Tianotak, N. (2011). Urgensi Cyberlaw di Indonesia dalam Rangka Penanganan Cybercrime di Sektor Perbankan. *Jurnal Sasi*, *17*(4), 20-21.

Waluyo, S., Feryanto, A., & Haryanto, T. (1977). *Ilmu Pengetahuan Sosial*. Jakarta: Grasindo.

Humans are startlingly bad at detecting fraud. Even when we're on the lookout for signs of deception, studies show, our accuracy is hardly better than chance.

Maria Konnikova

ABOUT AUTHORS

Asif Lutfiyana SH is an independent researcher at Data Privacy Research Center, Semarang Indonesia. She obtained a Bachelor of Law degree from Universitas Negeri Semarang. Since a student, she has been active in various student activities, one of which is in the student journalism unit (LEGIST Student Press Institute).