Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

FINANCIAL FRAUD - CRIMES IN THE DIGITAL PAYMENT SYSTEM AND THE PROBLEMS OF THEIR QUALIFICATION

Abdumominov Ruslan Rustamjon oglu
2nd Year Student, Group 24.74
Faculty of Law, Jurisprudence Fergana, Uzbekistan

Abstract
This Article Analyzes the Characteristics of Financial Fraud Committed Through Electronic Payment Systems and Bank Cards in The Digital Economy. The Problems of Correct Legal Qualification of Acts Based on The Norms of The Criminal Code of The Republic of Uzbekistan, In Particular the Legal Boundary Between Digital Theft and Cyber-Fraud, As Well As Illegal Actions in P2P Transactions, Are Highlighted. Proposals Have Been Developed to Prevent Digital Financial Crimes and Improve Criminal Legal Mechanisms Based on International Experience.

Keywords: Financial Fraud, Digital Payments, Bank Cards, Legal Qualification, Cybercrime, P2P Transfers, Theft.

Introduction

The Rapid Development of the Digital Economy in The Republic of Uzbekistan, In Particular, The Increase in The Share of Cashless Payments and The Popularity of P2P (Person-To-Person) Transfers, Has Led to The Complete Migration of Traditional Financial Crimes to Cyberspace. Today, Instead of Physically Stealing the Victim's Wallet, Criminals Prefer to Obtain Their Bank Card Details (PAN And CVV Codes) And Secret OTP (One-Time Password) Confirmation Codes Received Via SMS Using Social Engineering, Vishing (Phone Fraud) Or Phishing (Fake Links). According To the Central Bank of The Republic of Uzbekistan, in 2025 The Volume of Illegal Transactions Carried Out Through Commercial Banks and Payment Organizations (Click, Payme, Etc.)

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

And Cases Of Cyber Fraud Have Significantly Increased Compared To Previous Years [1].

The Sharp Increase In Such Crimes Is Seriously Undermining Not Only Economic Stability, But Also Citizens' Confidence In The Banking System. For Law Enforcement Agencies And The Judiciary, The Correct Qualification Of These Acts Based On The Norms Of The Criminal Code Of The Republic Of Uzbekistan Is A Major Test. In Particular, Legal Uncertainties And Different Approaches In Practice Remain On The Issue Of Whether The Withdrawal Of Funds From A Bank Plastic Card Without The Victim's Will, But With His Participation (By Obtaining A Confirmation Code By Deception), Should Be Qualified Under Article 168 (Fraud) Or Article 169 (Theft) Of The Criminal Code. The Purpose Of This Study Is To Analyze The Differences In The Legal Qualification Of Crimes Committed In Digital Payment Systems, Identify Gaps In The Current Legislation, And Develop Proposals To Improve Criminal Sanctions Against Financial Cybercrimes.

Level Of Research On The Topic (Literature Analysis)

The Transformation Of Property Crimes In The Digital Economy Is Being Actively Studied By National And Foreign Lawyers. In The National Legal Literature, Financial Crimes In Cyberspace Are Mainly Studied As A New Objective Aspect Of Traditional Property Crimes, And The Issues Of Unauthorized Access To Information Systems And Misappropriation Of Property Are Widely Discussed [2]. At The Same Time, Practicing Lawyers And Investigators Note That They Face Serious Problems In Defining The Boundary Between “Electronic Theft” And “Cyber Fraud”. In Particular, Despite The Explanations Of The Plenum Of The Supreme Court, If The Criminal Physically Steals The Victim’s Phone, Enters The Click Or Payme Application And Transfers Money (Theft), But Withdraws The Same Money By Calling The Victim, Introducing Himself As An Employee Of The “Bank Security Service” And Receiving An SMS Code (Fraud), The Level Of Social Danger In These Two Cases Is The Same, But The Different Application Of Sanctions Is Criticized [3].

Foreign Experience, Including The Provisions Of The European Union’s PSD2 (Payment Services Directive), Establishes That If A Client’s Money Is Stolen As

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

A Result Of Banks' Failure To Comply With Strong Authentication (SCA) Requirements, The Financial Institution Itself Is Directly Liable [4]. In Uzbekistan, The Problem Of Indifference To Security Requirements Of P2P Platforms And The Lack Of Financial Literacy Of Users Has Not Found A Complete And Strict Legal Solution In Criminal Law. This Situation Requires Further Deepening Of The Criminal-Legal Analysis Of Digital Financial Crimes.

The Article Was Prepared Using The Methods Of Systematic-Structural Analysis, Comparative Jurisprudence And Case Study. The Schemes Of Digital Financial Crimes In Uzbekistan Were Analyzed In Comparison With The Norms Of Traditional Criminal Law.

Main Part

The Most Dangerous Type Of Financial Cybercrime Today Is Not Random Fraud, But Organized And Technologically Well-Planned "Cascading Theft". One Of The Unprecedented Cases Observed In Real Practice Is When A Large Amount Of Credit Funds (For Example, 100 Million Soums Or More) Is Allocated To Citizens By The Bank And Credited To The Client's Plastic Card, And These Funds Are Immediately Withdrawn By Hackers.

This Criminal Scheme Is Often Committed Not As An External Attack, But As A Direct Result Of A Breach Of The Integrity Of The Bank's Internal Security System, That Is, As A Result Of Collusion Between Bank Employees (Insiders) And Criminal Groups. After Confidential Information About The Client Is Transferred To Hackers, The Client's Device Receives Continuous Confirmation Codes (SMS-Bombing), And The Funds Are Transferred To The Accounts Of Dozens Of Third Parties (Droppers) Within A Few Seconds. At The Final Stage, The Money Is Converted Into Foreign Electronic Wallets And Cryptocurrencies (Bitcoin, USDT), And Their Legal Trace Is Lost. One Of The Biggest Legal Gaps In The Current Criminal Code Is The Lack Of A Mechanism For Holding A Financial Institution That Does Not Provide Direct Security In Such Cases, Or Its Management, To Corporate Criminal Liability As A Legal Entity.

Another Popular Method Of Financial Fraud Is The Synthesis Of Information Technology And Social Engineering. Recently, There Has Been A Surge In The Use Of Phishing, Where Citizens Are Called Via IP Telephony (Codes Such As

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

"78") And Introduced As Employees Of A Payment System (Click, Payme) Or A Bank Security Service. Criminals Have Become So Sophisticated That In Some Cases There Is A Risk Of Bypassing Biometric Security Systems By Simply Answering The Call And Recording Their Voice (Voice Synthesis Using Deepfake Technologies).

Also, When Malicious APK Files (Trojans) Sent On Behalf Of Government Agencies (For Example, The Tax Office Or Social Security Agency) Via Telegram And Other Messengers Are Installed On Citizens' Devices, Hackers Gain Complete Remote Control Over All Banking Applications And SMS Notifications.

The Criminal-Legal Qualification Of The Above Actions Is Causing Serious Controversy In Practice. If The Victim Is Deceived And Voluntarily Transfers His Money To The Criminal, This Is Clearly Qualified Under Article 168 (Fraud). However, If Money Is Withdrawn Without His Consent By Dropping A Malicious APK File On The Victim's Device, This Practice Is Often Qualified Under Article 169 (Theft), Part 3, Subparagraph "B" (Unauthorized Access To An Information System) [5]. However, The Fact That The Crime Begins With Fraud (Deceiving The Victim Into Clicking On A Link) And Ends With Theft (Secretly Withdrawing Money) Creates A Competition Between These Two Norms. Most Foreign Countries Have A Special Norm Called "Fraud In The Field Of Computer Information" For Such Complex Digital Crimes [6], And There Is A Need To Introduce Such A Specific Specialized Article In Our National Legislation.

Conclusion

The Results Of The Study And The Analysis Of The Real Practice Of Modern Digital Crimes Require The Introduction Of The Following Comprehensive Legal Solutions To Improve The Fight Against Financial Cyber-Fraud. First, In Order To Eliminate The Competition And Legal Uncertainty Between The Current Article 168 (Fraud) And Article 169 (Theft) In The Criminal Code Of The Republic Of Uzbekistan, It Is Necessary To Introduce A Special Norm "Fraud In The Field Of Computer Information And Digital Payments", Based On The Experience Of Developed Foreign Countries. This Will Serve To Accurately And Fairly Qualify Mixed Crimes Committed Through Social

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

Engineering (Vishing, Phishing) And Malicious Programs (APK-Trojans). Secondly, As The Most Pressing Problem, If A Hacker Attack Is Carried Out On Customer Accounts With The Help Of Insiders (Responsible Employees) Within The Banking System Or Due To The Failure Of The Financial Institution's Cybersecurity (Anti-Fraud) Systems To Function At The Required Level, It Is Necessary To Strictly Define In The Legislation The Mechanism For Holding The Bank Or Payment Organization Itself, As A Legal Entity, Liable For Material And Criminal Liability. Based On The Experience Of The European Union (PSD2 Directive), It Is Proposed To Introduce The Practice Of Recovering Losses Caused To The Customer Directly From The Payment Organization For Suspicious Transactions That Do Not Meet Security Requirements. Thirdly, When Transferring Large Amounts Of Funds (For Example, More Than 50 Times The Base Settlement Amount) In P2P Payment Systems And Mobile Banking Applications, Mandatory Biometric Authorization (Face ID) And An Automatic 24-Hour “Holding” (Freezing And Re-Verification) Procedure For Immediately Transferring Newly Received Loan Funds To Other Accounts, Not Limited To SMS (OTP) Codes, Will Lead To A Sharp Reduction In Cybercrime.

References

1. O’zbekiston Respublikasi Markaziy Bankining “Tijorat Banklari Va To’lov Tizimlarida Axborot Xavfsizligini Ta’minlash Holati To’g’risida”Gi Hisoboti // O’zbekiston Respublikasi Markaziy Banki Rasmiy Veb-Sayti. 2026-Yil, Fevral. Elektron Manba: Https://Cbu.Uz/Oz/ (Murojaat Qilingan Sana: 12.05.2026).
2. Fozilov F., Saidov A. Zamonaviy Moliyaviy Kiberjinoyatlarning Kriminologik Xususiyatlari // Huquqiy Tadqiqotlar Jurnali. – Toshkent, 2024. – № 7. – B. 88-92.
3. O’zbekiston Respublikasi Oliy Sudi Plenumining “Firibgarlikka Oid Ishlar Bo’yicha Sud Amaliyoti To’g’risida”Gi Qarori Tahlili Va Amaliy Muammolar // Odil Sudlov Jurnali. – 2025. – № 4. – B. 15-18.
4. Directive (EU) 2015/2366 On Payment Services In The Internal Market (PSD2). Official Journal Of The European Union. Elektron Manba:

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 6, June, 2026
Website: usajournals.org

Https://Eur-Lex.Europa.Eu/Legal-Content/EN/TXT/?Uri=CELEX:32015L2366 (Murojaat Qilingan Sana: 12.05.2026).

5. O'zbekiston Respublikasi Oliy Sudi Plenumining "O'g'rilik, Talonchilik Va Bosqinchilik To'g'risidagi Ishlar Bo'yicha Sud Amaliyoti Haqida"Gi Qarori (Yangi Qo'shimchalar Bilan) // Qonunchilik Ma'lumotlari Milliy Bazasi. Elektron Manba: Https://Lex.Uz/Docs/1449622
6. Cyber-Fraud And Theft In The Digital Age: A Comparative Analysis Of Criminal Law Responses // International Journal Of Law And Information Technology. – Oxford University Press, 2025. – Vol. 33, Issue 1. – P. 112-118.
7. O'zbekiston Respublikasining Jinoyat Kodeksi // Qonunchilik Ma'lumotlari Milliy Bazasi, 01.01.2024-Y., 03/24/891/0001-Son. Elektron Manba: Www.Lex.Uz
8. O'zbekiston Respublikasi Oliy Sudi Plenumining "O'g'rilik, Talonchilik Va Bosqinchilik To'g'risidagi Ishlar Bo'yicha Sud Amaliyoti Haqida"Gi 1999-Yil 2-Sentyabrdagi 14-Sonli Qarori // Qonunchilik Ma'lumotlari Milliy Bazasi. Elektron Manba: Https://Lex.Uz/Docs/1449622
9. O'zbekiston Respublikasi Oliy Sudi Plenumining "Firibgarlikka Oid Ishlar Bo'yicha Sud Amaliyoti To'g'risida"Gi 2017-Yil 11-Oktyabrdagi 35-Sonli Qarori // Qonunchilik Ma'lumotlari Milliy Bazasi. Elektron Manba: Https://Lex.Uz/Docs/3394851