RESEARCH ARTICLE

Cybercrime Case Item Transaction Fraud in DotA Game 2

Anang Satriani Surya Pranata[1]✉
[1] Indonesian Law and Technology Literacy Society
(*Masyarakat Melek Hukum dan Teknologi Indonesia*)
✉ ananglive7@gmail.com

OPEN ACCESS

Citation: Pranata, A. S. S. (2021). Cybercrime Case Item Transaction Fraud in DotA Game 2. *Law Research Review Quarterly, 7*(2), 197-210. https://doi.org/10.15294/lrrq.v7i1.43189

Submitted : December 12, 2020
Revised : February 12, 2021
Accepted : April 22, 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 DotA 2 community is known for the largest gamers community in the entire worlds and there is no secrets that this community hub is going bigger and bigger, why this is always expanding is because the game itself offer a complex gameplay with such a huge diversity for the player to explore and enjoy the experience, and the one that this community love most is the microtransacsion in this game that provide the item in game of DotA 2. The value of this item is more and more provitable because the growth of its community and thats make some criminals spread their hand in this community by doing a cybercrime such a scamming, fraud seller and buyer and a hacker that hack someone DotA 2 account that have a provitable account.

Keywords: *DotA 2 Game; Fraud; Cybercrime; Online Transaction*

1. INTRODUCTION

In an era that is undergoing very rapid development, it is not surprising anymore if the virtual world feels more like the real world, this is what happened to a game, namely Defense of the Ancient 2 or often referred to as DotA, DotA 2 is this game made by VALVE which is a game with the largest number of communities in the world, this is marked by the number of in-game players who spend their time playing this game every day, the main factor that causes the development of this community is about the complexity offered by this game with all possibilities Different possibilities are ready for the players to explore, with a hero

pool of more than 100 making this game one of the most complex games in history (Mattinen & Macey, 2018).

Apart from the things above, what makes this game more interesting is the in-game item transaction because the price of the item has a high selling value so that trading transactions in this game are considered very tempting for the players, besides VALVE as the owner of this game also provides a place for players to make online buying and selling transactions for these items called the STEAM COMMUNITY MARKET (Irfan, 2018).

Starting from the high opportunity to do business in this game, of course there are irresponsible parties or criminals who try to take advantage of loopholes in the trend of buying and selling online items in this game. There have been many parties who have become victims of the cunning of these criminals who have harmed the players from the DotA 2 community which have damaged and unhealthy community forums and the stability of item prices in this game (Mattinen & Macey, 2018; Irfan, 2018; Nugroho, 2016).

Indonesian players are also inseparable from the targets of these criminals, what the author highlights this time is a case of fraudulent buying and selling of Dota 2 items, both by buyers and sellers, such as sellers who do not send the goods they have sold and buyers who do not transfer the promised money to buy the item even though the item has been sent.

With the issuance of Law No. 11 of 2008 concerning Informatics and Electronic Transactions, the author here wants to know the role of the ITE Law in ensnaring cyber criminals which is the topic of the author's discussion at this time and the extent to which the efforts of the game developer, namely VALVE, in preventing similar incidents from happening again.

2. METHOD

Sources of data used by the author are: Secondary data used by the author to obtain data, namely by Library Research, namely by studying the problems and literature as well as other data sources related to the problem of writing this final report, as a basis for comparison and writing data analysis. The method used is the literature method which collects

samples related to the new installation procedure, this method is done to complete the required data.

3. RESULT AND DISCUSSION

A. Cybercrime, Electronic Transactions, and DotA 2 Game

Before dealing with the main problem in this discussion, namely the issuance of Law no. 11 of 2008 concerning Informatics and Electronic Transactions, the author here wants to know the role of the ITE Law in ensnaring cyber criminals which is the topic of the author's discussion at this time and the extent to which the efforts of the game developer, namely VALVE, in preventing similar incidents from happening. Again, it would be nice if we first understand what DotA 2 is like, what is cybercrime and what forms of cybercrime have happened in this game (Rizki & Zaky, 2019; Hamzah, 1990; Kaligis, 2012; Golose, 2006).

The DotA 2 computer game launched from the official valve website, they define this game as a Free to play multiplayer battle arena (MOBA) game, this video game was developed and released by Valve Corporation. This game is a separate sequel to Defense of the Ancients (DotA), which is a mod created by the Blizzard Entertainment gaming community Warcraft III: Reign of Chaos and its expansion pack, The Frozen Throne. Dota 2 is played in matches between two teams of five players each, with each team occupying and defending their own base on the map. Each of the ten players independently controls a powerful character, known as a "*hero*", all of whom have unique abilities and different styles of play. During the match, players collect experience points and items for their heroes to successfully fight the opposing team's heroes in player versus player battles. A team is said to win if it is the first to destroy a large structure located at the opposing team's base, which is called "*THE ANCIENT*" (Mattinen & Macey, 2018; Irfan, 2018).

It has been explained previously that in this game there are items that can be traded and have a high economic price among the DotA 2 community which is the target of criminals in carrying out cybercrime targeting these communities as their victims.

Furthermore, the meaning of Cybercrime according to Law Number 11 of 2008 concerning Information and

Electronic Transactions can be classified into 2 forms, namely:

1. Cybercrime that uses computers as a crime tool, namely Online Pornography (Cyberporn), Online Gambling, Defamation through social media, fraud through computers, counterfeiting through computers, extortion and threats through computers, spreading false news through computers, violations against copyright, cyber terrorism
2. Cybercrime related to computers, networks as targets for committing crimes, namely unauthorized access (illegal access), disrupting computer systems and computer data, unauthorized wiretapping or interception, data theft, and misusing computer equipment (Wahid & Labib, 2005; Mansur & Gultom, 2005).

Cybercrime according to the Report of the 10th United Nations Congress in Vienna defines Cybercrime into two, namely Cybercrime in a narrow sense and Cybercrime in a broad sense. Meanwhile, cybercrime in a broad sense is the overall form of crime directed against computers, computer networks and their users, and traditional forms of crime that use or with the help of computer equipment.

Then the definition of cybercrime according to Prof. Widodo is every activity of a person, group of people, legal entities that use computers as a means, to commit crimes or make computers as targets of crime. All of these crimes are forms of actions that are contrary to the laws and regulations, both in the sense of being against the law materially or against the law formally (Pmounda, 2015; Raharjo, 2008).

According to Andi Hamzah, "*crimes in the computer field can generally be defined as the illegal use of computers*". From the understanding given by Andi Hamzah, it can be concluded that he broadened the notion of computer crime, namely all illegal activities that use computers for criminal acts. No matter how small the impact or consequences arising from the use of computers illegally or illegally is a crime. Cybercrime has several characteristics, namely:

1. Acts that are carried out illegally, without rights or unethically occur in cyber/cyberspace, so it cannot be ascertained which state jurisdiction applies to them.

2. The act is carried out using any equipment that is connected to the internet.
3. These actions result in material and immaterial losses (time, value, services, money, goods, self-esteem, dignity, confidentiality of information) which tend to be greater than conventional crimes.
4. The perpetrators are people who master the use of the internet and its applications.
5. These acts are often carried out transnationally/across national borders (Hamzah, 1990; Raharjo, 2008).

Crimes in the field of information technology generally consist of two groups, namely:

1. Conventional crimes that use information technology as a tool, for example purchasing goods using stolen credit card numbers via the internet;
2. Crimes arise after the internet, using computer systems as victims, examples of this crime are destroying internet sites (cracking), sending viruses or computer programs that aim to damage computer work systems (Sitompul, 2001).

Cybercrime itself also has several classifications, including:

1. Computer as Object
   In this category, forms of cybercrime include cases of damage to computers, data or programs contained in them or damage to computer facilities such as Air Condutouring (AC) and equipment that supports computer operations.
2. Computer as Subject
   Computers can also create a place or environment for committing crimes, such as theft, fraud, and counterfeiting of property in new forms that cannot be touched (intangible), such as electronic pulses and magnetic strokes.
3. Computer as a Tool
   Computers are used as a tool to commit crimes so that the nature of the crime is very complex and difficult to know. One example is a criminal who takes deposit slips from a bank and writes the perpetrator's account number in magnetic ink on the documents and then puts them back in their original place. The customer who is about to enter the money will take and fill in the script that has been affixed with the account number of the criminal who processes the customer's documents, the

computer will automatically credit the amount of money in the account of the criminal. Wrongly, the perpetrator of the crime withdrew money by check from his account before the depositing customer filed a complaint with the bank.

4. Computer as a symbol
   A computer can be used as a symbol to commit fraud or threats, in this category including the fraud "*Birth of Match*" which states that the matchmaking agency uses a computer to help the victim find a mate, but it turns out that the matchmaking agency does not use a computer for this purpose (Sitompul, 2001; Dep.Kominfo, 2007; Radjagukguk, 2017).

B. DotA 2 Game, Fraud, and Cybercrime

Returning to the topic of our main discussion, cybercrime cases in the world of DotA 2 can be said to be something commonly faced by the cybercrime community. The most common thing that occurs in this game community is item fraud. but the problem that arises here is about the identity of the perpetrator of the fraud who may not be an Indonesian citizen. Not to mention the lack of evidence that makes it difficult for law enforcement officials to disclose the occurrence of the fraudulent act and also reluctant victims to report this incident and prefer to handle it themselves (Arifah, 2011).

In addition, there are several things that cause the mode of cybercrime in this discussion to always develop, namely due to factors such as:

1. Public Legal Awareness
   The process of law enforcement is basically an effort to realize justice and order in social life. Cybercrime is an act that is despicable and violates decency in society and violates the law. Until now, the legal awareness of the Indonesian people in responding to cybercrime activities is lacking. This is caused, among other things, by the lack of public understanding and knowledge of the types of cybercrime. Lack of public attention. Society and law enforcement are currently still paying great attention to conventional crimes. In fact, the perpetrators of computer crimes still continue to commit crimes. So that it makes these crimes increase and the consequences are widespread.

2. Safety Factor

   A sense of security will certainly be felt by cybercrime perpetrators when carrying out their actions. This is because the internet is commonly used in relatively closed places, such as at home, in rooms, at work, in libraries and in internet cafes. The activities carried out by the perpetrators in these places are difficult for outsiders to know. As a result, when the perpetrator is committing a crime, very few outsiders know about it. This is very different from conventional crimes, where the perpetrator will be easily identified physically while carrying out the action. So that the sense of security obtained in committing these crimes makes cybercrime crimes occur continuously and increase.

3. Law Enforcement Factor

   Law enforcement factors are often the cause of the rise of cybercrime. This is motivated by the lack of law enforcement officers who understand the ins and outs of information technology (internet), so that when the perpetrators of criminal acts are arrested, law enforcement officers have difficulty finding evidence that can be used to ensnare the perpetrators. So not infrequently if the perpetrators can escape the law and the crime is increasing.

4. Socio-Economic Factors

   This factor also affects the rise of cybercrime crimes because the global issue which is then associated with the crime is actually a network security problem. Network security is a global issue that appears along with the internet. As an economic commodity, many countries are in dire need of network security devices. Cybercrime is in a big scenario in the world's economic activity, the increasing socio-economic situation creates gaps for the perpetrators to carry out their actions.

5. Globalization Factor

   The existence of internet technology will eliminate national boundaries that make this world so close and narrow. The interconnectedness of one network to another makes it easier for criminals to carry out their actions. Then, the uneven distribution of technology makes one more powerful than the other. Unlimited internet access. With unlimited internet access, internet users freely access sites on the internet, so this gives rise

to cybercriminals by downloading, uploading and so on illegally (Tahir, 2009; Soekanto, 2014; Saputro, 2020).

As explained above, cybercrime that often occurs in the DotA2 game is Fraud of buying and selling items in the community market because fraudulent crimes committed by humans through electronic media are crimes that often occur today, so that the crimes that occur can only be committed by people who master and understand advanced technology, and the advanced technology they use to commit criminal acts of fraud, this will make many victims of fraud where the victims do not understand and master the technology or electronic media. making it difficult to hold the perpetrators of fraud accountable. The crime committed through electronic media is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions. 8 of 2011 concerning Information and Communication technology does not specifically regulate the criminal act of fraud. So far, the crime of fraud itself is regulated in Article 378 of the Criminal Code ("KUHP"), with the following article formulation: "Anyone with the intent to unlawfully benefit himself or another person by using a false name or false dignity (*hoedaningheid*); by deceit, or a series of lies, inducing another person to hand over something to him, or to give a debt or write off a debt, is threatened, for fraud, with a maximum imprisonment of four years" (Mansur & Gultom, 2005).

Although the ITE Law does not specifically regulate the criminal act of fraud, related to the occurrence of consumer losses in electronic transactions, there is a provision in Article 28 paragraph (1) of the ITE Law which states: "Every person intentionally and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions."

Violation of Article 28 paragraph (1) of the ITE Law is punishable by a maximum imprisonment of six years and/or a maximum fine of Rp. 1 billion, according to the provisions of Article 45 paragraph (2) of the ITE Law.

Even so, the two crimes have one thing in common, namely that they can cause harm to others. However, the formulation of Article 28 paragraph (1) of the ITE Law does not require an element of "benefiting oneself or others" as regulated in Article 378 of the Criminal Code regarding fraud.

In the end, it takes foresight from the police investigators to determine when to use Article 378 of the Criminal Code and when to use the provisions in Article 28 paragraph (1) of the ITE Law. However, in practice the police can apply layered articles to a crime that meets the elements of a criminal act of fraud as regulated in Article 378 of the Criminal Code and fulfils the elements of a criminal act in Article 28 paragraph (1) of the ITE Law. This means that if the elements of a criminal act are fulfilled, the police can use the two articles.

Apart from that, according to legal practitioner Iman Sjahputra, there are many fraud cases that cause consumer losses from electronic transactions. On the other hand, Iman in the article Iman Sjahputra: Consumers Still Lose in Electronic Transactions also said that often cases of fraud in electronic transactions are not reported to the authorities because the transaction value is considered not too large. According to Iman, there are still many frauds in electronic transactions because until now, a Reliability Certification Agency has not been established as mandated by Article 10 of the ITE Law.

In my opinion, the fake news phrase in this article has become a sufficient offense in declaring someone committing fraud via the internet because the perpetrator has lied to have goods in his selling stall (in this case related to the fraud case of buying and selling items in DotA 2.

To overcome this, VALVE as the game developer has created a security or security program called STEAM GUARD AUTHENTICATOR where players are required to enter a telephone number in the transaction process that is carried out through the community market and special confirmation is needed through a separate application to make transactions. buying and selling where this confirmation notification can only be seen by those who have the account, then there is also a feature in the form of a day restriction which requires players who want to make buying and selling transactions in the community market, the seller and buyer must first be friends for approximately 15 days and to activation is approximately 3 months.

In addition, Valve also provides VAC (Valve Anti Cheat) which is a program that bans or disables certain accounts that violate VALVE policies, this deactivation is in

order to reduce cheaters and also parties proven to be fraudulent and phishing accounts.

Then Law Enforcement in the case of criminal acts of fraud through cybercrime is a process to make legal wishes come true. This legal desire will later become the mind of the legislature that is formulated in legal regulations. The formulation of the mind of lawmakers is stated in legal regulations which will determine how law enforcement is carried out. In fact, the law enforcement process culminates in its implementation by law enforcement officials. Law enforcement officers in Indonesia are judges, prosecutors, and police. The judge is one of the law enforcement officers who carry out a judicial system that has the duty to accept and decide cases fairly.

Judges are officials who exercise judicial power as regulated in Law Number 48 of 2009 concerning judicial power. In the context of law enforcement in Indonesia, the task of judges is to uphold law and justice through the cases before them. Prosecutors are law enforcement officers who are functional officials who are authorized by law and enforce court decisions. Next is the Police, the police as law enforcers are required to carry out their profession properly based on professional ethics. The professional ethics is based on the provisions that determine the role of the police as law enforcers. Police are required to carry out their profession fairly and wisely, as well as to bring security and peace.

Law enforcement will always involve humans in it and thus human behaviour is involved in it. The law cannot be enforced by itself so that it involves law enforcement officers, and the apparatus in realizing law enforcement must be by law, facilities, and culture, so that the law can be enforced fairly and fairly in accordance with the ideals of the law itself. This shows that the challenges faced by law enforcement officers it is not impossible that very many law enforcers are not only required to be professional and precise in applying their norms but are also required to prove the truth of criminal charges which are sometimes influenced by stimuli from community behaviour to both become law violators.

Soerjono Soekanto's opinion said that the main point of law enforcement lies in the factors that influence it. These factors, are as follows:

1. The legal factor itself, namely the laws and regulations in force in Indonesia
2. Law enforcement factors, namely the parties that form and apply the law.
3. Factors of facilities or facilities that support law enforcement
4. Community factors, namely the environment in which the law applies or is applied.
5. Cultural factors, namely as a result of work, creativity and taste based on human initiative in social life (Soekanto, 2014).

Of the five factors, they are closely related because they influence each other. These five factors can be said to be the essence of law enforcement and can be used as benchmarks for the effectiveness of law enforcement in Indonesia.

The emergence of difficulties in law application and law enforcement against cybercrime crimes, namely in the settlement of these crimes, this paperless condition creates problems in proving information that is processed, stored, or sent electronically. fundamental use of electronic evidence in the process of proving criminal cases, in particular, namely the absence of a benchmark or basis for the use of electronic evidence in our legislation. In addition, it is difficult to reveal the crime, both the perpetrator, and the crime which is often very difficult to prove so that it becomes a challenge in law enforcement for cybercrime (Mathias, 2021; Rahman, 2018; Lemuel, 2019).

Law enforcement efforts against cybercrime in addition to these rules should also be balanced with the skills and capabilities of law enforcement in eradicating cybercrime. This is because the modes of cybercrime are growing day by day, it is feared that these crimes will run rampant and the perpetrators are difficult to track and arrest, so that it can harm the community and the State and even the wider world.

4. CONCLUSION

Fraud in the cyber world, namely there is a provision in Article 28 paragraph (1) of the ITE Law which states: "*Everyone intentionally and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions*." Violation of Article 28 paragraph (1) of the ITE

Law is punishable by a maximum imprisonment of six years and/or a maximum fine of Rp. 1 billion, in accordance with the provisions of Article 45 paragraph (2) of the ITE Law. In my opinion, the fake news phrase in this article has become a sufficient offense in declaring someone committing fraud via the internet because the perpetrator has lied about having the goods in his selling stall (in this case related to the fraud case of buying and selling items in the DotA 2 game).

5. DECLARATION OF CONFLICTING INTERESTS

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

6. FUNDING

None

6. ACKNOWLEDGEMENT

None

7. REFERENCES

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi*, *18*(2), 185-195.

Dep.Kominfo. (2007). *Menuju Kepastian Hukum di Bidang: Informasi dan Transaksi Elektronik*. Jakarta: Dirjen Aplikasi Telematika.

Golose, P. R. (2006). Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri. *Buletin Hukum Perbankan*, *4*(2).

Hamzah, A. (1990). *Aspek-aspek Pidana di Bidang Komputer*. Jakarta: Sinar Grafika.

Irfan, M. (2018). Tindak Pidana Penipuan Daring dalam Jual Beli Item DoTA 2 Melalui Internet. *Thesis*. Banda Aceh: Universitas Syiah Kuala.

Kaligis, O. C. (2012). *Penerapan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dalam Prakteknya.* Jakarta: Yarsif Watampone.

Kitab Undang-Undang Hukum Pidana

Lemuel, Y. (2019). Internet and Crimes: How the Law Responds to Internet Based Crimes? A Book Review of 'Aspek Hukum Penipuan Berbasis Internet' Maskun & Wiwik Meilarati, CV Keni Media, Makassar, 2016, 238

Pages, ISBN 978-602-74375-5-5. *JILS (Journal of Indonesian Legal Studies)*, *4*(2), 343-350. https://doi.org/10.15294/jils.v4i2.34772.

Mansur, D. M. A., & Gultom, E. (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: PT Refika Aditama.

Mathias, J. (2021). Hate Speech and Its Threat to Law Enforcement. *The Indonesian Journal of International Clinical Legal Education*, *3*(1). https://doi.org/10.15294/ijicle.v3i1.43172.

Mattinen, T., & Macey, J. (2018, October). Online abuse and age in Dota 2. In *Proceedings of the 22nd International Academic Mindtrek Conference* (pp. 69-78).

Nugroho, O. S. (2016). Modus Penipuan Transaksi Barang dalam Game Online dan Prospek Penyelesaiannya. *Thesis.* University of Muhammadiyah Malang.

Pomounda, I. (2015). Perlindungan Hukum Bagi Korban Penipuan Melalui Media Elektronik (Suatu Pendekatan Viktimologi). *Thesis.* Tadulako University.

Radjagukguk, E. (2017). Pembaharuan Hukum Memasuki PJPT Kedua dalam Era Globalisasi. *Jurnal Hukum & Pembangunan*, *23*(6), 505-526.

Raharjo. A. (2008). *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya Bakti.

Rahman, M. A. (2018). One Hundred Thousand, Ended in Misery Five Years. *Law Research Review Quarterly*, *4*(2), 276-283. https://doi.org/10.15294/snh.v4i02.25573.

Republic of Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*.

Rizki, F. M., & Zaky, M. (2019). Analisis Kriminologis Korban Cyber Fraud Pada Transaksi Game Online Melalui Steam. *Anomie*, *1*(1).

Said, K., & Diniyanto, A. (2021). Determination of Advancement of Technology against Law. *Journal of Law and Legal Reform*, *2*(1), 125-134. https://doi.org/10.15294/jllr.v2i1.44525.

Saputro, H. C. (2020). How Does the Law Solve the Covid-19 Problem?. *The Indonesian Journal of International Clinical Legal Education*, *2*(3). https://doi.org/10.15294/ijicle.v2i3.38418.

Sitompul, A. (2001). *Hukum Internet (Pengenalan mengenai Masalah Hukum di Cyberspace*). Bandung: Citra Aditya bakti.

Soekanto, S. (2014). *Faktor-faktor yang Mempengaruhi Penegak Hukum*, Jakarta: RajawaliPers.

Tahir, A. (2009). Penegakan Hukum Cybercrime di Indonesia, *Thesis*. Universitas Gajah Mada.

Utari, I. S., & Arifin, R. (2019). Law Enforcement and Legal Reform in Indonesia and Global Context: How the Law Responds to Community Development?. *Journal of Law and Legal Reform*, *1*(1), 1-4. https://doi.org/10.15294/jllr.v1i1.35772

Wahid, A., & Labib, M. (2005) *Kejahatan Mayaantara (Cybercrime)*. Bandung: Refika Aditama.

Quote

There are three things in the world that deserve no mercy, hypocrisy, fraud, and tyranny.

Frederick William Robertson

ABOUT AUTHORS

Anang Satriani Surya Pranata is graduated from Faculty of Law Universitas Negeri Semarang, Indonesia. Now, he is serving as researcher and volunteer at Indonesian Law and Technology Literacy Society (*Masyarakat Melek Hukum dan Teknologi Indonesia*)