YANGI O‘ZBEKISTON, YANGI TADQIQOTLAR JURNALI
Volume 5 Issue 7 Noyabr 2026
https://phoenixpublication.net/ Online ISSN: 3030-3494

LAUNDERING CYBERCRIME PROCEEDS THROUGH VIRTUAL AND CRYPTO ASSETS (CYBER-LAUNDERING): TYPOLOGIES AND PREVENTION MECHANISMS

Rukhshona Uralova
Masters student, TSUL, Tashkent, Uzbekistan
ruxshonaoralova71@gmail.com

Annotation. *This article examines how proceeds of cybercrime are laundered through virtual and crypto assets. Drawing on FATF and EAG typologies, comparative case law and Uzbek legislation, it studies the general structure of cybercrimes in remote banking, and how crypto and e-money may facilitate the cyber-laundering. Based on the analysis, the paper provides policy suggestions to strengthen the legal framework.*

Keywords: *cybercrimes, cybersecurity, cyber-laundering, remote banking, crypto and virtual assets*

1. Introduction

Due to the advancement of the digital innovation, cybercrimes have become a growing transnational offence. [34] Current paper examines laundering of illicit funds obtained through cybercrimes committed against the banking sector which is becoming increasingly attractive to cyber criminals given its high dependence on digital devices and the Internet. Most widespread information and computer technology-related crimes in finance include unauthorized debiting (removal) of funds from bank accounts, payment card fraud, interference with online banking systems, distribution of computer viruses and information network fraud. [35] According to experts, global losses inflicted by cybercrime exceed USD 100 billion yearly. [36] Several characeristics of cybercrimes such as its high-speed and low-cost, complex and anonymous nature have posed concerning threat to the financial sector. [37]

[34] FATF, *Illicit Financial Flows from Cyber-Enabled Fraud* (FATF 2023) 3 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf accessed 6 November 2026.
[35] Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), *Cybercrime and Money Laundering* (EAG Typology Report 2014) page 4 https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf accessed 6 November 2026.
[36] ibid, page 6.
[37] International Monetary Fund, ‘Cyber Risk: A Growing Concern for Macrofinancial Stability’ in *Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks* (IMF April 2024) ch 3 https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/ch3.pdf accessed 6 November 2026.

To conceal the origins of the ill-gotten funds the criminals, in turn, use varios money-laundering techniques. As reflected in the practice of European Union’s 6th Anti-Money Laundering Directive, cybercrime is documented among 22 common predicate crimes for money laundering. [38] Online gambling platforms, crypto currency or other virtual assets have been commonly exploited by the criminals to introduce the illicit funds as “clean” earnings into the economy. [39] This article examines the typologies of the cybercrimes committed against the remote banking sector and laundering the illict gains through mainly virtual and crypto assets, based on which prevention mechanisms are suggested.

2. Methodology

The study uses a qualitative, multi-method design. First, the doctrinal analysis was applied to review the FATF (2019; 2023) and EAG (2014) reports to examine the typologies used to launder cybercrime proceeds, as well as the applied laws and regulations and scholarly works are discussed. Secondly, the paper includes jurisdictional comparison and examination of illustrative cases reviewed in the sphere. Besides, relevant quantitative statistical data and indicators are used to analyze the theme in question thoroughly.

3. Results and analysis

I. Description of common distant banking cybercrimes

While online banking is the multipurpose software and hardware system that allows clients to instruct a bank to execute certain money transfers, monitor their accounts and receive various financial updates without physically visiting a bank, cybercriminals also intend to target its remote fund transfer functions.

Typically, malware infection of technologies used for online banking usually occur as a result of spamming, visiting fake websites or using hacked data storage devices, where viruses are downloaded into a victim’s devices unnoticeably. [40] According to the report, the virus may do basic monitoring, collect the transaction information and victim’s bank credentials, and send it to the fraudster’s computer. [41] Later the virus may steal RBS access passcodes, digital signature keys and read wire transfer payment details. Malware virus that seizes confidential information when data is copied in a buffer or remote money transaction windows are opened on computer display may also infect the client’s device. [42]

[38] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law [2018] OJ L284/22, art 2(1)(v); ComplyAdvantage, ‘The 6th Money Laundering Directive (6AMLD)’ (*ComplyAdvantage Insights*) https://complyadvantage.com/insights/6th-money-laundering-directive-6amld/ accessed 6 November 2026.
[39] ComplyAdvantage (n 5).
[40] EAG (n 2) page 15.
[41] ibid, page 16.
[42] ibid.

Primary method of the fraudsters is to obtain the information, generate and perform money transactions, through online banking platforms, that seem typical for the current customer's regular transactional activities, and transfer funds to the account of a front man or shelf company. The criminals aim to create a usual pattern of transaction types and purposes to avoid the obvious fraud identification in the bank account analysis. Gaining the stolen funds, they tend to cash out through ATMs to avoid live contact with bank officers.

One of the case precedents reviewed in the practice of Ukraine, the law enforcement agency investigated the unauthorized transfer of 250 thousand USD in the "Customer- Bank" system of the government-owned company C to the account of four other companies opened in different banks. The case was launched under Article 361(2) (Unauthorized Interference with Operation of Computers, Computer-Aided Management Systems, Computer Networks or Telecommunication Networks) of the Ukrainian Criminal Code. During the investigation, it was revealed that the "Customer- Bank" system of the company was infected with malware, where the criminal used the stolen digital signatures of managers to remotely send the fake payment instructions on behalf of the company. In cooperation with the Ukrainian FIU, the bank accounts of the above-mentioned entities are blocked, and the investigations are ongoing. [43]

In the practice of Tajikistan, unidentified individuals hacked the security system of the remittance office of the bank and stole USD 130 200 by transferring them to the accounts of several foreign nationals. The criminal investigation was initiated under Article 289 (1) (Unauthorized Access to Computer Data) and Article 244 (4) (Theft) of the Tajik Criminal Code.[44]

Notably, it is acknowledged that at the edge of Russian invasion of Ukraine since February 2022, the number of cyberattacks has surged significantly, followed by the same trend after the Middle east conflicts, whose reasons remain uncertain. [45]

II. Cyber-laundering schemes

While traditional money laundering heavily relies on the conventional banking system, cyber-laundering tends to exploit advanced transactional and financial service providers, such as e-money transactions to "money-mules", virtual assets and crypto currency sale-purchase. [46] However, in both category of laundering, the conversion of funds into cash in the last stage

[43] EAG (n 2) page 22.
[44] ibid.
[45] IMF (n 4).
[46] EAG, *Legalization (Laundering) of the Proceeds of Cybercrime, as well as Financing of Terrorism from the Said Offence, Including through the Use of Electronic Money or Virtual Assets and the Infrastructure of their Providers* (EAG Typology Report, WGTYP (2022) 12 rev 1, 2022) <https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_eng.pdf> accessed 6 November 2026.

is common through ATMs since it enables the criminals to avoid face-to-face contact with bank employees as well as tracking the cash operations beyond the bank system becomes almost impossible. [47]

In the transnational cyber-laundering case of “QQAAZZ network”, the group of Russian-speaking cybercriminals from 16 countries gather to offer/seek for specific skills and services to obtain the funds illicitly through cyber-attacks and launder them. [48] The network possessed hundreds of bank accounts in several jurisdictions and shell companies, through which the funds could be transferred/ withdrawn or converted into crypto currency to extinguish their original source. Taking up to 50% of the stolen funds, the QQAAZZ returned the “clean” money to the original owner.

Analysis of the common cyber-laundering techniques by FATF summarizes what type of initial layering accounts are applied depending on the specific cybercrime as provided below.

Type of CEF	**Type of first layer account**
BEC fraud	Corporate (e.g., shell or newly registered companies)
Phishing fraud	Individual money mules
Social media telecommunication impersonation fraud	Individual money mules
Online trading/ trading platform fraud	Corporate (e.g., shell or newly registered companies)
Online romance fraud	Individual money mules
Employment scams	Individual money mules

Table 1: Relationship of common cybercrimes and first layer account. [49]

Beyond such professional networks, two channels are currently dominating in cyber-laundering: electronic money and virtual assets. As regards e-money, stolen funds are rarely moved directly to the offender. Instead, they are split across e-wallets, prepaid and virtual cards opened in the names of nominees, the so-called “drops” or money mules. The EAG’s 2022 typology study lists the typical indicators: instruments owned by nominees, significant turnover within around 24 hours, several accounts linked to one person, cards with short validity and systematic cash withdrawals.[50] E-wallets and bank cards are also used as a bridge

[47] EAG (n 2).
[48] FATF (n 1) 16.
[49] ibid 20.
[50] EAG (n 12) 14–15.

to buy cryptocurrency from informal exchangers, and investigators often cannot establish which exchanger passed the funds.[51] E-money, thus, links the banking system with the crypto-asset ecosystem.

The scale of mule-based laundering is illustrated by the ninth European Money Mule Action (EMMA 9). [52] According to Europol, in operational phases conducted between June and November 2023, law enforcement agencies from 26 countries, supported by Europol, Eurojust, INTERPOL and 2 822 banks and financial institutions, identified 10 759 money mules and 474 recruiters and arrested 1 013 individuals.[53] According to Europol, the funds originated from online fraud schemes such as phishing, investment scams and business e-mail compromise, and the operation also revealed crypto-assets being transferred from virtual currency exchanges to e-wallets controlled by mules.[54]

Turning to the judicial practices, a Dutch court sentenced Tornado Cash developer Alexey Pertsev to 64 months' imprisonment for laundering about USD 1.2 billion,[55] whereas in the United States the Fifth Circuit held in Van Loon that immutable smart contracts are not sanctionable "property",[56] and a jury in Storm convicted the co-founder only of conspiring to operate an unlicensed money transmitting business.[57] Notably, this uncertainty in liability may cause regulatory arbitrage.

4. Discussion

Uzbekistan has built a comprehensive framework in fight against cyber-laundering. Article 243 of the Criminal Code criminalizes the legalization of criminal proceeds, Chapter XX¹ (Articles 278¹–278⁷) covers cyber offences, and Law No. 899 of 2024 added Articles 278⁸–278⁹ on illegal crypto-asset turnover and mining.[58] Under Law No. 660-II and Regulation No. 2886, as amended in 2026, banks must scrutinize app-based transfers to cards or e-wallets reaching 500 base calculation units (BCU) within 30 days and transmit full payer

[51] ibid 13, 15–16.
[52] ZIGRAM, 'European Money Mule Action (EMMA 9)' (*ZIGRAM*, 27 December 2023) https://www.zigram.tech/resources/european-money-mule-action-emma-9/ accessed 8 November 2026.
[53] Europol, "Paper Trail Ends in Jail Time for 1 013 Money Mules" (Press release, 4 December 2023) https://www.ebf.eu/ebf-media-centre/paper-trail-ends-in-jail-time-for-1-013-money-mules-2-822-banks-and-financial-institutions-join-forces-with-law-enforcement-agencies-in-global-effort-against-money-laundering/ accessed 6 November 2026.
[54] ibid.
[55] Rechtbank Oost-Brabant 14 May 2024, ECLI:NL:RBOBR:2024:2069 (*Pertsev*).
[56] *Van Loon v Department of the Treasury* 122 F 4th 549 (5th Cir 2024).
[57] *United States v Storm* No 23 Cr 430 (KPF) (SDNY, jury verdict 6 August 2025); "Tornado Cash Cofounder Convicted of Conspiring to Operate an Unlicensed Money Transmitting Business" (*Willkie Compliance Concourse*, 8 August 2025) https://complianceconcourse.willkie.com/articles/tornado-cash-cofounder-convicted-for-conspiring-to-operate-an-unlicensed-money-transmitting-business/ accessed 6 November 2026.
[58] Criminal Code of the Republic of Uzbekistan 1994, arts 243, 278¹–278⁹; Law of the Republic of Uzbekistan No. 899 "On Amendments and Additions to the Criminal Code, the Code of Criminal Procedure and the Code of Administrative Responsibility" of 19 January 2024.

and payee data for domestic transfers above 25 BCU.[59] Only the Central Bank and commercial banks may issue e-money,[60] residents may trade crypto-assets only through providers licensed by the National Agency of Perspective Projects (NAPP),[61] the Cybersecurity Law treats banking as critical infrastructure,[62] and Resolution No. 153 of 2025 announced liability for persons who let their cards, accounts, SIM cards or e-wallets be used in cybercrime, together with a centralized anti-fraud system.[63]

The need is pressing since in 2025 information technologies were used in 82% of frauds and 76% of thefts, causing over UZS 2 trillion in damage,[64] yet the EAG's 2022 mutual evaluation rated the effectiveness of money-laundering prosecution (IO.7) and confiscation (IO.8) as only moderate.[65] The following four points illustrate the issue.

Firstly, crypto-asset regulation rests largely on presidential acts and NAPP regulations rather than a statute,[66] and enforcement targets licensing breaches rather than proceeds. The first case, heard on 14 May 2024, punished 125 unlicensed transactions through Binance with five days' administrative arrest,[67] and later prosecutions under Article 278[8] likewise targeted individual traders.[68] Such cases punish the secondary crime without deeply investigating whether the funds derived from cybercrime, while peer-to-peer and foreign-platform transfers

[59] Rules of Internal Control for Combating the Legalisation of Proceeds from Criminal Activity, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction in Commercial Banks (registered by the Ministry of Justice No 2886, 23 May 2017, as amended by No 2886-12, 8 May 2026); "Uzbekistan to Tighten Control over Bank Transfers and Card Transactions" (*Yep.uz*, May 2026) https://yep.uz/en/2026/05/uzbekistan-tightens-control-bank-transfers-card-transactions/ accessed 6 November 2026.

[60] Law of the Republic of Uzbekistan No. 578 "On Payments and Payment Systems" of 1 November 2019; Rules on the Issuance and Circulation of Electronic Money in the Republic of Uzbekistan (registered by the Ministry of Justice No 3231, 29 April 2020).

[61] Decree of the President of the Republic of Uzbekistan No UP-121 of 27 April 2022; National Agency of Perspective Projects, "Attention of Citizens of the Republic of Uzbekistan" https://napp.uz/en/news/o-zbekiston-respublikasi-fuqarolari-diqqatiga accessed 6 November 2026.

[62] Law of the Republic of Uzbekistan No. 764"On Cybersecurity" of 15 April 2022.

[63] Resolution of the President of the Republic of Uzbekistan No. 153 "On Measures to Further Strengthen the Fight against Crimes Committed Using Information Technologies" of 30 April 2025; "Uzbekistan Strengthens Measures to Combat Cybercrime" (*UzDaily*, 6 May 2025) https://www.uzdaily.ru/en/uzbekistan-strengthens-measures-to-combat-cybercrime accessed 6 November 2026.

[64] "Government Proposes Tougher Measures against Cybercrime and Financial Pyramids" (*Kun.uz*, 12 March 2026) https://kun.uz/en/news/2026/03/12/government-proposes-tougher-measures-against-cybercrime-and-financial-pyramids accessed 6 November 2026.

[65] EAG, *Mutual Evaluation Report of the Republic of Uzbekistan* (EAG 2022) https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-uzbekistan-2022.html accessed 6 November 2026.

[66] Decree No UP-121 (n 31).

[67] Bakhtiyor Primov, 'Problems of Qualification of Criminal Offenses in the Sphere of Crypto-Assets Turnover and Mining' (2026) 4(5) Uzbek Journal of Law and Digital Policy 260 https://doi.org/10.59022/IRSHAD-ujldp.14.

[68] '17-Year-Old Arrested in Bukhara for Illegal Crypto Trading Worth $2.6 Million' (*Kun.uz*, 13 December 2024) https://kun.uz/en/news/2024/12/13/17-year-old-arrested-in-bukhara-for-illegal-crypto-trading-worth-26-million accessed 6 November 2026.

largely escape banks' controls,[69] so both predicate offences and laundering are rarely prosecuted simultaneously under Article 243.

Secondly, drops can currently be prosecuted only as accomplices, which requires proof of intent. The regulation project criminalizing the transfer of bank cards, e-wallets and crypto-wallets to third parties and allowing the temporary suspension of suspicious transactions was sent to the Senate in July 2026,[70] but it does not appear to stipulate the criteria to differentiate knowing contributors from deceived victims.

Thirdly, the fixed 500 BCU threshold (roughly UZS 206 million)[71] is easily evaded by droppers that split proceeds into small "smurfed" payments,[72] so rule-based monitoring must be complemented by risk-based monitoring.

Lastly, international cooperation seems weaknesses since proceeds leave the jurisdiction within hours, yet Uzbekistan is not a party to the Budapest Convention. The UN Convention against Cybercrime, opened for signature in Hanoi on 25 October 2025, offers a new basis for cross-border evidence preservation and freezing,[73] without such channels, domestic suspension powers cannot reach assets already moved abroad or into decentralized protocols.

5. Conclusion

Laundering the proceeds of cyber-attacks on banks is now the final stage of the attack itself. Once a criminal group gets into a bank's systems or customer accounts, the stolen funds move within hours through mules, e-wallets, stablecoins and decentralized protocols that are beyond the reach of traditional AML gatekeepers. Therefore, tracing and freezing these proceeds quickly have become a cyber-security task. While Uzbek regulatory framework is quite comprehensive in fight against cyber-crimes, legislation in preventing cyber-laundering has presented some weaknesses.

To strengthen the regulatory framework, four measures are recommended. First, a comprehensive law on crypto-assets and virtual assets should recognise them as property for the purposes of Article 243 and confiscation, and should strictly apply sender/receiver identification. In parallel, the bill on drops should punish mules who knowingly or recklessly lend their accounts and wallets, while protecting victims who were deceived. Second, BCU

[69] EAG (n 12) 10.
[70] 'Uzbekistan to Introduce Legal Accountability for Citizens Facilitating Cybercrime' (*Kun.uz*, 29 April 2026) https://kun.uz/en/news/2026/04/29/uzbekistan-to-introduce-legal-accountability-for-citizens-facilitating-cybercrime accessed 6 November 2026; 'Uzbek Cybersecurity Bill Strengthens Payment Protection' (*UzDaily*, 22 July 2026) https://www.uzdaily.uz/en/uzbek-cybersecurity-bill-strengthens-payment-protection/ accessed 6 November 2026.
[71] Rules of Internal Control (n 29).
[72] EAG (n 12) 17.
[73] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (adopted 24 December 2024, opened for signature 25 October 2025) UNGA Res 79/243.

thresholds should be supplemented by risk-based monitoring in the Central Bank’s anti-fraud system. That system should be linked in real time to NAPP-licensed providers and supported by blockchain analytics in the financial intelligence unit. Third, a judicially supervised rapid-freezing mechanism should cover bank accounts, e-wallets and crypto-wallets alike, as part of cyber-incident response. Fourth, specialised cyber-crime units should run a parallel financial investigation, including on-chain tracing, in every cyber-fraud case. This work should be supported by ratifying the UN Convention against Cybercrime and by joining EMMA-style public–private operations. Thus, development of legislation in both cybersecurity and anti-money laundering would contribute effective Uzbek legal regime in the sphere.

BIBLIOGRAPHY

Primary sources

Cases

Pertsev, Rechtbank Oost-Brabant 14 May 2024, ECLI:NL:RBOBR:2024:2069

United States v Storm No.23 Cr 430 (KPF) (SDNY, jury verdict 6 August 2025)

Van Loon v Department of the Treasury 122 F 4th 549 (5th Cir 2024)

Legislation and international instruments

Criminal Code of the Republic of Uzbekistan 1994

Decree of the President of the Republic of Uzbekistan No. 121 of 27 April 2022

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law [2018] OJ L284/22

Law of the Republic of Uzbekistan No. 660-II “On Combating the Legalisation of Proceeds from Criminal Activity, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction” of 26 August 2004

Law of the Republic of Uzbekistan No. 578 “On Payments and Payment Systems” of 1 November 2019

Law of the Republic of Uzbekistan No. 764 “On Cybersecurity” of 15 April 2022

Law of the Republic of Uzbekistan No. 899 “On Amendments and Additions to the Criminal Code, the Code of Criminal Procedure and the Code of Administrative Responsibility” of 19 January 2024

Resolution of the President of the Republic of Uzbekistan No. 153 “On Measures to Further Strengthen the Fight against Crimes Committed Using Information Technologies” of 30 April 2025

Rules on the Issuance and Circulation of Electronic Money in the Republic of Uzbekistan (registered by the Ministry of Justice No 3231, 29 April 2020)

Rules of Internal Control for Combating the Legalisation of Proceeds from Criminal Activity, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction in Commercial Banks (registered by the Ministry of Justice No 2886, 23 May 2017, as amended by No. 2886-12, 8 May 2026)

United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (adopted 24 December 2024, opened for signature 25 October 2025) UNGA Res 79/243

Secondary sources

“17-Year-Old Arrested in Bukhara for Illegal Crypto Trading Worth $2.6 Million” (Kun.uz, 13 December 2024) https://kun.uz/en/news/2024/12/13/17-year-old-arrested-in-bukhara-for-illegal-crypto-trading-worth-26-million accessed 6 November 2026

“By bit Hackers Move over Half the Stolen ETH onto Bitcoin, Largely Using Thor Chain” (The Block, 27 February 2025) https://www.theblock.co/post/343855/bybit-hackers-half-the-stolen-eth-bitcoin-fbi-confirms-lazarus accessed 6 November 2026

Bakhtiyor Primov, “Problems of Qualification of Criminal Offenses in the Sphere of Crypto-Assets Turnover and Mining” (2026) 4(5) Uzbek Journal of Law and Digital Policy 260 https://doi.org/10.59022/IRSHAD-ujldp.14

Chainalysis, The 2026 Crypto Crime Report (Chainalysis 2026)

ComplyAdvantage, “The 6th Money Laundering Directive (6AMLD)” (Comply Advantage Insights) https://complyadvantage.com/insights/6th-money-laundering-directive-6amld/ accessed 6 November 2026

“Crypto Crime Topped $150 Billion in 2025 as State-Backed Actors Scaled On chain: Chain alysis” (The Block, 8 January 2026) https://www.theblock.co/post/384753/crypto-crime-150-billion-usd-2025-state-actors-scale-onchain-chainalysis accessed 6 November 2026

Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), Cybercrime and Money Laundering (EAG Typology Report 2014) https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf accessed 6 November 2026

Legalization (Laundering) of the Proceeds of Cybercrime, as well as Financing of Terrorism from the Said Offence, Including through the Use of Electronic Money or Virtual Assets and the Infrastructure of their Providers (EAG Typology Report, WGTYP (2022) 12 rev 1, 2022) https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_eng.pdf accessed 6 November 2026

Mutual Evaluation Report of the Republic of Uzbekistan (EAG 2022) https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-uzbekistan-2022.html accessed 6 November 2026

Europol, “Paper Trail Ends in Jail Time for 1 013 Money Mules” (Press release, 4 December 2023) https://www.ebf.eu/ebf-media-centre/paper-trail-ends-in-jail-time-for-1-013-money-mules-2-822-banks-and-financial-institutions-join-forces-with-law-enforcement-agencies-in-global-effort-against-money-laundering/ accessed 6 November 2026

FATF, Illicit Financial Flows from Cyber-Enabled Fraud (FATF 2023) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf accessed 6 November 2026

Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (FATF June 2025) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html accessed 6 November 2026

Federal Bureau of Investigation, “North Korea Responsible for $1.5 Billion Bybit Hack” (Public Service Announcement I-022625-PSA, 26 February 2025) https://www.ic3.gov/PSA/2025/PSA250226 accessed 6 November 2026

“Government Proposes Tougher Measures against Cybercrime and Financial Pyramids” (Kun.uz, 12 March 2026) https://kun.uz/en/news/2026/03/12/government-proposes-tougher-measures-against-cybercrime-and-financial-pyramids accessed 6 November 2026

Gulomov S, “Analysis of the Legal Foundations of Crimes in the Sphere of Crypto-Asset Turnover” (2025) Special Issue 03 Society and Innovations 499

International Monetary Fund, “Cyber Risk: A Growing Concern for Macro financial Stability” in Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks (IMF April 2024) https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/ch3.pdf accessed 6 November 2026

National Agency of Perspective Projects, “Attention of Citizens of the Republic of Uzbekistan” https://napp.uz/en/news/o-zbekiston-respublikasi-fuqarolari-diqqatiga accessed 6 November 2026

Rubenfeld S, “Cryptocurrency Money Laundering Reached $82 Billion in 2025, Chainalysis Says” (MLex, 27 January 2026) https://www.mlex.com/mlex/articles/2434866 accessed 6 November 2026

“Tornado Cash Cofounder Convicted of Conspiring to Operate an Unlicensed Money Transmitting Business” (Willkie Compliance Concourse, 8 August 2025) https://complianceconcourse.willkie.com/articles/tornado-cash-cofounder-convicted-for-

conspiring-to-operate-an-unlicensed-money-transmitting-business/ accessed 6 November 2026

“Uzbek Cybersecurity Bill Strengthens Payment Protection” (UzDaily, 22 July 2026) https://www.uzdaily.uz/en/uzbek-cybersecurity-bill-strengthens-payment-protection/ accessed 6 November 2026

“Uzbekistan Strengthens Measures to Combat Cybercrime” (UzDaily, 6 May 2025) https://www.uzdaily.ru/en/uzbekistan-strengthens-measures-to-combat-cybercrime accessed 6 November 2026

“Uzbekistan to Introduce Legal Accountability for Citizens Facilitating Cybercrime” (Kun.uz, 29 April 2026) https://kun.uz/en/news/2026/04/29/uzbekistan-to-introduce-legal-accountability-for-citizens-facilitating-cybercrime accessed 6 November 2026

“Uzbekistan to Tighten Control over Bank Transfers and Card Transactions” (Yep.uz, May 2026) https://yep.uz/en/2026/05/uzbekistan-tightens-control-bank-transfers-card-transactions/ accessed 6 November 2026