FRAUD AND OTHER VITAL PROBLEMS OF THE MODERN DIGITAL SOCIETY

Gedakyan D.A.

3rd year student

Academy of Law and National Security

Southern University

email: diana.gedakyan@yandex.ru

Scientific supervisor: Galoyan Y.E.,

PhD, Head of the Academy of Humanitarian Technologies

Abstract: The given article deals with a problem of fraud in telecommunication nets, a special attention is given to new schemes of illegal activities of the fraud in the modern society. There has been offered a special set of recommendations preventing the type of fraud under the discussion. The preventive strategy of the given type of the crime is suggested.

Keywords: telecommunication networks, telecommunication fraud, counteraction, theft, responsibility, preventive measures

Digital society in modern conditions gives rise to new schemes of deception of citizens. The advancement of technological tools such as computers, the internet, and cellular phones has made life easier and more convenient for most people in our society. However some individuals and groups have subverted these telecommunication devices into tools to defraud numerous unsuspecting victims. It is not uncommon for a scam to originate in a city, country, state, or even a country different from that in which the victim resides.

While senior citizens are believed to be the most frequent targets of scam artist, community outreach is another underutilized strategy to address telecommunications fraud. If community outreach can prevent even a few persons from being victimized, the effect on law enforcement resources can be very beneficial. Possible community outreach strategies include a fraud alert system, public service announcements released to the media, and training community groups about on-line and telephone safety.

Telecommunication fraud is the theft of telecommunication service (telephones, cell phones, computers etc.) or the use of telecommunication service to commit other forms of fraud. Victims include consumers, businesses and communication service providers.

There are several types of telecommunications fraud:

- 1) Identity theft the misuse of information that is specific to an individual in order to convince others that the imposter is the individual, effectively passing one self off as someone else.
- 2) Internet fraud any type of fraud scheme that uses one or more components of the internet such as chat rooms, email, message boards, or web sites to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.
- 3) Telemarketing fraud any scheme to defraud in which the persons carrying out the scheme use the telephone as their primary means of communicating with prospective victims and trying to persuade them to send money to the scheme.
- 4) Auction and retail schemes these schemes typically attract consumers by purporting to offer high-valve merchandise ranging from expensive jewelry to computers to sport memorabilia at attractive prices. After persuading victims to send money in the form of a personal check, money order, or cashier's check, schemers either send an inferior item or nothing at all.
- 5) Investment scams market manipulation scams are the forefront of this type of scheme. Two methods are used, the first is commonly known as the pump and dump, attempts to drive up the price of thinly traded stocks or stocks of shell companies by sending out e-mails that inflate the value of the company. When new purchases of the stock push its price to a high enough level, the scammers sell off the stock to realize a significant return which in turn drives down the stock price. The second method, referred to as short-selling or scalping, tries to decrease a stock value.

The most common cases in the Russian Federation are SMS requests when a subscriber receives a message from "relatives" or "friends" asking for a transfer of funds due to a problem. Telephone calls, as well as messages about the help of scammers, manage to deceive a very trusting part of the population - elderly people. In order to convince the victim of fraud, criminals can use different methods, namely acoustic technologies that allow changing the timbre and pace of voice beyond recognition, psychological tricks that make it possible to gain confidence in the interlocutor [2]. According to statistics, in the total traffic of telephone conversations, fraudsters account for 2 to 6%, as well as many methods of telephone fraud harm ordinary cellular users. Cellular operators should think about full-fledged security systems: for example, automatically track frequent small transfers to the same telephone number with a subsequent zeros

For the counteraction with the fraud activities the Ministry of Internal Affairs is against of fulfilling the operations according to the instructions obtained in the result of the telephone conversations. In case of doubts about the integrity of the caller, it is better to complete the call and call back the phone number of the bank or mobile operator. You should never trust suspicious calls and text messages - messages, and you should not tell anyone about your bank card, pin code, passwords to log in to your personal account. It is not recommended to click on links to suspicious sites, transfer money only to verified information sources and those who inspire confidence [3]. Telephone fraudsters should be punished, and stolen funds should be returned to deceived victims. If you are still the victim of fraudsters, or indirectly faced with telephone fraud, you must contact your own mobile operator. Law enforcement agencies can easily track who owns the phone number that was used in the crime. When the caller still gives instructions and advice on the transfer of funds and their specific size, but the owner of the phone takes absolutely no action and does not cause any damage, then the crime is considered unfinished. The actions of fraudsters in this case are qualified as preparation or attempted crime. Punishment follows only with a large amount of possible damage and the collusion of several persons. Liability for fraud is provided for in Article 159 of the Criminal Code of the Russian Federation.

Even in the absence of aggravating circumstances, the offender faces up to 2 years in prison. If the fraudsters acted as a group or at least ten thousand rubles were received from the victim by deception - they face up to 5 years in prison. Criminals can be obliged to return the received by deception, as well as compensate for moral damage. If we examine the judicial practice on these types of fraud, decisions in such cases are made in favor of the victim.

In this respect the conclusion can be made that there exists different types of the fraud as the fraudsters can mislead the citizens due to the lack of knowledge and information by the subscribers of the tariffs for the mobile operators, trusting relationships, lack of experience in the use of online shopping and applications concerning money transactions.

The state should also provide both the mobile operators and their customers with the legal protection. Law enforcement agencies are seriously investigating cases of cellular fraud. Mobile operators, companies that produce various equipment and mobile phones are constantly developing new ways and methods to protect against criminals. Nevertheless, we note that the complete eradication of this type of fraud in modern society is impossible, but preventive measures to combat it reduce the number of deceived people, as well as prevent new crimes related to telephone fraud.

References

- 1. Criminal Code of the Russian Federation. Moscow: Prospect, 2020. 336 p.
- 2. Antoshina, S.M. Fraud in the modern telecommunications /S.M. Antoshina // History and Law. 2018. N_2 3. p. 12-27.
- 3. Bolzhelarskaya K.N. Legal awareness in the conditions of digitalization of society // Intellectual Resources for Regional Development. 2019. p. 291-294
 - 4. Rassel, Jessy Mobile fraud / J.Rassel. M.: VSD, 2019. 524 p.
- 5. Shabelnikova E.V. The role of state regulation of the transport industry of the Russian Federation in the conditions of digitalization // Intellectual Resources for Regional Development. 2019. p. 294-297.
 - 6. Sheinov, V.P. How to protect against fraud/ V.P. Sheinov. M.: Harvest, 2019. 464 p.