sciendo
JOURNAL OF LEGAL STUDIES
"Vasile Goldiş" Western University of Arad
J. L. S.
2020 – 26(40)
DOI: 10.2478/jles-2020-0009

# ANALYSIS OF CRIMINAL ACTIVITIES EXPLOITING SOCIAL MEDIA: WITH SPECIAL REGARDS TO CRIMINAL CASES OF WECHAT FRAUD IN CHINESE JURISDICTION

**Xingan Li***
*Arcada University of Applied Sciences, Finland; International Institute for Innovation Society, Finland, E-mail: xingan.li@yahoo.com*

**(Received: July 2020; Accepted: September 2020; Published: November 2020)**

**Abstract:** Social media provide a more convenient way for daily communication and business transaction, while they are also exploited by potential criminals to perpetrate offenses of different natures. Fraud is one of the most frequently reported offenses, some of which involve the use of WeChat, an application now used by 846 million users worldwide. The article is designed to give a comprehensive statement of features, causes, and types of WeChat fraud currently existing in China. The article also formulates important countermeasures based on academic conclusions, law enforcement opinions as well as written criminal judgments collected from Chinese courts during the research.

**Keywords:** Social media; WeChat; fraud; crime; criminal; detection.

## 1. Introduction

Social media, being utilized by both conventional and unconventional offenders, have caused concern about unlawful access to accounts, disclosure, and infringement of privacy, as well as misuse and abuse of anonymity. Due to more sensitive information and clues and traces to daily activities and movements, it is uncomplicated for possible malefactors to select possible victims of varieties of offenses. Social media can facilitate both traditional and untraditional privacy-related crimes with a both traditional and untraditional scheme, and reviewed alternative solutions to privacy protection and their concomitant dilemmas (Dong and Li 2016). Wechat is a mobile application program for instant messages developed by Tencent Company on 21 January 2011, supporting group chatting by sending a text, audio, video, and pictures via the network. Due to its open platform, Wechat soon became a promotion platform making shopping more convenient (The People's Supreme Court of the People's Republic of China 2013). It has

* Corresponding author: Xingan Li. *E-mail: xingan.li@yahoo.com.*

multiple functions, for example, text messaging, hold-to-talk voice messaging, broadcast (one-to-many) messaging, video conferencing, video games, sharing of photographs and videos, and location sharing (Xu 2015). WeChat allows people to add friends by a variety of methods, including searching by username or phone number, adding from phone or email contacts, playing a "message in a bottle" game, or viewing nearby people who are also using the same service within a radius of 20 kms. Compared with old instant messaging systems or similar social media, the WeChat platform provides a more speedy, open, flexible, and smarter communication way.

To some extent, all the three unique functions of WeChat can induce some risks for their users. For example, the function of “message in a bottle” (drifting bottle) enables a user to send a message to another random user located possibly in anywhere in the world, most likely never known to each other. The user to send the message may be full of curiosity or in need to communicate with others, or sometimes simply killing spare time. The user who receives the "message in a bottle" can have a similar motive. The function of "shake" means that two random users in the same application shaking their smartphones simultaneously can be networked in WeChat and start a conversation. The function of “people nearby” enable a user to find other WeChat users within a radius of 20 kms based on geographical positioning information. A list of "people nearby" can be generated by such a function, which can further the contact by letting the user to “send greeting" to any users in the list. Once the other counterpart is willing to receive the “greeting,” they can get network and become WeChat “friends.” Strangers are targeted in all these three functions, which can easily be abused to realize a fraudulent scheme.

In China and some other countries, Wechat becomes very popular among smartphone users, across Android, iPhone, BlackBerry, Windows Phone, and Symbian phones. It is currently the unique most popular social networking service. Due to these functions of open networking and accurate positioning, while Wechat brings about convenience for users to communicate with each other, it also leaves loopholes for more and more potential perpetrators to victimize other users through Wechat. In many cases, the functions of searching users nearby, or shaking to find other users can lead to unfortunates due to abusive activities. While these functions can be deactivated by the user, they attract many users to try to find some funny things or some lucky opportunities, for example, making a friend of different sex, who might be young, pretty, well-educated, rich, and open-minded “guan erdai” or “fu erdai" (official second-generation, rich second-generation. Two popular terms in contemporary China used to denote young persons whose parents are government officials or chief corporate officers). These users are innocent, but they

take a risk of being victimized by fake beauties. Therefore, WeChat, as well as some other social media, is becoming a new tool to commit some offenses. In reality, there have been numerous criminal cases in which WeChat and other social media services were abused in offenses of different nature (The Supreme People's Court of the People's Republic of China 2015). In some verdicts available, WeChat was the main tool or media in carrying out prostitution brokering (Nanshan District People's Court 2014), dissemination of pornographic materials (Ruian City People's Court 2015; Nangang District People's Court 2016; Taocheng District People's Court 2016; Jiashan County People's Court 2016), selling pornographic materials (Yankeshi City People's Court 2015), kidnapping (Foshan Intermediate People's Court 2013; Taipusi Qi People's Court 2015; The Supreme People's Court of the People's Republic of China 2015. In some case, forcible rape was also involved victims were female), drug trafficking (Jiaoling County People's Court 2015; Mawei District People's Court 2016; Xiangzhou District People's Court 2016; Huma County People's Court 2016), theft (Nanxi District People's Court 2014; Anning District People's Court 2015; Xinshi District People's Court 2016), fraud (Longtan District People's Court 2013; Quangang District People's Court 2015; Beilin District People's Court 2015; Emeishan City People's Court 2016; Yiwu City People's Court 2016), illegal business operations (Xinji People's Court 2016), selling fake and inferior products (Zigong Intermediate People's Court 2016), gambling (Chengzhong District People's Court 2015; Xuhui District People's Court 2015; Lufeng City People's Court 2017), extortion (Songjiang District People's Court 2016) and so on. In a certain case, unauthorized access to another person's WeChat also caused international injury during the dispute and fight (Fengtai District People's Court).

"Weixin chapian fanzui"(the offense of WeChat fraud) is a term specifically coined in the Chinese language to describe the act of defrauding a large amount of property through the application platform of Wechat, by way of fabricating facts or concealing the truth committed by playing various functions of the WeChat with the purpose of possession such property. This is a new type of fraud derived from ordinary fraud. Even though the offense of fraud in Chinese criminal law can only be convicted when the amount of value of the defrauded property reaches the sum of 6000 yuan, acts of fraud of smaller amount of property can more frequently occur and accumulate to a large sum altogether, meaning that such smaller frauds can also severely threaten users' rights of property.

According to the third quarterly report of Tencent Company in 2016, the number of monthly active users of WeChat reached 846 million, an increase of 30% than 2015 (Tencent 2016). The users are distributed in more than 200 countries and territories, using more than 20 different languages. In addition, public Wechat

platforms, which were approved to publish news, literature, and academic works, articles of popular sciences, and commercial and marketing information, have reached 20 million. There were 400 million users who opened the account of WeChat Pay, which is a digital wallet service incorporated into WeChat, which allows users to perform mobile payments and send money between contacts. There is no doubt that WeChat had a giant user base for any social activities, including deviance and crime.

## 2. Features of Fraud on Wechat

### 2.1. The offense can be highly concealed from discovery

Anonymity and identity camouflage are core factors in successful WeChat fraud (Zhu 2015, p. 48). People's Bank of China, the central bank of this country issued on 1 July 2016 "Management Measures on Network Payment Business of Non-Bank Payment Institutions," a document that requires Alipay, WeChat Pay and other payment institution to manage users according to the principle of real-name system, and manage users' accounts by classifying them into different categories. However, there can hardly be a practical method to verify whether the registered name and identification number are that of the user. Criminals register the WeChat account by using a fake identity and commit the offense of fraud, after which they delete their account immediately and thus conceal their whereabouts. At the same time, due to limits of detection methods, information technique, and consideration of users' privacy, law enforcement is confronted with obstacles that hinder the efficient investigation of the suspects' real data and whereabouts. The difficulty and inefficiency in detection and investigation lead to a low probability of successful punishment, lowering the costs of criminals and risks of being caught and punished. This in turn encourages criminals to commit more frauds by using the WeChat Platform (Chen 2014, p. 48).

### 2.2. Funds defrauded through the WeChat are difficult to be recovered

In fraud cases committed through the Wechat, criminals usually choose to avoid the supervision system of the substantive bank, but turn to a net bank, making use of its feature of express fund flow. They entice potential victims to transfer funds through net bank accounts or WeChat express payment. When funds arrive at the accounts of the fraudsters, they either transfer the sum through net bank or cash through bank terminals. When the victims found the reality of the scam, funds in their accounts have already been transferred to others' accounts, usually in other regions or countries. Final fund flow can hardly be identified by law enforcement,

subsequently, it is more difficult to recover the defrauded losses than in cases of other types of fraud (Li 2015, pp. 42-43).

### 2.3. Transterritoriality of WeChat fraud

Like other cybercrime, Wechat Fraud is also transterritorial. Criminals of WeChat fraud can be at every corner of the globe, wherever there is a network connection (Zhu 2015, p. 48; Li 2015, p. 43). Once they register WeChat accounts, they are capable of impersonating users' friends, spreading fake winning information, and Trojan Horse malware, by which they are able to defraud others. Transterritoriality of WeChat fraud can play a comprehensive role in crime and punishment, it does not only make it more convenient, efficient, and fast for criminals to commit the offenses, make it more difficult for law enforcement to detect and investigate the case but also decrease the possibility of recovering losses, as mentioned in the last section (Chen 2014, p. 47; Zhu 2015, p. 48).

### 2.4. WeChat fraud is a cost-effective way to make profits

WeChat fraud can be achieved by merely a smartphone and unsophisticated techniques, meaning at a very low cost. The basic condition is to download the application of WeChat and install it on the smartphone, and then register an account. The technical implication and financial input of such WeChat fraud are both lower than other types of frauds. At the same time, the easy portability of the smartphone and simple operation of the WeChat makes it straightforward to perpetrate the offense. Inevitably, low cost and simple perpetuation of the crime lead to the prevalence of the fraud, an increase of the victimization, and growth of the losses from it (Chen 2014, p. 47-48; Zhu 2015, p. 48).

### 2.5. Victimization of WeChat fraud at a very young age

According to the report of Quest Mobile, as of March 2016, the average age of WeChat users is at 20 years old, of which 87.7% are under 50 years old, 86.2% between 18 and 36 years old. The low average age of WeChat also makes victimization age lower. In addition, lower age may mean the identity of the victims concentrated in students, mostly university students. It is understandable that students have a high level of curiosity and are willing to test emerging high-tech products and functions, during which they actively test some links and data on WeChat, some of which are potentially harmful. Furthermore, younger age also means that the students are people who easily trust others due to their lack of social and legal experience. These features make them the main target of WeChat fraudsters. Some others, who are still young but unemployed, target users of their age to carry out fraudulent activities (Chen 2014, p. 46).

### 2.6. Increasing variety of means of defrauding

At the very beginning, simple methods could already be sufficient in defrauding users. With the increased awareness of such fraud, users do not always believe the scam and it becomes harder and harder for the criminals to deceive others. But they turn to invent newer and more sophisticated methods to infringe others' property and rights (Zhu 2015, p. 48). So the evolutionary and accumulated methods can ensure the success of scams in attracting and deceiving users. In a 2015 case, the defendant Wen networked with Zhang, a temporary employee as a cleaner, through WeChat. He pretended to be the boss of a cement factory and could help Zhang to be employed permanently. From August 2015, Wen asked Zhang to transfer more than70,000 yuan in the name of giving bribery to certain officials (Emeishan City People's Court 2016). In another case with a similar situation, the perpetrator and the victim got networked via QQ and later they communicated via WeChat. The perpetrator defrauded a sum up to 180,000 yuan from the victim (Beilin District People's Court 2015). In a 2016 case, WeChat played a role in a way that fabricated screenshot of WeChat communication between the perpetrator and a non-existent third party was used as proof to get trust from the victim (Yiwu City People's Court 2016).

## 3. Causes of Fraud on Social Media

### 3.1. Novel and unique functions of social networking

WeChat functions, such as "message in a bottle" (sent to the "sea" and intended for a random user even thousands of kms far away to pick up and start contact), "people nearby" (registered a WeChat account and open the same function within a radius of 20 kms), and "shake" (to randomly find a user who uses the shake the phone at the same time), attract users to try to make contact with other users whether they are far away or nearby. When strangers start to communicate with each other, they have to actively make conversation with each other so that they can get known. This is a process during which strangers get in touch and acquire trust. When potential criminals acquire the trust of the potential victims, they are able to carry out their criminal activities, fraud being one type (Chen 2014, p. 48). Yu and Liang got networked by using the WeChat "shake" feature in February 2013. But Yu fabricated a name and falsely claimed that she worked in a company hundreds of kilometers away from her real location. Liang, the potential victim was serious to make a girlfriend with Yu. By taking advantage of such a situation, within several months, Yu falsely claimed that her company did not pay her salary and asked to borrow some money from Liang, who transferred 13,800 yuan to a

bank account Yu opened using her mother's name. She squandered all the money and could not repay it to Liang (Longtan District People's Court 2013).

### 3.2. Rapid development of WeChat business

Unlike other businesses in China, the official business register is compulsory for doing business on WeChat. It makes it more convenient and more profitable for ordinary users to do business, while at the same time supervision on such transactions is completely left in lack: tax evasion, lower transaction cost, no quality check, no advertising expenses, and so on. A lethal fault of WeChat transaction is that, without official registration, authentic identifications and addresses of WeChat merchants are by no means easy to verify. Once there are disputes or frauds, it is almost impossible to maintain "consumer rights" or pursue the perpetrators. Selling fake goods are another way of fraud. WeChat merchants can upload authentic pictures, but with fake goods sent to the buyers. Particularly, when transactions are done in the WeChat function of "comments", there is no third-party payment platform employed and high risks exist for buyers' money or commodity.

### 3.3. Convenience and rapidity of WeChat Pay

The increasing popularity of the WeChat platform facilitates the development of a new payment platform, that is, the current WeChat Pay, which is an integrated function of WeChat terminal and operated via mobile phone. WeChat Pay is bound with users' bank accounts so as for the payment to be safe, fast, and efficient. In China today, it is very common to pay for a small sum, however tiny it is, by scanning a QR code in a shop, which is now acquiring great efficiency in dealing with small-sum payment. This is also employed more and more by potential perpetrators of fraud on and through WeChat. use

### 3.4. Non-real-name registration system of WeChat users

In the past, registration of a WeChat account required only an email address or a QQ account. Nowadays, when a user registers a WeChat account, a telephone number is the only prerequisite. When fraud is committed, there is hardly any trace of the perpetrator, no real name, no real identification, nor real address. Reporting of the case by the victim to law enforcement can be very difficult, let alone investigation (Chen 2014, p. 48; Zhu 2015, p. 48).

### 3.5. Missing of law and supervision

While higher and more extensive requirements for supervision are possibly necessary, some of the issues involved in WeChat business do not fall into

provisions of existing laws and regulations. For example, the Advertisement Law of the People's Republic of China cannot well be applied to regulate those messages in WeChat "comments" when they are used in soliciting buyers. Being free from business registration and official supervision leaves WeChat merchants in anarchic status, without the management of or administrative penalty on malicious advertisements existing (Chen 2014, p. 48).

## 4. Primary types of WeChat fraud

### 4.1. WeChat business fraud

In the name of companies, criminals solicit WeChat users to join as business partners, during extra expenses such as which affiliation fee, training fee, product supply fee, or marketing fee are paid by victims, who may receive certain goods but usually they are with low quality and bad sales expectation. In the process of soliciting, fraudsters usually entice victims to stockpile more goods, participating in more training courses and lectures by successful persons. In such circumstances, the victims invest big sums of funds, but there will never be the possibility of high return. In actual fact, many such victims are female acquaintances, whose trust is the basis of another party's wrongdoing (Li 2015, p. 40). For lack of a third-party capital hosting platform in the case of regular shopping websites, victims of WeChat business fraud cannot seek assistance and protection from any intermediaries (Recent Customer Service 2015; Zhu et al. 2015; Ministry of Public Security 2016). Prostitution is not a legal business in China. But in some cases, fraud could be perpetrated under the disguise of prostitution. Between August and November 2014, the suspect Ye and her husband Liu used IP spoofing software, WeChat account, bank card, mobile phone, and SIM card all bought online to issue fake information of prostitution service. From 1 September 2014, when victims contacted them via WeChat or telephone call, Ye disguised as the receptionist or the prostitute to ask for payment of service fee, transportation deposit, personal safety deposit, etc. This way, Ye defrauded victims 35997.57 yuan (Quangang District People's Court 2015).

### 4.2. Abroad purchasing agent fraud

As a result of consumption habits, many domestic Chinese consumers like to purchase goods from abroad. In some cases, goods are not available in the Chinese market. Purchasing from abroad is the main way of acquiring such goods. In other cases, purchasing from abroad is cheaper than in the domestic market, by evading import tax. Lacking a direct transaction method, these consumers seek help from purchasing agents to acquire such goods. There has been for long a grey industry of

abroad purchasing agency. This being a case beneficial to both parties, the consumers, and the agents. For the state, there is no so much interest and energy to deal with such a large amount of small value cross-border transactions. However, another problem takes place. Some criminals claim in WeChat "comments" that they can help purchase from abroad. After the victims pay for the goods, perpetrators claim that the goods are seized by customs and an extra customs duty is required. Victims are required to pay such presumed fees to the perpetrators. However, after all, such presumed fees are paid, not only goods are missing but also perpetrators disappear (Tecent Customer Service 2015; Ministry of Public Security 2016).

### 4.3. QR code fraud

Because QR code is so popularly used in China as a payment method, it is also found by criminals to be a way to make quick money. One of the detected mechanisms is that fraudsters sell products at a discounted price, the payment for which is for the buyer to scan a QR code. Unfortunately, the QR code is in fact implanted with Trojan Horse malware, which can be used by the perpetrators to acquire victims' identification data, including account name and password of the net bank, Alipay, etc. (Tecent Customer Service 2015; Ministry of Public Security 2016).

### 4.4. Stealing WeChat account

The easiest way to acquire users' data, including all the acquaintance contacts of WeChat, is to get control of the WeChat account through stealing account name and password by using Trojan Horse malware. Upon log into a victim's WeChat account, a fraudster can impersonate the victim to send fake messages to WeChat "friends" (including real-world friends, colleagues, classmates, neighbors, or relatives). In these messages, the perpetrator may fabricate some urgent events and ask these "friends" to transfer a certain amount of money. For example, sometimes the perpetrator, in the name of the victim, claims that a certain product is bought and a sum of money should be paid, with the help of the friend. Or, in other circumstances, the perpetrator can also claim that s/he meets special difficulties where a large amount of money is needed and asks a "friend" to transfer money to a bank account (Tecent Customer Service 2015; Ministry of Public Security 2016). This is a simple way of fraud, yet many of the criminals succeeded in the scam. In a case, Liu, a user from Heze City, Shandong Province chatted with Wang, his business partner, saying that he met financial tension in his business and would like to borrow 10,000 yuan from Wang, and promised to repay in two days. Because the two cooperated in their businesses for many years, Wang lent Liu by

transferring the asked sum into an account without delay. After the transfer, Wang made a telephone call to Liu to check the account. Only at this point of time, Wang got to know that Liu had not logged into his WeChat account for a few days, and had never borrowed money from him (Dong and Gao 2014).

### 4.5. Fraud via identity spoofing

”Shake", "people nearby" and "message in a bottle" can be used in finding strangers to send unsolicited messages in order to make new WeChat "friends" (contacts). Similar to the real-world meeting, fraudsters firstly ask for the main information of a victim, such as sex, age, marital status, and so on, based on which the perpetrator fabricates information about him/herself. If the victim is a single person, the fraudster can shape him/herself as one who is a suitable potential girl/boyfriend of the victim, according to the counterpart's own information. One day, they become friends of different sexes and are talking about potential marriage. But at some point in time, the fraudster fabricates some urgent events where a big sum of money is needed and where benevolence of the victim is a natural process. The fraudster will not directly ask the money from the victim, pretending that s/he has an image of independence and inspiration. Only after a period of time, the fraudster lies that s/he has no other choice than to borrow money from the victim, and this is the final result of the scam (Tecent Customer Service 2015; Ministry of Public Security 2016). Another way is to impersonate a friend of the victim (Li 2015, p. 40). Ying is an accountant of a company. One day, she received a request from a user to add as a “friend”. The person impersonated as her company leader. So she confirmed him as the “friend”. Shortly after, the leader invited her to a WeChat group, where 5-6 members are company "leaders", discussing a project, involving a discussion about the issue of investment. The leader commanded her to make an urgent transfer of a sum of 1.4 million yuan to an account, and approval formalities could be supplemented afterward. Ying rushed to the bank to make the transfer and returned afterward to the leader to sign the formalities. Unexpectedly, the leader denied the fact, without knowing anything about the WeChat group. When Ying reported to the police, a preliminary investigation found that all the "leaders" in the group were fake. Fortunately, the police had time to freeze two bank accounts involved in the scam and avoided the whole loss (Lin 2015).

### 4.6. “Likes” collection scam

There are two fraudulent modes in this category. One way is to claim that if a user collects a certain number of "likes", the user can be granted a gift or sold a kind of product at a discounted price. However, when the user has collected the "likes", the

gift or the product is not like what it was described. Another mode is about acquiring other users' data. Usually, fraudulent businesses or merchants will not reveal their authentic location but only goes with a telephone number, by which they claim that only the winners of the "likes" collectors will be notified. So the users have to give their name and telephone numbers to the businesses or the merchants. As a result, the "likes" collection scam appears to be a legitimized way of collecting information from multiple users, including their names and telephone numbers. Once they have collected a certain amount of data, these websites will be rendered unavailable automatically (Tecent Customer Service 2015; Ministry of Public Security 2016).

### 4.7. Fake subscription account fraud

The scammer starts with group messaging with the content of distributing a gift to anyone who follows the subscription account. Whoever follows, who will get. Victims have to fill in detailed contact information as required by the notice of the subscription account. Such data cover the WeChat account name, real name, mobile phone number, address of residence, etc. These are reasonably needed for any product delivery in China. But of course, they will not be used in delivering any gift b the fraudsters. On the contrary, fraudsters make a one step further to defraud the victims, by claiming that "in order to endure that each person receive only one gift, verification code should be submitted once it is received." Once the verification code is input, money in the WeChat Wallet will be transferred from the victim to the criminal. It turns out that such a verification code is used when a transfer is made from WeChat Wallet. Only when this happens, the user can find that s/he has become victimized in the scam (Tecent Customer Service 2015; Ministry of Public Security 2016).

### 4.8. Fake "red packet" fraud

The red packet, distributed frequently on the WeChat platform, is a digitalized variant of the traditional "red envelope". It is mostly a new mode of amusement and entertainment among WeChat "friends". Users are amused and entertained when they can "grab" a red packet, sometimes with a bigger sum of money, or sometimes only a sum of money with a number that lower-educated persons think is a "lucky" number. Criminals will consider the psychology of such users and programmed a kind of Trojan Horse malware, disguised as red packets to distribute on the WeChat platform. Once clicked open, the malware will be able to steal the mobile user's password of WeChat Wallet, bank card number and password, and even intercept verification code sent via instant messaging, redirecting the message from the victim's mobile phone. Once the mobile is infected with the Trojan Horse

malware, fraudsters can easily have control over the mobile phone and spend money from the user's WeChat Wallet and linked bank card. Because verification sent via instant messaging meant for the victim is intercepted by the perpetrator, the victim can hardly know that s/he becomes victimized and suffers a loss (Tecent Customer Service 2015; Ministry of Public Security 2016).

### 4.9. Fake benevolence fraud

Criminals distribute notices by fabricating information of a missing person, or a person in special financial need. Many benevolent WeChat users help to publicize the notices to a broader audience, many of whom dial the telephone numbers in the notices. But some of these telephone numbers are themselves are designed to induce high telephone fees. Other numbers can also be used in further telecommunication fraud (Tecent Customer Service 2015; Ministry of Public Security 2016). In a criminal case sentenced in 2016, multiple social media services were involved. Yang, the suspect fabricated the name "Xu Zihao" to make "friends" with Yang A on social media "Momo" in January 2016. During their virtual communication, Yang registered a WeChat account, uploaded fake photo, and fabricated identification and life experience, which produced a good impression on Yang A. IN the same month, when Yang knew that Yang A would travel to Lanzhou, where Yang lives, he pretended as "Wang Xin", the elder brother of "Xu Zihao" to meet Yang A. In order for Yang A to trust him, Yang continued to contact via telephone and WeChat with Yang A. Later, Yang asked Yang A to help him to raise funds on the grounds that he would replay a sum of the usurious loan and pay compensation. From 22.1.2016 to 7.5.2016, Yang A transferred 36620 yuan to Yang via the WeChat account. The defendant was sentenced to one year of imprisonment with one year period of probation, and 5000 yuan of fine, considering that the suspect returned the whole sum of money when the case was reported to the police (Qilihe District People's Court 2016, see also Longtan District People's Court 2013).

## 5. Prevention of Fraud on Social Media

### 5.1. Promotion of security awareness of WeChat users

Even though victims are not to be blamed, the biggest loopholes for WeChat fraud exist at the side of potential victims, who are careless in making new "friends". The WeChat users need to remember that "jiaoyou xu jinshen" (be careful in making new "friends"), as an old Chinese saying told. In addition, being keen on getting petty advantages is the main psychology in suffering a big loss. A WeChat function

of blocking the "friend" can also be used to help users free from being harassed (Chen 2014, p. 48).

### 5.2. Enhancement of prevention consciousness

As a new type of fraud, WeChat fraud is an offense that many users do not have sufficient consciousness of prevention. In a sentenced case, Song, falsely claiming that his mobile was missing, borrowed and used Pan, the victim's mobile phone. Taking advantage of using Pan's mobile phone, Song stole Pan's data, including his identification card number, bank account number, etc. In addition, Song also used Pan's tablet to log into his own WeChat account, to which he bound pan's bank account. Then, he transferred Pan's money, a total sum of 8900 yuan, in the bank card to his own account through WeChat Transfer and WeChat Red Brackets (Jiangwu District People's Court). In fact, if the victim has the prevention consciousness, such as the case would never have taken place. Training and education (usually missing) should be taken to help users to be careful in WeChat shopping, during which buyers should always verify sellers' identity and address, ask for receipts from sellers. Officials from law enforcement also propose that government agencies should organize such training, education, and issue alerting to users so as to improve their consciousness of prevention (Chen 2014, p.48).

### 5.3. Real-name system in registration

For a long time, verification of WeChat accounts and subscription accounts has not been strictly executed. Registration can be completed only when a user fills in part of his/her data. If the service operator can borrow from other institutions' real-name registration mode, requiring a user to provide sufficient compulsory data, such as name, identification number, mobile phone number, address, bank card information, that can be used to find the whereabouts of the user. At the same time, the consistency of such information and the real person should be verified. The proposed stricter method is that the user should be required to provide photos of his/her identification card, to realize a system of one account for each person, and one account for each telephone number. Another mechanism is for the WeChat to introduce a channel for reporting suspected accounts, which can be blocked by an individual user or permanently blocked by the service operator.

### 5.4. Supervision of network

In China, due to the prevalence of online illegal activities, supervision of the network by public security agencies has been a routine practice for years. It is easy to understand that many officials from law enforcement proposed stricter supervision on WeChat messaging, implementing immediate disposal upon illegal

activities. Due to the existence of such real-time supervision, the suspect can be more quickly detected and found. Of course, there are more social media than WeChat, it requires much investment of human and financial resources into the supervision.

### 5.5. Enhancing supervision of WeChat business

WeChat business is operated in completely a free market without specific supervision. As mention above, there can be an advertiser, purchasing agent, selling agent, and individual wholesaler and retailer. Generally, WeChat merchants advertise their goods with WeChat "comments", demonstrating product pictures for their "friends", who are potential buyers of these products. A normal understanding of such a business is that this is a kind transaction in a completely free market, free of supervision, free of tax, free of transaction fee, and voluntary transaction. However, understanding in another way, as in fact, WeChat is increasingly used by potential perpetrators who register WeChat accounts deliberately designed to defraud others, who become "friends" via functions such as "shake", "people nearby" or "message in a bottle". After they become "friends", the perpetrator claims that s/he is abroad purchasing agent or has sources of certain popular goods, which are not true. After the victim pays, s/he will not receive anything, while the fugitive will close the account and disappears. Therefore, some writers propose some extra alerting be used in WeChat to warn of risks in WeChat business, such as pop-up alerting, etc. In addition, a real-name system can also be an effective way to deter occurrences of fraud.

### 5.6. Training of police team

It has also been recognized that techniques, skills, and experience of law enforcement officials also face great challenges due to the fast development of information technology, as well as a fast change of laws and regulations. It is natural that frequent training and education should also be provided for law enforcement officials.

## 6. Conclusions

As many other offenses committed online, WeChat fraud can also be highly secret with a big dark figure and difficult to be detected and investigated. Even the case is found, the defrauded funds through the WeChat are difficult to be recovered. One of the features characterizing WeChat fraud is its transterritoriality which puts a spatial distance between the criminal and the victim. While WeChat fraud is a cost-effective way for potential perpetrators to make profits from illegal activities, it is a costly process for the law enforcement to investigate the case. It is an "expensive"

crime for the young generation, to which most of the criminals and victims belong. In addition, only such profitable new forms offenses can "inspire" criminals to invent more and more means of defrauding.

The reason why social media fraud is so popular among contemporary telecommunication users can be attributed to curiosity induced by the novel and unique functions of these social networking services, the rapid development of WeChat business, convenience and rapidity of new payment methods, as well as loopholes, such as non-real-name registration system of WeChat users, and missing of laws and supervisory mechanisms. Whenever there are some new inventions, there will be at the same time malicious exploitation of such inventions. It proved to be a general rule from the point of view of the history of crime and punishment.

The article gave more evidence that can support the idea to classify WeChat fraud into different types, including WeChat business fraud, abroad purchasing agent fraud, QR code fraud, WeChat account theft, fraud via identity spoofing, “likes” collection scam, fake “red packet” fraud, and fake benevolence fraud. Some of them have been practiced in traditional offenses, others in new cyber frauds, yet some are particular tailored to cope with specific functions of the WeChat platform.

Based on the analysis of the features, types, and reasons of WeChat fraud, the article proceeded to recommend preventive methods, such as the promotion of security awareness of WeChat users, enhancement of prevention consciousness, a real-name system in registration, enhanced supervision of network services, enhanced supervision of WeChat business, and training of police team. These can be seen as the active intervention of the society in the maintenance of the social order in cyberspace.

As every kind of crime, fraud through WeChat and other social media can have a process of development, from fewer to more, reaching a climax, and then keeps at a stable level, becoming a routine type of crime. Nevertheless, active prevention will constrain such a developing tendency to an extent as small as possible, beneficial to the preservation of a healthy social environment.

**Acknowledgments**

The author thanks the anonymous reviewers and editor for their valuable contribution.

**Funding**

This research received no specific grant from any funding agency in the public, commercial, or not–for–profit sectors.

## Author Contributions

The entire article was written by Xingan Li.

## Disclosure Statement

The author has not any competing financial, professional, or personal interests from other parties.

## References

1. Anning District People's Court, Lanzhou City, Gansu Province, (2015). Criminal Judgment (2015) Gan 0105 Xing Chu 213 Hao.
2. Beilin District People's Court, Suihua City, Heilongjiang Province, (2015). Criminal Judgment (2015) Sui Bei Xing Chu Zi Di 267 Hao.
3. Chen, L., (2014). Weixin fanzui de tedian, chengyin ji fangkong (Features, causes and prevention of WeChat crime). Journal of Jiangsu Police Institute. vol. 29, no. 1. pp. 45-50.
4. Chengzhong District People's Court, Liuzhou City, Guangxi Autonomous Region, (2015). Criminal Judgment (2015) Chengzhong Xing Chu Zi Di 397 Hao.
5. Dong, M. and Gao, Y., (2014). Weixin zhapian fangshi duoyang, pianzi dao taren weixin hao tao zoi wanyuan (Various means of WeChat fraud, fraudster stole WeChat account and swindled 10000 yuan). Qilu wanbao (Qilu Evening). Retrieved 10 December 2019, from http://www.ccidnet.com/2014/1008/5625585.shtml
6. Dong, Shujun; Li, X., (2016). Besieged Privacy in Social Networking Services. International Journal of Electronic Security and Digital Forensics, 8 (3), 224–233.
7. Emeishan City People's Court, Sichuan Province. Criminal Judgment, (2016). Chuan 1181 Xing Chu 223 Hao.
8. Fengtai District People's Court, Beijing Municipality, (2015). Criminal Judgment (2015) Feng Xing Chu Zi Di 1652 Hao.
9. Foshan Intermediate People's Court, Guangdong Province, (2013). Criminal Judgment (2013) Fo Zhong Fa Yi Zhong Zi Di 447 Hao.
10. Huma County People's Court, Heilongjiang Province, (2016). Criminal Judgment (2016) Hei 2721 Xing Chu 18 Hao.
11. Jiangwu District People's Court, Shaoguan City, Guangdong Province, (2016). Criminal Judgment (2016) Yue 0203 Xing Chu 219 Hao.
12. Jiaoling County People's Court, Guangdong Province, (2015). Criminal Judgment (2015) Mei Jiao Fa Chu Zi Di 104 Hao.
13. Jiashan County People's Court, Zhejiang, (2016). Criminal Judgment (2016) Zhe 0421 Xing Chu 500 Hao.
14. Li, Y., (2015). Dangqian wangluo zhapian anjian zhi tedian jiqi zhencha lujing (Characteristics of recent cases of cyber fraud and approach to detection). Journal of Shanghai Police College. vol. 25, no. 4, pp. 38-46.
15. Lin, J., (2015). “Lingdao” weixin zhishi huikuan 1.4 million yuan (”Leader” demanded via WeChat to transfer 1.4 million yuan), Beijing wanbao (Beijing Evening). 27.12.2015, C4.

16. Longtan District People's Court, Jilin City, Jilin Province, (2013). Criminal Judgment (2013) Long Xing Chu Zi Di 340 Hao.
17. Lufeng City People's Court, Guangdong Province, (2017). Criminal Judgment (2017) Yue 1581 Xing Chu 31 Hao.
18. Mawei District People's Court, Fuzhou City, Fujian Province,( 2016). Criminal Judgment (2016) Min 0105 Xing Chu 186 Hao.
19. Ministry of Public Security, (2016). Gongan Bu Gonkai 48 Zhong Changjian Dianxin Zhapian Fanzui Anjian (Ministry of Public Security publicized 48 types of telecommunication scams). Retrieved 10 December 2019, from http://society.people.com.cn/n1/2016/0127/c1008-28090338.html
20. Nangang District People's Court, Haerbin Ciity, Heilongjiang Province, (2016). Criminal Judgment. (2016) Hei 0103 Xing Chu 188 Hao.'
21. Nanshan District People's Court, Shenzhen City, Guangdong Province, (2014). Criminal Judgment. (2014) Shen Nan Fa Xing Chu Zi Di 773 Hao.
22. Nanxi District People's Court, Yibin City, Sichuan Province, (2014). Criminal Judgment (2014) Nanxi Xing Chu Zi Di 134 Hao.
23. Qilihe District People's Court, Lanzhou City, Gansu Province, (2016). Criminal Judgment. (2016) Gan 0103 Xing Chu 566 Hao.
24. Quangang District People's Court, Quanzhou City, Fujian Province, (2015). Criminal Judgment (2015) Gang Xing Chu Zi Di 222 Hao.
25. Ruian City People's Court, Zhejiang Province, (2015). Criminal Judgment (2015) Wenrui Xing Chu Zi Di 1418 Hao.
26. Songjiang District People's Court, Shanghai Municipality, (2016). Criminal Judgment (2016) Hu 0117 Xing Chu 1278 Hao.
27. Taipusi Qi People's Court, Inner Mongolia Autonomous region, (2015). Criminal Judgment (2015) Tai Xing Chu Zi Di 54 Hao.
28. Taocheng District People's Court, Hengshui City, Heibei Province, (2016). Criminal Judgment (2016) Ji 1102 Xing Chu 15 Hao.
29. Tencent Customer Service, (2015). Weixin shi da changjian zhapian shouduan (Ten popular means of fraud). Retrieved 10 December 2019, from http://kf.qq.com/touch/faq/1509157Bvyq21509152eaQBj.html?platform=48.
30. Tencent Holdings Company, (2016). Tecent Published 2016 Third UQarterly Report. Retrieved 10 December 2019, from http://www.tencent.com/zh-cn/articles/15000551479986174.pdf.
31. The People's Supreme Court of the People's Republic of China, (2013). Civil Judgment (2013) Min San Zhong Zi Di 4 Hao, Qihu v. Tenxun.
32. The Supreme People's Court of the People's Republic of China, (2015). Tongguo wangluo shishi de qinfan funv weichengnian rend eng fanzui dianxing anli (Typical criminal cases against women and minors through netowkr). Retrieved 10 December 2019, from http://www.court.gov.cn/zixun-xiangqing-13328.html.
33. Wexin Customer Services, (2019). Ten Popular Tricks of Fraud in Wechat. Retrieved 10 December 2019, from https://kf.qq.com/touch/faq/1509157Bvyq21509152eaQBj.html?platform=48.

34. Xiangzhou District Peoples Court, Zhuhai City, Guangdong Province, (2016). Criminal Judgment (2016) Yue 0402 Xing Chu 1405 Hao.
35. Xinji People's Court, Hebei Province, (2016). Criminal Judgment (2016) Ji 0181 Xing 88 Hao Chu.
36. Xinshi District People's Court, Wulumuqi City, Xinjiang Uygur Autonomous Region, (2016). Criminal Judgment (2016) Xin 0104 Xing Chu 830 Hao.
37. Xu, H., (2015). Qian tan weixin tongxun de xingqi (Talking about the emergence of WeChat communication). Retrieved 10 December 2019, from http://www.xuehuile.com/thesis/70c8f9abedce434fbe2e099cd1d6668f.html.
38. Xuhui District People's Court, Shanghai Municipality, (2015). Criminal Judgment (2015) Xu Xing Chu Zi Di 1063 Hao.
39. Yakeshi City People's Court, Inner Mongolia Autonomous region, (2015). Criminal Judgment (2015) Ya Xing Chu Zi Di 172 Hao.
40. Yiwu City People's Court, Zhejiang, (2016). Criminal Judgment (2016) Zhe 0782 Xing Chu 697 Hao.
41. Zhu, K., (2015). Gongan jiguan yingdui weixin zhapian de celue (Strategy of Public Security Agency in Dealing with WeChat Fraud). Society and Youth, no. 31, pp. 48-50.
42. Zhu, X; Wei, L., and Wang, L., (2015). Weixin pengyouquan cheng shoujia xin qudao. Procuratorial Daily. 26.4.2015. C1.
43. Zigong Intermediate People's Court, Sichuan Province, (2016). Criminal Judgment (2016) Chuan 03 Xing Zhong Zi Di 18 Hao.