ISSN: 2053-3578 I.F. 12.34

# IMPROVING CRIMINAL LIABILITY FOR FRAUD COMMITTED USING INFORMATION TECHNOLOGIES

**Sharapov Bakhtiyor Mukhtarhanovich**
independent researcher at the Ministry of Foreign
Affairs of the Republic of Uzbekistan

**Abstract**: This article examines the modern manifestations of fraud crimes committed using information technologies, their social dangerousness, and the issues of improving criminal liability for this type of offense are analyzed. With the development of the digital economy and electronic services, the number of crimes such as cyber fraud, phishing, fraud through online payment systems, and illegal appropriation of funds via social networks is increasing. The article highlights certain shortcomings in the current legislation and proposes recommendations for improving criminal-legal norms based on foreign experience

**Keywords**: information technology, fraud, cybercrime, criminal liability, electronic payment, phishing, legislation, digital security. Introduction

Today, digital transformation processes have not only driven economic growth but have also ensured the “evolution” of crime. In Uzbekistan, the dynamics of cybercrime have sharply increased over the last three years, with information technology accounting for more than 40-50% of all fraud.

Unlike traditional fraud, digital fraud is characterized by remoteness, anonymity, and cross-border nature. This, in turn, necessitates a review of existing criminal law provisions and the introduction of new approaches to judicial and investigative practices.

Moreover, in recent years, digitization processes have accelerated dramatically worldwide. A large portion of government services, the banking system, commerce, education, and daily communication processes are now conducted via the internet and information technologies. While this has made society's life easier, it has also led to an increase in a new type of crime, particularly fraud committed using information technologies.

While in traditional fraud the offender gains a financial benefit by directly deceiving or abusing trust, in digital fraud this process involves the internet, mobile communication, electronic payment systems, fake websites, messengers, and social networks. Many citizens are facing situations such as losing bank card information, investing in fraudulent investment schemes, and being deceived by false advertisements.

This situation requires the introduction of new mechanisms in criminal law and the improvement of specific liability measures for fraud committed using information technologies.

**Research Methodology**

In preparing this article, the methods of scientific analysis, comparative legal analysis, statistical observation, study of normative legal documents, and generalization were used. The provisions of national criminal legislation were compared with the practices of foreign states. Additionally, the practical manifestations of modern cyber fraud methods were analyzed.

**Results**

The main forms of fraud committed through information technologiesCurrently, the following forms of fraud are widespread:

1. Phishing

Criminals send fake messages from a bank, government agency, or a well-known company to obtain a citizen's login, password, or card information.

2. Fake online shoppingLow-priced products are advertised online, and a down payment is taken, but the product is never delivered.

3. Investment and Crypto Scams

Money is collected from citizens through platforms that promise artificial income, and the funds are later embezzled.4. Social Media Fraud

On platforms like Telegram, Instagram, and Facebook, scams occur through dating, offers of help, grants, or job offers.

5. SIM Swapping and OTP Code Fraud

Scammers take control of a person's bank account by obtaining their one-time verification code. Analysis of these methods shows that 3Scammers take control of a citizen's bank account by obtaining their one-time verification code.

An analysis of these methods shows that the number of cybercrimes in 2023 increased by nearly 1.5 times compared to the previous year:1. Issues with Current Legislation and Qualification

Article 168, Part 3(g) of the Criminal Code of the Republic of Uzbekistan establishes liability for fraud committed using information technologies. However, the following problems are observed in practice:

· The problem of demarcation: Withdrawing money from a person's bank card without their knowledge (using a code) is sometimes classified as theft (Article 169) and sometimes as fraud (Article 168).

· The issue of intermediaries: There is no uniform approach to legally assessing the actions of individuals who have provided their plastic cards to fraudsters in exchange for a fee ("money mules").

**Some problems in the current legislation**

Analysis shows that while many countries have a general framework for fraud, the specific aspects of fraud committed through information technology are not fully reflected.Key problems:

· digital methods of commission are not specifically addressed;

· transnational crimes are difficult to investigate;· The mechanism for collecting electronic evidence is insufficient;

· Identifying the perpetrator is complicated due to anonymity and VPN technologies;

· Many victims do not report;

· There are problems in determining the amount of damage.Statistics (Trends)

According to the Ministry of Internal Affairs, the number of cybercrimes in 2023 increased by nearly 1.5 times compared to the previous year.

The most common method is obtaining bank card information through a fake link, in which over 70% of victims voluntarily (under deception) provided their confidential code.

**Discussion**

We consider the following directions for improving criminal liability:

1. Introducing a separate qualifying featureThe crime of fraud should be designated as an aggravating circumstance when committed using information technologies.

Substantive Law Proposals

· Differentiate the concept of "cyber-fraud": In Article 168 of the Criminal Code, the penalty for this form of fraud should be enhanced as a qualifying circumstance rather than as a separate offense (e.g., regardless of the amount of damage).

· Liability of intermediaries:

It would be appropriate to introduce a new article (for example, Article 168-1) into the Criminal Code to address the unlawful acquisition of another person's bank card or other identification instruments, or the presentation of one's own card for fraudulent purposes.

2. Development of a Special Provision

It is advisable to codify the concept of cyber fraud or electronic fraud as a separate article in the criminal code.3. Strengthening the institution of electronic evidence

In judicial and investigative practice:

ISSN: 2053-3578 I.F. 12.34

· IP addresses,

· transaction history,

· electronic correspondence,

· server logs,

· digital footprints

must be effectively used as evidence.4. Strengthening International Cooperation

Many fraudsters commit crimes from the territory of another state. Therefore, it is necessary to strengthen the mechanisms of:

· extradition,

· rapid information exchange,

· transnational investigations.5. Differentiation of Punishment

Penalties should be increased in the following cases:

· when significant damage is caused;

· when committed by an organized group;

· when minors are involved;

· when the banking system is attacked;

· when it is a repeat offense.6. Legal codification of preventive measures

Banks, mobile operators, and platforms should be obligated to warn users, stop suspicious transactions, and take security measures.

**Processual-legal proposals**

· Transaction Freeze (24-Hour Rule): In the event of signs of fraud, grant investigators the authority to temporarily suspend bank transfers for up to 24 hours without a prosecutor's sanction (by amending the JPK).

· Classification of digital evidence: Expand the concept of “electronic data” in the JPK, strengthening the mechanism for recognizing IP addresses, blockchain transactions, and messenger conversations as original evidence.

Countries such as the USA, the UK, Germany, and Singapore apply strict penalties for cyber fraud. In some countries, the mere illegal acquisition of bank card data is also considered a crime.

Many countries operate special cybercrime units. These practices are important for improving national legislation. In conclusion, fraud committed using information technologies has become a serious threat to modern society. These crimes are dangerous due to their speed, secrecy, remoteness, and the large number of victims they affect.

ISSN: 2053-3578 I.F. 12.34

Therefore, the improvement of criminal liability must be carried out in the following areas:· introducing specific provisions for cybercrime;

· harshening and differentiating penalties;

· improving the handling of electronic evidence;

· expanding international cooperation;· strengthening preventive measures;

· increasing citizens' legal and digital literacy.

Strengthening not only punitive measures but also preventive mechanisms is a key factor in combating these types of crimes.

**References**

1. O‘zbekiston Respublikasi Jinoyat kodeksi.
2. Cybercrime Convention (Budapest Convention).
3. Smith J. Digital Fraud and Criminal Law. London, 2022.
4. Brown T. Cybersecurity and Financial Crimes. New York, 2021.
5. Interpol Annual Cybercrime Report. 2024.