ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 12, December 2021 SJIF 2021 = 7.492
A peer reviewed journal

QUALIFICATION OF FRAUD AND WAYS TO AVOID ONLINE BANKING FRAUDS: A STUDY FROM UZBEKISTAN AND INDIAN PERSPECTIVE

Khurshida Mirziyatovna Abzalova*; Dr. Bhupinder Singh**

*Associate Professor, Doctor of Law,
Tashkent State University of Law UZBEKISTAN
Email id: khurshida.abzalova@yandex.ru

**Associate Professor,
CHRIST (Deemed to be University) INDIA

DOI: 10.5958/2249-7137.2021.02728.2

ABSTRACT

Currently, so-called "high technologies" are actively used in the banking sector, including remote banking systems or online banking. Meanwhile, the emergence of these banking services has significantly complicated the qualification of thefts committed in the field of banking services. Online banking is a set of information technologies aimed at providing banking services via the Internet, without a client's personal visit to the bank. The most common example of online banking is banking operations using telephones, computers, ATMs.

KEYWORDS: *ATM, modifying, Criminal Code, globalization, regulatory, Triangle fraud, Banking, M-banking, BSBD, CCTV.*

INTRODUCTION

At present, a number of problems can be identified that arise during the qualification of this type of theft. First of all, what will be the qualifications of thefts committed using these devices, if the offender uses the input or modification of computer information and deception of the victim at the same time. In this case, one and the same set of criminal acts often receives a different criminal legal assessment. For example, let's say a person finds advertisements for the sale of property on the Internet, contacts the advertiser and convinces him to provide his bank card number and access code. After that, the offender registers in automated systems on behalf of the cardholder and gains access to all the accounts of the victim. And then there is a transfer of funds from the accounts of the victim to the accounts controlled by the fraudster. **[1]**

In this regard, it seems appropriate to formulate rules for the qualification of theft committed simultaneously by entering (modifying) computer information (Article 278^4 of the Criminal Code) and deception (paragraph "c" of Part 2 of Article 168 of the Criminal Code), which will solve this problem.

The Main Part

We believe that the distinction between fraud and fraud in the field of computer information should be based on the following rules.

Firstly, in cases where deception is used by a person to facilitate access to someone else's property, which is then stolen in another way, action cannot be qualified as fraud (under Article 168 of the Criminal Code).

Secondly, action cannot be qualified as fraud also if the opportunity for the criminal to dispose of the thing does not occur as a result of deception. **[2]**

Based on these rules, it seems necessary to make a number of clarifications to the Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan dated October 11, 2017 No. 35 "On judicial practice in cases of fraud". Firstly, it is necessary to establish that in cases where deception is used by a person to gain access to bank account data, and property is stolen by entering, modifying computer information, the deed should be qualified by a set of crimes in the form of fraud using computer equipment (paragraph "c" of Part 2 of Article 168 of the Criminal Code), and modification of computer information (Article 278 of the Criminal Code). Secondly, it should be indicated that if a criminal, using computer information (by sending via a mobile device via the Telegram messenger, e-mail or other means of sending various messages), acquires the ability to dispose of the property or property rights of the victim directly as a result of deception (for example, a person voluntarily transfers a sum of money to the criminal), then the action must be qualified as a fraud, taking into account the size of the stolen property according to the relevant parts of Article 168 of the Criminal Code, but without reference to paragraph "c" part 2 of this article, since a mobile device cannot be equated to a computer device. **[3]**

The second problem in the field of qualification of crimes committed using online banking systems is the qualification of thefts committed using payment cards using an ATM. Today, they have begun to receive a fairly noticeable spread. In this regard, in law enforcement practice and science, discussions began to arise regarding the qualification of these actions as fraud under paragraph "c" of Part 2 of Article 168 of the Criminal Code, since an ATM in its essence is a computer.

At the same time, many note the specifics of this fraud: the impact is carried out on computer information, and not on the consciousness of the victim; there is no deception of the person, there is no transfer of property or the acquisition of the right to property with the help of the victim; information, means of storage, transmission and processing of computer information is recognized as an instrument of crime.

It is worth noting that, for example, in foreign judicial practice (Resolution of the Plenum of the Supreme Court of the Russian Federation No. 51 of December 27, 2007 "On judicial practice in cases of fraud, misappropriation and embezzlement"), these actions are qualified as theft.

Getting a credit at a terminal and receiving money at an ATM using a fake card have a common feature - the absence of deceptive actions inherent in fraud. Therefore, for qualification of a getting a credit by using someone else's passport, from which a copy is automatically taken by the terminal, paragraph "c" of Part 2 of Article 168 of the Criminal Code cannot be used. These actions contain rather signs of theft and should be assessed by virtue of their identity in the same way as the theft of funds at an ATM by using a fake credit card.

It is hardly possible to recognize as justified the different qualifications of the theft of credit in the form of cash and cash from an ATM, if in both cases the counterparty in the transaction was

a computer, and not a person authorized by the organization, misled by the actions of the subject, and the item of the crime was cash.

At the same time, we believe that the actions of a person installing special technical devices on an ATM, followed by the theft of funds from a bank card (by reading information, codes and passwords of the card) should be qualified not only under paragraph "c" of Part 3 of Article 169 of the Criminal Code (with unauthorized entry into a computer system), but also under Article 278^2 of the Criminal Code (Illegal (unauthorized) access to computer information), since the disposition of the article refers, among other things, about "interception of information". **[4]**

As a solution to these problems, we propose to amend the Plenum of the Supreme Court of the Republic of Uzbekistan No. 35 dated October 11, 2017 "On judicial practice in cases of fraud" and state paragraph 20 of the Resolution as follows:

"20. Explain that fraud with the use of computer equipment (paragraph "c" of the second part of Article 168 of the Criminal Code) is understood as theft by deception of someone else's property located in financial, banking institutions, funds, etc. through manipulations performed with the help of computer equipment. Such fraud can be committed both by changing information processed in a computer system stored on appropriate media or transmitted over data transmission networks, and by introducing false information into the computer system of financial and banking institutions.

In the case when deception is used by a person to gain access to bank account data, and property is stolen by entering, modifying computer information, the action should be qualified as a set of crimes in the form of fraud using computer equipment (paragraph "c" of Part 2 of Article 168 of the Criminal Code), and modification of computer information (Article 278^4 of the Criminal Code).

At the same time, if a criminal, using computer information (by sending via a mobile device via the Telegram messenger, e-mail or other means of sending various messages), acquires the opportunity to dispose of the property or property rights of the victim directly as a result of deception (for example, a person voluntarily transfers money to the criminal amount), then the action must be qualified as fraud, taking into account the size of the stolen property in accordance with the relevant parts of Article 168 of the Criminal Code, without reference to paragraph "c" of Part 2 of this article.

The actions of a person installing special technical devices on an ATM, followed by the theft of funds from a bank card (by reading information, codes and passwords of the card) must be qualified under paragraph "b" of Part 3 of Article 169 of the Criminal Code (with unauthorized entry into a computer system), as well as under Article 278^2 of the Criminal Code (Illegal (unauthorized) access to computer information)".

In our view, the introduction of these clarifications, in the absence of currently relevant articles on cyber theft in the Criminal Code of Uzbekistan, can assist law enforcement agencies and courts in the uniform and correct qualification of this kind of new types of theft. **[5]**

The Web Revolution has occurred in India over the previous decade, and it is one of the most significant events in human history. The fast expansion in the usage of the web, the Internet, Intranet and Extranet, e-business or e-commerce, and mobile commerce has transformed the way

practically every company does business. Traditional financial intermediaries such as commercial banks, investment banks, and specialist finance businesses are blurring due to technological innovation. The rise of e-business, along with technical advancements and globalisation, is forcing organisations to rethink their company processes in terms of value chain re-engineering and business model restructuring. The financial industry is most likely undergoing a transformation as a result of competitive, regulatory, and technological dynamics. The financial system, particularly the banking sector, is now under transformation. Banks are the engines that fuel the financial sector's operations, which are critical to every country's economy. One of the oldest industries in the world is banking. The Indian banking industry has not remained a completely oblivious observer of the global information technology revolution. The banking business in India has seen significant changes as a result of the 'web Revolution.' In today's digital era, computers and electronic media are used to conduct all financial transactions. To cope with the growing rate of change in the business environment, banks have placed themselves on the World Wide Web to take use of the internet's power and reach. 'PC banking,' 'online banking,' 'Internet banking,' 'Telephone-banking,' or'mobile banking' are all terms used to describe electronic banking. E-banking is a phrase that encompasses all of these methods of doing financial transactions online. **[6]**

In the world of internet banking, fraudulent transactions have become a significant concern. As technology advances, fraudsters' tactics of deception evolve as well. There are also growing technologies that allow fraudsters to imitate the transaction behaviour of actual consumers, and they are constantly modifying their approaches to make fraud detection harder.

The importance of fraud has a great economic impact on a society. This issue is certainly relevant in every country, but also in to every organization. Well-known world financial scandals warn that fraud is increasingly having not only individual characteristics but also organizational ones. In literature and practice. Numerous studies of this concept have been conducted on the basis of which numerous models of fraud have been conceived. The first model that was conceived, it was a model of the triangle of deception. This basic model has existed for 60 years and was proposed during that period are different elements of modification, but this model served and as a basis for designing other, new models. Theoretical and empirical research has shown that this model in modern business conditions it is no longer efficient either unreservedly applicable. **[7]**

The main issues highlighted in this paper relate to the various shortcomings that this the model shows. From the proposal to all three elements of the triangle mathematically ratify, through the economic logic of the triangle, to the psychological aspect of studying the triangle of deception. It's in the works presented one of the mathematical models which encompasses all three elements of the triangle and which tries to answer the requirement of practice and possible mathematical expression of the probability of committing fraud from the point of view of mathematical ratification all three elements of the triangle. The fraud triangle analysis is significant and because of audit and audit risk. An analysis of opinions is presented, which gives paramount importance to the interaction of management integrity and pressure and integrity management and opportunity. Model reviews triangle frauds are rooted in the shortcomings of this model. Behavior of individuals in the same situation as one commits fraud and the other does not, is one of the open questions for criticism and request for improvement of the base model. Triangle

fraud describes the conditions under which fraud is committed, but not describes the actions taken by the fraudster.

The backbone of a country's economy is banking and financial services, and information technology serves to fuel this infrastructure. Financial systems should be stable in a developing economy. As technology progresses, the reach of Online Banking expands as consumers find it more convenient to perform their banking online rather than in person to visit the bank. For example, opening an account online, making transactions online, and double-checking all the information online. All of this is quite convenient for the consumers. As a result, the majority of banks are now insolvent offering people with internet services Banking entails preserving consumer relationships and, if necessary, trust nature is crucial. Customer happiness is critical to retaining long-term business.

A user can use the website of a financial institution to complete several activities on his account connected to finance in online banking. It's also known as 'Internet Banking.' Banking systems, as we all know, are where a bank employee physically deals with the consumer and answers his questions, but with Internet Banking, we're attempting to integrate the primary banking systems with Online Banking to make things easier for customers.

The Indian banking business is unique, with no analogues in the history of banking in any other country. The banking industry has gone through three stages since independence: character-based lending, ideology-based lending, and competitiveness-based lending. Despite having a robust regulator, the financial services industry has been identified as the most vulnerable to fraud. ICT has infiltrated practically every aspect of life. The primary consumers of the internet and online transactions are banking, insurance, and financial institutions. They utilise ICT to perform cash transfers, payments, account information submissions, and other remittance services. Banking services have, without a doubt, been greatly enhanced as a result of the usage of information and the internet. At the same time, internet transactions and data are vulnerable to hacking and manipulation. Financial scams related with these transactions are also on the rise, resulting in significant financial losses every year throughout the world. The use of possibly unlawful means by workers to get money, assets, or other property owned or held by a bank or financial institution, or to collect money from depositors by falsely masquerading as a bank or other financial institution, which is a significant component of operational risk. In India, the number of bank frauds is significant, and it is growing with the passage of time and technology.

The internet and mobile phones are two technical advances that have had a significant impact on all of us in the previous decade and are presently on the rise. This association's goods are mobile data services. Services are being developed using a number of platforms to enable mobile devices to fulfil many of the traditional internet's functions, although in a compressed manner for mobile devices. Mobile banking is one of the areas of activity (one of the first areas of commercial transaction on the wireless internet). Banking has expanded in a variety of ways in recent years, notably through telephone and internet banking. M-banking adds another route for financial services, with the potential to become the major channel in emerging economies. The hottest area of growth in the banking business is mobile banking, which is a symbiosis of technology and financial services and is predicted to replace the debit/credit card system, as well as internet banking.

How to avoid online banking frauds in India?

The Reserve Bank of India has issued certain guidelines for users in case they fall victim to online banking frauds:

1. Banks must create their banking system and procedures in order to make way for safe net banking for customers.
2. The liability of customers is limited in case of any unauthorised net banking transactions.
3. The banks must inform their customers about SMS and email alerts for online banking transactions.
4. If an unauthorised online transaction has taken place because of a third party and it is reported within 3 days by the customer, the bank must credit the amount back in the customer's account within 10 days of receiving the complaint.
5. If a customer delays in reporting an online banking fraud within 3 days and delays for 4-7 days, the customer will be penalised with up to Rs. 25,000 fine depending upon the type of bank account, credit card held by the customer and any gift cards used.
6. The liability for delay in reporting online banking fraud for Basic Savings Bank Deposit (BSBD) account is Rs. 5000; the liability for delay in reporting online banking fraud for Savings account, prepaid transactions, an overdraft account, Current account, cash credit account, gift cards accounts for MSMEs and accounts for individuals with an annual balance or limit of Rs. 25 lakhs, is Rs. 10,000; for other accounts with credit card limit of Rs. 5 lakhs, the maximum liability is Rs. 25,000.
7. For the loss caused by an unauthorised transaction, the bank will be held liable.
8. For unauthorised transactions with third party liability, any delay in reporting will attract liability up to the amount of transaction.
9. For a delay beyond 7 days, the customer liability will be determined in accordance with the bank's policy approved by the Board.
10. The banks must resolve the customer complaint within 90 days of receiving it.

For more queries or confusion regarding the legal nitty gritty of online banking fraud in India, ask for **expert legal advice** from us now!

How to file a complaint about online banking fraud in India?

The first step is to report the crime immediately to the bank. The bank has to ensure that reasonable measures are taken to provide sage net banking to its customers. The bank must install CCTV camera in bank premises and ATM outlets, notify customers through email and SMS alert about any transaction from their account, track irregular or unusual transaction, etc.

A person who falls victim to any online banking fraud can file an application with the Adjudicating Officer under **Section 46 of Information Technology Act, 2000** for lack of reasonable security measures taken by the bank. **Section 43A of Information Technology Act, 2000** states that the banks and other intermediaries that do not use reasonable security measures for safe banking will be liable to pay adequate compensation to the customer. The bank has the

liability to prove that it took sufficient measures to prevent any illegal and unauthorised transactions.

REFERENCES

1. Orekhov VV. Necessary defense and other circumstances precluding the criminality of the act. St. Petersburg: "Piterubl", 2008. p.46.

2. Kozak VN. The Right of Citizens to Necessary Defense. Saratov: "Publishing house Sarat", 1972. p.41.

3. Borodin SV. Responsibility for murder: qualification and punishment under Russian law. M: Jurist, 1994. p 93.

4. Kochoi SM. Criminal law. General and Special parts: Textbook. Short course. M.: "CONTRACT", 2009. p.78.

5. Naumov AV. Russian criminal law. A common part. Lecture course. M.: BEK, 1996. S. 509.

6. Koni AF. On the right of necessary defense. M.: Ostozhie, 1996. p.73.

7. Pertsev DV. Criminal-legal and criminological problems of necessary defense: monograph. Kaliningrad: Publishing house of the Rgu im kant. Immanuel Kant Russian State University. 2009. p.102.