Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030402
ISSN 2616-2296 Vol. 3 Num. 4

The investigation and prevention countermeasures of virtual property theft cases

Xingjian Du[*], Zhuo Xiao, Xun Liu, Junru Cao, Kai Zhang

Hunan Police College, Changsha, Hunan, 410138, China
[*]Corresponding author

Keywords: Virtual property, criminal law, protection to prevent theft

Abstract: With the development of network economy, network virtual property is paid more and more attention. At the same time, the theft of virtual property crime cases are becoming increasingly threatening. From the characteristics of virtual property theft cases, the criminal of these cases are highly professional, the virtualization of the crime space, and the volatility of the case evidence. There are also many problems in the process of investigation. This paper mainly puts forward the investigation countermeasures from the perspective of the investigation department of the public security organ, and systematically summarizes the preventive measures from the multiple aspects of the society.

1. Introduction

1.1 Definition of virtual property theft cases

Virtual property generally refers to the digital, non-materialized form of property. It includes online games, E-mail, online paging and a series of information products with certain value, as well as the characters formed in the virtual life. At present, online games are relatively popular. Virtual property also includes the property existing in online game, including the level of game account, currency in games, various equipment owned by game characters, etc. These virtual property can be converted into real property under certain conditions[1].

According to the law, virtual property theft behavior, is for the purpose of illegal possession, secretly steal virtual property. The secret theft mentioned here refers to the criminals using the way that is not known by others or difficult for others to know, especially refers to the hacking strategies to steal others' virtual property. The criminal object of this kind of crime is specific virtual property, including both currency virtual property, including goods and account virtual property.

1.2 Characteristics of virtual property theft cases

1.2.1 The subject of the crime generally has certain computer expertise

In judicial practice, the theft cases of virtual property are mostly carried out in two ways: first, the use of system loopholes to illegally invade the computer information system to steal the network virtual property. This type of virtual property theft often requires to find the loopholes in the computer system, so it requires certain technology to complete this kind of crime. Second, by intrusion, broken certain computer system to steal virtual property stored in the computer system, this practice commonly known as "hacking", through the implanted Trojan program and computer virus to hacker specific targets, by controlling the corresponding computer information system to dispose or transfer the fair value of the virtual property. Therefore, the criminals engaged in virtual property theft are generally people with a certain knowledge of computer network, and may even be professionals engaged in related industries.

1.2.2 The crime are all taking place in the cyberspace

In virtual property theft cases, this kind of theft is different from the common "visible theft", which occurs in virtual space. This point is significantly different from the traditional theft cases. Because the criminal object of this kind of crime is virtual property, which only exists in the network virtual space, it means that such crime can only be carried out through the network.

1.2.3 The process of such cases are short, the behaviors of it are highly concealed

Because such cases occur in cyberspace and have the instantaneous nature of their criminal behavior, the owners, holders, custodian and other stakeholders of virtual property are difficult to respond in time, which leads to a certain lag in the discovery of crimes. After the crime, criminals can erase the traces by changing IP and etc., which greatly increases the difficulty of investigation.

1.2.4 The value of the crime object is often small, and the victims are mostly teenagers

Young people are the main force of virtual property purchase and consumption. According to a 2018 research report by the Pew Center in the United States, more than 64% of young people (13-19 years old) have reached virtual property transactions, the main content of which are game currency and game equipment (93%). This situation is also common in China, where the protection of virtual property is closely related to the youth.

2. Problems existing in the investigation and prevention of virtual property theft cases

2.1 Problems existing in the investigation

2.1.1 Difficulties in finding the cases

First of all, because the virtual property can only be reflected in the network system, if it is not timely inquired or understood through the network, it is difficult to find its theft. Therefore, the virtual property owners can not find their virtual property infringed in time, not to mention report the case to the public security organs. Therefore, there is a certain "criminal black number" in virtual property theft cases

Secondly, after the virtual property owners found that their virtual property was stolen, because the amount involved in some cases is not large and the judicial procedures are complicated, many victims think that more is less than one thing. As a result, many small theft of virtual property can not enter the field of the public security organs.

2.1.2 Qualfying the case is difficult

One is the question of crime and non-sin. Because the virtual property is not different from the "physical property", the evaluation standard of its specific value is not unified. The value of virtual property, especially goods virtual property (usually game equipment) is only for specific subjects. For example, in Counter-Strike Global Offensive, a "dragon sniper" can be worth $500,000, but not for non-players. In addition, the value of the virtual property volatility is bigger, for the value of what is reference to the loss of the victim, or issued by the professional appraisal institution of legal evidence significance, or on the basis of network operators pricing and perpetrators of fence price, in the judicial practice of virtual property theft cases of various standard, but the lack of unified standard. Value cannot be determined, and it is difficult to judge whether the theft is established. Secondly, the problem of this crime and that sin. For the case of virtual property theft, it is generally believed in academic circles and judicial practice that virtual property theft involves computer crimes. However, some scholars and judges believe that, from the perspective of the object and the object of the crime and the subjective purpose of the crime. This brings difficulty to the characterization of the case and affects the development of the investigation work[2].

2.1.3 Evidence collection is difficult

Because the virtual property theft cases occur in the network virtual environment, the investigation work also needs the existing space of the virtual property, that is, the "crime scene" of the virtual property theft cases to find the criminal traces and criminal evidence.

Electronic data is formed in the process of a case, stored, processed and transmitted in digital form, and can prove the facts of the case. Unlike those traditional evidence, the electric counterparts such as Wechat records, alipay payment records and so on involved more information than the former. Based on electric data, the electric evidence are easy to fade out and hard to preserve. In reality, the electric evidence exists in certain platform such as phone application or computer programs. This character gives the chance of doctoring and wiping out electric evidence to those who master specific computer skills, which can prove the unstable feature of the E-evidence. Furthermore, the E-evidence is highly duplicable. Therefore, it is prone to be changed. In addition, the collection of this kind of evidence can not support the whole accusation, the further legal process of the cases is highly relied on the restructuring and decoding skills.

Electronic evidence has the characteristics of perishable and high threshold for evidence collection. Moreover, the acquisition of electronic data is not the same to directly support litigation. Instead, these data must be cleaned and structured to extract meaningful evidence to prove the crime, and form a complete evidence chain, which is also the difficulty in investigation and case handling.

2.1.4 Difficult investigation and cooperation

First of all, because virtual property theft cases are carried out in cyberspace, the investigation of virtual property cases is often difficult to be fully carried out in the grass-roots public security organs. High-level public security organs carry out the investigation. Due to the lack of manpower in many cases, the investigation efficiency may be affected to a certain extent. Secondly, virtual property theft cases are usually committed on specific websites, and the public security organs need to cooperate with third-party platforms to obtain corresponding evidence. Such cooperation will also consume the time and funds of the handling authorities. Finally, there is usually a time and space interval between the occurrence place and the result place of virtual property theft cases, which requires the cooperation of the public security organs in different places, which will undoubtedly increase the judicial cost.

2.1.5 Poor awareness of network prevention.

The owners of virtual property include both online developers and the vast number of citizens who trade in cyberspace. But in real life, many virtual property owners lack awareness of the virtual property they own. According to the Daily Mail, the most common passwords worldwide are "123456" and "password (password)", and "iloveyou (I love you)" is also a popular password for people in most countries. Studies show that people tend to prioritize "good memory," but ignore security issues —— 83% of passwords can be deciphered in less than a second.

The study found that there were great differences in users in different countries and gender when setting passwords. In the UK, men prefer to use team names such as liverpool (Liverpool) as passwords, while women prefer charlie (Charles), tiger (tiger) and sunshine (sunshine). In addition, Americans have a preference for using numbers as a password. If the virtual property is compared to a vault, the account number is the door of the vault, and the account number and password is the key to the door of the vault.

3. Investigation and prevention countermeasures of virtual property theft cases

3.1 Investigation and countermeasures

3.1.1 Expand the source of clues and improve the ability of case discovery

For the immediate virtual property theft cases, especially if the victim can provide direct clues, the public security organs are often able to locate the suspect. However, the lack of tracking ability for fake theft in cyberspace, in many times can only rely on network operators to provide further clues, which provides a gap for criminals to evade detection and crackdown.

In terms of the current situation of virtual property protection, the public security organs, as the investigation organs, lack the ability to take the initiative in addition to accepting the reports from the masses. For the public security organs to occupy a more active position in the case of virtual property theft, the key is to implement the basic policy of combining special groups, and combine their own business work with the active spirit of the people. The cooperation between different walks of community is of great importance in preventing such cases. Meanwhile, the police department at every level shall work with local network runner companies to obtain relevant clues concerning virtual property theft cases. It is also necessary to establish a special research and judgment platform to form a "big police type" of synthetic operations.

3.1.2 Unified identification standards and improve the ability to judge the nature of cases

For the judicial department, the legal issues related to virtual property are a "gray area" in practice. Relevant laws and regulations are not very perfect, the upstream investigation of evidence is difficult, to prosecute and trial link is often difficult to form a complete chain of evidence, therefore, the relevant judicial departments to further deepen the cognition in practice, strengthen the review of evidence, extract the experience of judicial practice, the judicial explanation to the corresponding situation to supplement relatively lagging law. The judicial department should also start from a practical perspective, feed back legislation, provide the basis and suggestions for legislation, further improve the socialist rule of law system with Chinese characteristics, adapt to the Internet normal in the new era, and deal with the emerging illegal and criminal situation of telecom network. Judicial and judicial departments should also strengthen cooperation with relevant government departments to form joint efforts to jointly deal with new crimes. At the same time, how to properly evaluate the value of the virtual property has become a significant problem in the judicial practice.Without doubt,the standard of the evaluation of the virtual property can not subject to subjectivism and relativism.The severity of the crime should be evaluated in a fair way.Some specific ways can be used in this process includes platform pricing,market pricing,user spending and intermediary evaluation and so on.

3.1.3 Strengthen the ability of electronic forensics and accurately collect evidence fixed

Virtual property theft crime mainly occurs in the cyberspace, the suspects left relevant information in the form of electronic data. Criminal evidence is directly related to the judicial process of such cases. The virtual property theft detection is very important part, therefore, we need to use existing forsenic science skills and technique, strengthen the virtual scene exploration, standardize electronic evidence collection process, to discover the facts of the case and provide high quality evidence.

First of all, the electronic data evidence collection personnel before forensics work to understand related to forensic target, to conduct a comprehensive assessment, has determined the scene of the evidence, and then in a variety of electronic equipment and massive data to confirm the truth of the case of the material carrier and data, and by printing, backup, photography, photography, making documents to fix and save the electronic data. It is followed by the analysis and identification stage of electronic data, where professional software and equipment are used to analyze data, mine the potential links between electronic data, and form an evidence chain. Finally, the evidence will be presented in the form of an inquest record, an analysis report or an inspection report.

Secondly, the material preparation of electronic forensics should be strengthened. Because the scene investigation of the virtual property theft crime belongs to the technical and professional work, the construction of equipment and facilities is the basis of the scene investigation. Therefore, for the scene of the crime of investigation, electronic forensics must keep pace with The Times specification material preparation, including forensic hardware and software preparation: in hardware aspects, mainly including the laptop or mobile PC, mobile hard disk or U disk, high-speed hard disk copy machine, forensics rubik's cube, one-way hard disk read only lock, USB cable, network cable and other necessary communication transmission line, computer interface transfer card, screwdriver and other disassembly tools, power socket, anti-static gloves, mobile phone signal shielding box, card reader, etc. In terms of software, it mainly includes self-made tool data floppy disk, password decoding tools, data recovery tools, log analysis software, file browsing tools, network monitoring tools, evidence analysis software, forensics master, etc[3].

3.1.4 Improve the linkage mechanism to improve the efficiency of investigation and case handling

First of all, strengthen the linkage of the upper and lower levels of public security organs. Generally speaking, affected by technical equipment and personnel quality, the grass-roots public security organs lack enough resources and ability to handle virtual property theft cases. In practice, the grass-roots public security organs generally need to transfer the cases to the higher public security organs for investigation after accepting the cases. Therefore, it is necessary to improve the linkage investigation mechanism of the upper and lower levels, and establish a "green channel for handling virtual property cases". Secondly, strengthen the linkage of the public security organs in different regions. In the case of virtual property theft, the place where the case occurs and the result occurs are often inconsistent, and the case investigation needs to be carried out across regions. The internal coordination mechanism of the public security organs should be further improved to realize information sharing, cooperative investigation, and improve the investigation efficiency.

3.2 Prevention and control countermeasures

3.2.1 Improve the legal system and clarify the criminal responsibility

For the nature of the virtual property, academic mainly has two points of view, because as the game of the accumulation of the equipment and weapons itself, no economic significance, it is in a form of a set of data, the data in the computer game the software running, may have played a role, independent itself, no sense. The intellectual labor here is relative to the whole game, and obviously belongs to the network producer of the game company. The other is that virtual property has its inherent value, because the helmets, armor and other weapons and equipment accumulated by online game players are acquired by game players spending their time, money and energy, and to some extent, it should be a kind of labor income. This virtual property, can buy directly from game developers, can also be obtained from the virtual currency trading market, both value and use value, can transfer, close to the intellectual property, so the virtual property has a general commodity property, should belong to the scope of private property, the property shall be stolen, shall be protected by criminal law, theft shall be investigated for criminal responsibility. The theft of network virtual property is fully in line with the four criminal elements of theft. For the theft of network virtual property reaching the amount stipulated by the criminal law, we should severely crack down on the theft, integrate the network virtual property into the protection category of the criminal law as soon as possible, to ensure the harmony and stability of the society. When it is clear that the network virtual property should be protected by the law, the attribute problem of the network virtual property has become the first problem we need to solve. There are limitations in simply classifying the legal attribute of network virtual property into property right, creditor's right, intellectual property right or a new type of property rights[4].

Virtual property should be protected as a new property rights, rather than based on the protection of existing rights, because the virtual property has property rights, but its personality is also very prominent, the original civil law rights protection is not enough to cover the virtual property rights, thus improve the legislation, clear ownership is a priority. According to the principle of subjective and objective unity of our criminal law, it is more appropriate to commit the crime of theft. First, the perpetrator steals virtual property for the purpose of illegal possession, which complies with the subjective purpose of larceny. Secondly, the actor secretly stole other property in a peaceful way that thinks it is not easy to find, which also meets the objective requirements of the crime. Thirdly, for the definition of "property", China's criminal law does not stipulate that it is "physical", so in the object of crime, also accord with the provisions of the crime[5].

3.2.2 Strengthen prevention publicity and enhance the awareness of prevention

The protection of virtual property should be based on prevention. In the prevention work, the propaganda department is undoubtedly the main force, as the mouthpiece of the party, the propaganda organ should be under the unified leadership of the central government, for the virtual property fraud activities often occur in the area to prevent propaganda, to help the people to see through the trick of criminals. At the same time, we should actively publicize the corresponding anti-theft knowledge, mobilize the masses, eliminate potential hidden dangers, use multimedia tools to expand the publicity, improve the people's awareness of virtual property protection and vigilance to potential crimes. Special education should be carried out for the vulnerable groups, and anti-fraud can be integrated into life. When it comes to virtual property protection, the majority of vulnerable groups are young people (mainly students), so the publicity department can incorporate the knowledge of anti-fraud and anti-fraud into the main channel of the classroom, and deepen the impression of the target group through text publicity and video playback. With the expansion of the promotion campaign, the awareness of how to protect their virtual property has been greatly raised. For the vulnerable victims in the area, especially the students, we should pay attention to their trend and psychological state, communicate more with the guardians, and improve their vigilance awareness and prevention ability. First of all, young people themselves should establish a correct consumption concept, limit the game time, and actively invest into real life. Secondly, even if you want to participate in virtual property transactions, you should keep a prudent attitude and conduct transactions through credible and guaranteed platforms. For transactions with large transactions, you should keep the transaction records and remember the details of the transaction for a rainy day. In addition, for young people who often participate in virtual property transactions, they should choose familiar platforms and Windows whenever possible[6]. For the identification and control ability of the youth group, in the complex network environment travel, being cheated is inevitable, the key is to timely feedback. Like most victims, the victims of virtual property fraud are often afraid of negative social evaluation. At the same time, often due to the small amount of loss, the victims' relatives are difficult to find, making many illegal acts to escape the legal sanctions. This phenomenon also brings difficulties for the investigation. For the victims, timely reporting of the situation is the best option to recover the loss.

3.2.3 Improve the trading mechanism and strengthen the cooperation between the police and enterprises

The transaction of virtual property is decided by the buyers and sellers, and the protection of virtual property is inseparable from the joint efforts of the buyers and sellers. In addition to the buyer to establish a rational consumption concept and enhance the vigilance consciousness, the seller (trading platform) should also improve the corresponding mechanism. First of all, for the loss of bills similar to the bill system, the platform should conduct a comprehensive risk assessment for large transactions involving virtual property, and for those with huge risks, the payment can be stopped first. In addition, the authenticity of the operation can be further determined through the operation of telephone verification. In fact, developers or trading platforms turn a blind eye to many unjust enrichment behaviors in and out of the game, because the platform itself can also profit from the trading. Even as noted above, employees within the platform may have been involved in this activity, with an extremely negative impact on players and society. Therefore, the establishment of a sound risk assessment system is the key to solve the problem. In addition to the use of big data for real-name authentication payment, the amount of payment should be limited for young users without civil capacity. For the transaction exceeding a certain amount (a large amount), we should contact the payer in time and inform the risk, and record the transaction on record for future reference to avoid the loss of evidence[7].

Because most of the carrier of virtual property transactions of —— network space is a broad and abstract scope, specific each transaction must be borne by the specific platform, it can be network game operators, but also can be other third party platform, nowadays, the network operator trading system general channel formal, have certain security, so this paper mainly discusses how to third party platform (such as idle fish, taobao) virtual property transaction protection, and to prevent possible risk of fraud. First of all, the establishment of the early warning mechanism is divided into two aspects. On the one hand, check options should be set for transactions involving virtual property, so that buyers and sellers can realize the nature, consequences and significance of their behavior. For the seller of virtual property should make the actual name certification, can not be taken lightly. On the other hand, when conducting the virtual property transactions, a risk reporting mechanism should be established, that is, to inform the buyer of the possible risks, and to guide the buyer to record the relevant transaction information when conducting the virtual property transactions. Secondly, the establishment of preventive measures also includes the credit evaluation of the seller, the seller of the virtual property with large transactions and many customers can issue the credit proof, and guide the virtual property buyer to find the appropriate virtual property purchase[8].

3.2.4 Ban high-risk platforms and eliminate hidden dangers of illegal crimes

For the protection of virtual property, the focus is on prevention. The public security organs should collect social conditions and public opinions in time, and timely remind enterprises with bad credit and transfer with high risks. For platforms and enterprises obviously suspected of illegal crimes, they should immediately contact the network and information departments to close and stop losses in time. In addition, the public security organs should strengthen the governance of cyberspace, control the public opinion position, timely publish high-risk or trust-breaking enterprises and their virtual products, and at the same time, they should also crack down on criminal individuals and purify the cyberspace. "When the people look at the public security bureau, the key depends on solving crimes." Normal risk control is conducive to the backinvestigation, to deter criminals and unscrupulous enterprises. It is the best way to carry out the aim of serving the people wholeheartedly and protect the people's life and property safety.

4. Conclusions

The crime of virtual property theft is a crime that has emerged recently in the world. In the author's opinion, the key to the investigation and prevention of virtual property theft cases is to unite and solve them together, which requires the extensive participation of all parties. First of all, the legislature should collect the social conditions and public opinions of all parties, refer to the relevant systems of other countries, and improve the top-level system design. In addition, for the characteristics of virtual property crimes, the public security departments should analyze and make full preparations, and the government departments should strengthen publicity, go deep into the grass-roots level, grasp the key points, and solve the "last kilometer" of the work. Seller's platforms should also bear the corresponding social responsibilities, and improve the corresponding mechanisms, so that criminals cannot take advantage of the opportunity. A large number of consumers, mainly youth, in such a period, we should establish a good sense of prevention.

Today, with the rapid development of the Internet, the socialist rule of law system with Chinese characteristics is gradually improved, and the public security organs are increasingly strong ability to investigate cyber crimes, the author believes that in the near future, the problem of virtual property theft cases can be alleviated and finally solved.

Acknowledgement

Research project: This paper is the phased achievement of the innovative training project "Social Harm Analysis of Virtual Property Fraud and Research on Prevention and Control Measures" (S202111534012) of Hunan College Students' Innovation and Entrepreneurship Project. The project is headed by Xun Liu and Professor Jianyun Jiang Serve as an advisor.

References

[1] Chen Wei: "Investigation countermeasures of network virtual property theft cases", Journal of Beijing People's Police College, 2008 (5).
[2] Yao Ning: Analysis of Internet Virtual Property Crime, 2010 master's dissertation of Jilin University, 2010.
[3] Ma Zhihai, Legal Analysis of stealing Internet Virtual Property, Master thesis of Chongqing University, no. 3,2015.
[4] Wang Qinkun: "The restriction bottleneck and countermeasures of network theft case investigation", Journal of Hubei Police College, 2016 (1).
[5] Du Wei, Peng Jianxin: "Research on Network Electronic Evidence Evidence Technology", Guangdong Public Security Technology, 2012 (1).
[6] Chen Xingliang, The Criminal Law attribute of Virtual Property and its Protection Path, Chinese Law, No. 4, 2017.
[7] Gao Limei. Interpretation path of network virtual property protection. Tsinghua Law, 2021
[8] Yang Shimei: "Prevention strategy for cyber crime", Journal of Shanxi Institute of Political Science and Law Cadre Management, 2014 (1).