

# Research on Fraud Methods and Governance in the Era of Big Data

## --Taking Contemporary College Students as an Example

Xuanrong Liu, Changjin Qian, Huilin Jiang

Anhui University of Finance and Economics, Bengbu City, 233030, China.

### Abstract

In the era of big data, all the rapid development, the Internet for people to bring convenience at the same time network fraud also derived. Internet fraud has brought great harm to the whole society, especially rampant in colleges and universities. It not only damages the money and heart of students, but also has a great impact on the harmony of families, the management of colleges and universities and the stability of society. After summarizing the types and characteristics of big data fraud in the existing campus, the author deeply analyzes the reasons for the frequent occurrence of campus network fraud, and deeply studies how to effectively manage and prevent big data fraud. In order to create a safe and stable learning environment for students and protect their own rights and interests, the whole society must work together to promote the governance and prevention of campus Internet fraud from the four aspects of families, universities, students and the government.

### Keywords

**Big data; College students; Means of fraud; Governance.**

## 1. Introduction

With the development of science and technology, the application field of computer big data technology continues to expand, and all aspects of human experience such as society, economy and contact methods are undergoing unprecedented changes. At the same time, the security issues of Internet technology and the existing legal system are not perfect, there are still some deficiencies. According to the 2021 Mobile Payment Security Survey Report released by China UnionPay, one in seven people have experienced online fraud, an increase of 6% compared with 2020[ ]. In recent years, the frequent occurrence of fraud incidents against college students, colleges and universities have become the worst hit area of network fraud, many college students are persecuted by this, money and spirit suffered serious damage, governance and prevention of campus network fraud is urgent.

## 2. Research on Big data fraud in colleges and universities

### 2.1. Definition of big data fraud

Big data fraud is a means of defrauding others of property in various forms on the Internet in order to achieve a certain purpose. Where the main act or link of a crime occurs on the Internet, the act of defrauding public or private property of a relatively large amount by fabricating facts or concealing the truth. The concept of big data fraud in universities, also known as campus network fraud, refers to fraudsters using illegal means to defraud teachers and students in universities to obtain large amounts of property[ ]. At present, there are many kinds of campus network fraud, which is difficult to control.

## 2.2. Existing patterns of big data fraud in universities

Fraud in the era of big data is different from the ordinary traditional means of fraud, mostly committed by groups. And the methods of crime are more varied, more hidden and more high-tech. Statistics show that from 2017 to 2021, people's courts at all levels concluded 103,000 online fraud cases of first instance. Among them, the year-on-year increase was 71.69% in 2018; In 2019, the year-on-year increase was 25.15%; A year-on-year increase of 40.36% in 2020; In 2021, the year-on-year decrease was 17.55%.

According to the Special Report on Judicial Big Data on the Characteristics and Trends of Information Cyber Crimes (2017.1 -- 2021.12), online fraud has involved more than 223,000 defendants in the past five years, with an average of 2.2 defendants in each online fraud case. When the defendants carried out online fraud cases, they used to apply for loans, impersonate others, publish false recruitment, dating information, induce participation in gambling, fabricate online shopping problems, put false advertisements and other ways or tactics to deceive the victims. Among them, loan cases accounted for the highest proportion, about 16.71%.

The crime of fraud accounted for the largest proportion of information network crimes, accounting for 36.53% of the list, and the types of online fraud such as loans, pretending to be acquaintances, part-time recruitment accounted for more.

**Table 1:** The main types of network fraud cases accounted for the proportion

Internet fraud case	Proportion (%)
loan	16.71
Pretend to be an acquaintance	15.08
Part-time recruitment	10.16
Online dating	4.46
gambling	2.88
Online shopping	2.70

At present, there are three major patterns of big data fraud in universities.

### 2.2.1. "Guide and lure"

"Inducement" refers to the process by which criminals collect a large number of email addresses and send fraudulent information based on the collected network information addresses to entice users to fill in the user's private account number, password and other information. Or is a variety of urgent reasons to require the object of fraud immediately login to the web page with security vulnerabilities submit user name, password, credit card and other sensitive information, and then theft of the object of fraud funds or according to such behavior to further deceive other relevant contacts of the object of fraud, such as their relatives, friends, etc. Or to obtain the mobile phone number of the target of fraud by improper means, the SMS "mass sender" that stores the mobile phone number sends out a large number of false information, in the name of "winning the lottery", "tax free", "investment" and other names to deceive the target of fraud for remittance, transfer and other operations.

### 2.2.2. "Fishing"

Phishing refers to the creation of fake websites to cheat users of their account passwords in order to commit financial theft. Criminals imitate the construction of domain names, web pages and other content is very similar to the real online banking system, online securities trading platform, lure the target of fraud to enter personal account, password and other information,

and then steal the target of fraud funds. Or publish false information on well-known e-commerce websites to sell goods under the names of "cleaning warehouse products", "super low prices of products", "tax exemption", "charity bazaar", and so on, and use fake e-commerce to commit fraud.

### **2.2.3. "Theft"**

"Theft" refers to the use of advanced computer application technology and means to create special computer viruses to steal relevant information. The virus program hides the submitted fake e-mails or websites, and takes advantage of the characteristics of some users who are greedy for convenience (such as setting "123456" and other simple password security), so that the virus records the relevant accounts and passwords of users in online transactions, so as to crack the simple passwords set by users.

## **3. Specific means of big data fraud in colleges and universities**

As for the characteristics of cyber crime, there are many opinions in the theoretical circle. Some scholars in mainland China believe that cyber crime has the characteristics of high technology, low crime cost and great harm, trans-temporal and not easy to prevent. Network fraud is a kind of network crime, with the above-mentioned characteristics and reasons, but as an independent crime type, especially for college students on campus network fraud behavior[ ].The author collects and analyzes the big data fraud that has occurred in various colleges and universities, and concludes that the current campus network fraud is mainly divided into the following types.

### **3.1. Impersonating friends to commit fraud**

At present, with the development of social software, college students love online communication. Fraudsters take advantage of the loopholes to steal QQ, wechat and other social accounts, send false information, pretend to be friends or relatives around, and pretend to be in urgent need of borrowing money in an emergency, so that students have panic psychology, and then transfer money successfully cheated.

### **3.2. Online shopping fraud**

With the rapid development of online shopping, people can choose the clothes they want without leaving home, especially the contemporary college students are extremely passionate about online shopping. Fraudsters will use the leaked online shopping information to call consumers and pretend that there is a problem with the order package to double the refund compensation for the parties. They only need you to enter the website provided by him and enter the account password or verification code. Little did you know that the information entered into your property would then be transferred.

### **3.3. Online dating fraud**

Most of these frauds are friends added online, who become good friends or develop romantic relationships after a long time of contact. Scammers are good at deceiving victims with sweet words and making up various reasons to defraud victims of money. When you think you have found a bosom friend or love, but do not know that you have fallen into the opposite carefully designed pig killing dish.

### **3.4. Scholarship fraud**

Fraudsters will be in each university scholarship evaluation period, to send fraud mail to students, explaining that this is the scholarship evaluation list, and attached to the unknown link or two-dimensional code for you to open to view, when you really open to enter the input information then your property will be transferred.

### **3.5. Brush single part-time fraud**

This kind of fraud will be in the name of recruitment agents, the release of false advertising information, claiming that only need to move a finger every day, a few hours can earn hundreds of dollars, low investment high return, when you contact him after the early will let you complete small tasks and return the principal and commission and win trust, to the late fraudsters will be required to complete the specified number or the order has not taken effect, etc., Lure to continue to brush single, and to refuse to return cash on various excuses, after being discovered directly shield the victim.

### **3.6. Campus loan fraud**

Campus loans exist in various forms, such as pushing loan advertisements to college students through Internet platforms to avoid inducing student loans with mortgage and low interest, and requiring payment of loan "commission fee", "management fee", "deposit" and other fees, and "blocking" students from contacting them after receiving the payment. In a more extreme form, students are asked to provide photos, videos, ID cards and phone numbers of their family members as collateral and security for loans, threatening to extort money if the students fail to pay.

Recently, the various colleges and universities have appeared "cancel campus loan" new fraud, this means is mainly divided into two categories, one is for the registered network loan platform account or loan records, fraudster claimed that "according to the relevant national policies need to cooperate with cancel the account, otherwise it will affect personal credit"; The second is for no registered network loan platform account or no loan record, fraudsters said that "your identity information stolen registered network loan account, need to cooperate with the cancellation, otherwise it will affect personal credit". The property was transferred to the fraudster's account when the victim believed he had complied with the fraudster's request.

### **3.7. Game account trading fraud**

Most of this kind of fraud occurs in college students who love playing games. Some want to buy accounts, some want to sell accounts, and this kind of fraud is roughly divided into three types. The first is to check the number on the grounds of login victim account password and face recognition change stolen; The second is to trade on other unknown platforms. The scammer asks the victim to use his designated platform to trade on the grounds that the old players are trading on other platforms. When the victim transfers the money on this platform, the scammer has already disappeared; The third is to make the victim pay a margin before continuing to trade. When the victim realizes that he has been cheated, it is too late.

### **3.8. Health code nucleic acid fraud**

In recent years, with frequent outbreaks of COVID-19 and the country's focus on epidemic prevention and control, fraudsters seize the loophole. Fraudsters pretend to be epidemic prevention departments and call victims, falsely claiming that the victims' nucleic acid test results and travel code are wrong, and may be close friends. If the victim says that he has not been to the medium-high risk area or come into contact with the risk group during this period of time, the fraudsters will say that there may be a problem with the system and need to re-verify the victim's identity information and itinerary information. Then they will send a link to the victim to fill in the victim's ID information and phone number again. After filling in the information, The victim would receive a verification code, and he would ask the victim to send it to them, saying that he would send the travel code back to the victim, and when the victim sent the verification code to them, he had already been tricked.

### 3.9. Ticket and ticket fraud

Online ticket service is fast, convenient and cheap, which is gradually selected and recognized by people. Air tickets, train tickets, etc., can be completed by telephone or online booking business. Some fraudsters made fake websites to publish information about cheap air or train tickets, taking advantage of the convenience of the Internet to carry out online telecom fraud. In addition, the fraudsters ask the victims to remit money multiple times, claiming that their accounts have been frozen, tickets need to be activated, and extra fees have to be paid. In addition, such fraud also fraudsters in the name of helping victims handle ticket refund business fraud.

## 4. The existing college network fraud management measures

At present, the means to deal with network fraud in colleges and universities is usually the cooperation between network operators and communication operators and management departments at all levels and public security departments. On the one hand, through their own management and technical means to block all kinds of false information, strengthen prevention; On the other hand, actively cooperate with the public security organs to strengthen the use of network virtual space fraud suspects to crack down. At the same time, through radio, television, newspaper, Internet and other media, to increase the publicity of online fraud means, improve the public's awareness of prevention, try to minimize the occurrence of online fraud cases.

When the case has happened, the public security will collect and analyze the information data, and use professional technology to find out the IP location of the fraudsters and the direction of money, but because the network fraud is usually cross-border crime, the police need to collect the amount of data is very miscellaneous and huge, and most fraudsters are outside the country, with multiple accounts, After the success of the fraud, the amount of money will be remitted to a number of different overseas bank accounts in batches, which makes it more difficult for the police to follow up, and most of the college online fraud cases can not recover the money at last.

## 5. Governance of campus Internet fraud related means

Online fraud in colleges and universities has certain same characteristics as online fraud in society -- professional fraud organizations, various means of fraud, high tracking difficulty, wide range of fraud targets. In addition, online fraud in colleges and universities also has the characteristics of gullibility, great harm, high repetition, and low alarm rate[1]. Through the analysis of the types and characteristics of Internet fraud in colleges and universities, this paper will put forward suggestions on how to deal with Internet fraud in colleges and universities from four aspects: students, schools, families and the government.

### 5.1. Students

(1) the main body of campus network fraud is the student, so the student himself must improve the awareness of fraud prevention, learn more knowledge to prevent campus fraud, independent understanding of the current network fraud cases occurred in colleges and universities and prevent in advance, avoid because of do not understand, do not know and fall into a scam.

(2) College online fraud in the era of big data is mostly due to the leakage of students' personal information, giving fraudsters opportunities, so students in this "Internet +" era must pay attention to the protection of personal information, do not disclose personal privacy at will, especially bank card number, account password, mobile phone number and other highly private information must pay more attention to, Try not to fill in, do not give fraudsters the opportunity to "find".

(3) Students themselves should develop a good habit of surfing the Internet, do not open the location website at will, do not listen to the words of strangers lightly, do not download dangerous software, especially borrowing online loans, online brushing, online love, buying second-hand goods and other online transactions involving money must be far away, if necessary also must be in a guaranteed software and safe environment.

(4) Students should be vigilant, have the ability to identify Internet fraud, in the encounter of Internet fraud to keep calm, have a clear judgment, do not be a few words of fraud intimidation, threat, lure to believe him, if really be fraud intoIf you are a teacher, you must call the police immediately, keep the evidence, find your counselor to seek the help of the school, and recover the money as soon as possible. Do not refuse to call the police for help because of fear. Meanwhile, you should keep a good state of mind to avoid being trapped in self-blame and affecting your normal life.

## 5.2. School

(1) Increase the publicity of fraud harm, popularize the types of fraud, always put the publicity of the rule of law in an important position, and can cooperate with the local public security, combined with typical cases in the school, hold lectures to explain the law.

(2) To enrich the anti-fraud education methods, through vivid anti-fraud education activities to let students personally experience the terrible campus network fraud and improve their vigilance, such as enriching the education forms of themed class meetings, carrying out fraud scenes to allow students to experience immersion, holding anti-fraud knowledge contests, etc[ ].

(3) The school should carry out the fight against the current telecom fraud activities as the focus of the current campus public security rectification, purifying the campus atmosphere to catch, to achieve a clear division of labor, responsibility to the person, at the same time learn to learn lessons, summarize the campus has occurred in the Internet fraud cases to come up with countermeasures, draw one example from another, quick action, improve the efficiency of preventing campus Internet fraud.

(4) Schools should be alert to the theft of personal information of teachers and students, strengthen the management of personal information of teachers and students, and use safe and secure teaching software with high privacy to avoid the leakage of personal information of teachers and students.

## 5.3. Government

(1) To improve the network supervision mechanism, the government should first let the network supervision department strengthen the supervision of software development, website construction and application operation, kill some fraud tools from the root, timely shut down illegal accounts, remove illegal software; At the same time, the improvement of real-name online system should be strengthened, and social software involving money transactions must be authenticated by all real-name users, so as to prevent fraudsters from using loopholes to commit crimes and not using police tracking[1].

(2) The government should vigorously train professional talents. At present, one of the reasons why it is difficult to bring fraudsters to justice in campus online fraud is the technical limitation, which makes it impossible to accurately track the whereabouts of fraudsters. It is suggested that the government extensively look for professionals and vigorously train relevant technologies to improve the lack of this aspect; At the same time, the government should encourage the development and application of software that can identify fraud information, intercept it, remind it, and directly alarm it, and vigorously promote it for use by the whole people. For example, the current National Anti-fraud Center APP can be further optimized and developed on this basis, so that everyone on campus can have it.

(3) Improve laws and regulations, strengthen the rectification, the current campus network fraud is so rampant part of the reason is that the punishment is not strong enough, the government should formulate and improve the relevant laws and regulations, increase the punishment, so that fraudsters do not dare to commit; At the same time, the relevant government departments can set up a special group to rectify campus network fraud, and curb campus network fraud through precise attack and centralized rectification.

#### 5.4. Family

(1) Parents should carry out anti-fraud education to their children in daily life, and set up correct outlook on money and values for their children, so that students know how to be diligent and thrifty, do not love vanity, keep up with the Joneses, and correctly understand the existence and use of money.

(2) Parents should communicate with their children, keep in touch with them, take the initiative to understand their children's daily dynamics, and ask their children whether they have other needs recently, which can be met under reasonable circumstances; At the same time, parents should ensure that their children's living expenses are sufficient to avoid being cheated by fraudsters because of insufficient living expenses.

(3) after the child was defrauded parents must maintain a good state of mind, comfort the child, positive guidance, do not scold excessively, things have happened to think about solving, avoid causing secondary damage to the child, increase psychological pressure, astray.

### 6. Conclusion

The frequent occurrence of campus network fraud in the era of big data has caused great harm to contemporary college students, both financially and spiritually, leaving indelible damage. Only when the whole society works together to crack down on online fraud and build a secure and solid network system can we create a good learning environment for college students and build a real "fraud-free campus".

### Acknowledgements

This paper is a funded project of Anhui University of Finance and Economics College Students' Innovation and Entrepreneurship Training Program. Project name: Research on Fraud Methods and Governance in the Era of Big Data -- Taking Contemporary College Students as an example (Project number: S202110378103)

### References

- [1] Xu Hua, Wang Zhong yan. Research on prevention and control measures of campus Internet fraud under the background of "big data" [J]. Journal of Zunyi Normal University,202,24(04):145-147+161.
- [2] Huang Chengkun. Research on Harm Countermeasures of Campus Network Fraud Crime based on the Internet era [J]. Legal Review,2021,(04):159-160.
- [3] Xiao Xie, Huang Jiangying. Research on Types, Causes and Countermeasures of Online Fraud among College Students [J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition),2015,27(05):67-72.
- [4] Liao T, Zhang J G. Multiple governance of telecom fraud in universities under the background of big data [J]. Law & Economics, 201,30(09):12-15.