

Financial Pyramids in Uzbekistan: Criminalisation, Detection, and the Preventive Role of Financial Institutions

Sardor Khushvaktov

Tashkent State University of Law, Uzbekistan



DOI : <https://doi.org/10.61796/ijblps.v3i7.519>



Sections Info

Article history:

Submitted: April 07, 2026

Final Revised: May 26, 2026

Accepted: June 18, 2026

Published: July 24, 2026

Keywords:

Financial pyramid

Ponzi scheme

Article 188

AML/CFT

Transaction monitoring

Payment organisations

Investor protection

ABSTRACT

Objective: This article argues that effective prevention requires criminal law to operate together with AML/CFT controls, anti-fraud systems, transaction monitoring, inter-agency coordination, early asset restraint and consumer protection. **Method:** The study combines doctrinal analysis of Uzbek legislation, risk-based compliance analysis, a limited comparison with Kazakhstan, Russia and the United States, and review of publicly documented enforcement episodes. **Results:** The principal gaps are the absence of published pyramid-specific typologies, a consolidated official warning mechanism, coordinated real-time response and a victim-oriented asset-recovery framework. Priority reforms should therefore focus on early detection and interruption of collection flows rather than on increasing punishment. **Novelty:** It proposes a legal-economic test for distinguishing pyramids from lawful commercial and investment models and identifies the transactional indicators available to banks and payment organisations.

INTRODUCTION

Financial pyramids persist in Uzbekistan for structural reasons. Bank cards, mobile payments, electronic money and instant peer-to-peer transfers allow a scheme to collect at a scale that once required cash couriers and physical offices. Recruitment has migrated to Telegram and other social platforms, while crypto-asset language supplies both a plausible profit narrative and an alternative settlement channel. Recent reporting shows schemes presenting themselves as international ventures while directing participants to personal bank cards [1].

Uzbekistan addressed the conduct through Article 1881 of the Criminal Code, introduced in 2016. The provision defines the offence by its economic mechanism: earlier obligations are serviced from newly attracted money or property. Its sanctions are substantial, but criminal procedure ordinarily begins after complaints or collapse, when funds may already have been withdrawn, converted into other assets or moved abroad. The weakness is therefore temporal rather than conceptual [2].

Preventable harm accumulates between a scheme's first mass collection and its interruption. That interval is largely visible to the licensed institutions through which contributions flow. A collection account may show many small inbound payments from unrelated persons, rapid redistribution to earlier participants and turnover inconsistent with the customer's declared profile. Existing AML/CFT systems can detect this pattern while a scheme is still growing, provided that monitoring expectations and escalation typologies are clearly articulated [3].

This article treats financial pyramids as a problem of institutional integration. It defines the boundary between unlawful and lawful models, identifies detection points available to financial institutions, evaluates the Uzbek legal and institutional framework, and proposes reforms that shift the response from prosecuting collapses to interrupting collections [4].

RESEARCH METHOD

The study applies doctrinal analysis to Uzbek criminal, AML/CFT, banking, payments, advertising, consumer-protection and crypto-asset rules. Comparison is limited to Kazakhstan, Russia and the United States because each offers a mechanism potentially adaptable to Uzbekistan.

Public enforcement material is treated as case-study evidence. Allegation, investigation, regulatory warning, charge and conviction are distinguished. Where an official judgment is unavailable, established media reporting is identified as such and unsupported figures are omitted.

Detection and institutional response are assessed through a risk-based compliance methodology consistent with FATF standards. Sources are ranked by authority: primary legislation, official regulatory material, enforcement information, international standards, peer-reviewed research and, only where necessary, reputable media reporting.

RESULTS AND DISCUSSION

Results

A financial pyramid is an arrangement in which obligations to earlier participants are discharged predominantly from contributions made by later participants rather than from genuine commercial or investment income. This economic formulation captures both Ponzi and classical pyramid structures and closely corresponds to Article 188 [5].

In a Ponzi scheme, an operator collects funds centrally from participants who believe they are investing in a managed venture and pays purported returns from incoming principal. A classical pyramid is more decentralised: participants pay to join and are rewarded for recruiting others, with payments moving through a hierarchy. Hybrid forms are common, so classification should follow the source and movement of funds rather than the label used in marketing [6].

The decisive question is the source of participant payouts. Revenue from genuine retail sales, identifiable assets or a real loan portfolio may support a lawful but risky model. Where payouts depend predominantly on new participant contributions, the arrangement is a financial pyramid, whatever its branding [7].

Pyramids imitate lawful forms. Multi-level marketing is lawful only where compensation is driven by genuine retail sales rather than recruitment or inventory loading [8]. A licensed fund relies on identifiable portfolio assets, custody, disclosure and audit; crowdfunding directs funds to identified projects with disclosed risk; referral

programmes treat bonuses as marketing expenditure for a genuine product; and bank deposits are supported by licensed prudential intermediation. Crypto products require the same economic scrutiny because virtual-asset language can obscure a classic Ponzi payment structure [9].

The differentiation test can accordingly be stated compactly. The analysis asks: (1) what is the genuine source of revenue, and does it exist at a scale commensurate with the funds collected; (2) does the model depend on recruitment or continuing new contributions to meet its obligations; (3) is there real commercial or investment activity, evidenced independently of the scheme's own materials; (4) could the arrangement survive if recruitment stopped; (5) is financial information transparent and independently verifiable, ideally audited; (6) is the activity licensed where the applicable regime requires it; (7) are promised returns economically realistic relative to the claimed activity; and (8) are withdrawals restricted, delayed, penalised or conditioned on further participation. Criteria (1), (2) and (4) are decisive; the remainder are corroborative and evidentiary [10].

No single indicator is conclusive. Guaranteed returns may exist lawfully in deposits, recruitment incentives in referral programmes and redemption restrictions in some investment products. The decisive question sales or investment income versus participant inflow is answered by tracing funds, which explains the central role of financial institutions [11].

Table 1. Core distinguishing criteria

Criterion	Financial pyramid	Lawful multi-level marketing	Licensed investment activity
Source of payouts	Contributions of later participants	Retail sales to end consumers	Income on identifiable portfolio assets
Role of recruitment	Structurally necessary	Permitted; commissions track sales	Absent
Real activity	Absent or incidental	Genuine marketable product	Real assets under custody
Sustainability	Requires continuous growth	Stable at constant size	Independent of participant inflow
Licensing and transparency	Unlicensed; no audited accounts	Trade registration; consumer-law duties	Licensed; disclosure, valuation, audit
Returns and exit	Guaranteed or implausible; exit obstructed	No investment return promised	Variable; redemption terms disclosed ex ante

Discussion

Detection operates on two layers, and the analytical error most often made in public discussion is to treat the first as sufficient.

Public warning signs include guaranteed or commercially unrealistic returns; recruitment-dependent income; an unclear profit source; collection to personal cards or shifting accounts; unverifiable licences or accounts; pressure to invest quickly; withdrawal restrictions; and false claims of state approval or institutional partnership. These indicators recur in regulatory guidance and empirical studies, but they must be assessed collectively [12].

Regulated institutions can see the transactional layer: numerous payments from unrelated persons, repetitive or rounded amounts, mass inflows to a personal or newly opened account, rapid redistribution, turnover inconsistent with the customer profile, complaints and chargebacks, related or nominee accounts, and movement into cash, crypto-assets or cross-border channels. Payment references may also contain recurring terms such as “investment,” “profit,” “bonus,” “package” or “activation [13].”

Neither layer proves an offence. An online retailer or fundraiser may display some of the same features. Suspicion arises from a cluster of indicators implausible promises, recruitment-led inflows, opaque profit sources, informal collection channels and obstructed withdrawals viewed against the customer’s known profile. Treating one indicator as decisive creates false positives and risks excluding lawful customers [14].

The institutional response has four stages. Onboarding should verify identity, beneficial ownership, licences, the business model and the expected transaction profile. Ongoing monitoring should test actual activity against that profile and use network analysis to detect mass collection and layered redistribution. Enhanced due diligence should obtain contracts, accounts and evidence of genuine goods, services or assets. Where the legal threshold is met, the institution should escalate, preserve evidence and file a suspicious-transaction report while separately assessing any lawful restriction or termination decision [15].

This response requires coordinated functions. AML/CFT owns reporting and customer-risk standards; anti-fraud often receives the earliest complaints; compliance and risk govern scenarios and risk appetite; legal reviews restrictions and tipping-off risk; information security preserves digital evidence; and internal audit tests effectiveness. Internal suspicion, proof of an offence, regulatory reporting and an account decision are different determinations and should not be conflated [16].

Financial pyramids are not only a fraud problem. Their proceeds may generate money-laundering risk; collection may amount to unauthorised financial activity; and organisers may use nominee accounts, cash, property, crypto-assets and cross-border transfers. The response must therefore integrate anti-fraud, AML/CFT, licensing, consumer-protection and operational-risk controls [17].

Article 188, introduced in 2016, criminalises the unlawful attraction of money or other property through promises of a property benefit where earlier obligations are met from newly attracted funds or property. It also covers directing the activity, ensuring its operation and advertising participation, including through mass media and the internet [18].

Liability is graduated. The basic offence may result in a fine, correctional labour, restriction of liberty or imprisonment for three to five years. Aggravated conduct including large-scale or repeated conduct, group participation, dangerous recidivism, or use of mass media or the internet may attract five to seven years' imprisonment. Especially large-scale conduct or organised-group involvement may attract seven to ten years. The current consolidated text confines advertisers to the basic composition [19].

Defining the offence by economic mechanism reduces dependence on proving separate deception for every participant and accommodates hybrid structures. Express liability for advertising reaches knowing promoters, but intent remains essential. No dedicated administrative offence for lower-level pyramid promotion was identified, leaving a difficult boundary between criminal advertising and conduct by a participant who did not understand the scheme [20].

Article 188 may interact with fraud, unlawful entrepreneurial activity and money laundering, depending on the facts and statutory elements. Civil claims for restitution, damages or unjust enrichment may proceed alongside criminal confiscation. Liability for organisers, promoters, account providers and advisers must therefore be based on provable knowledge, intent, role and benefit rather than participation alone.

The AML/CFT Law No. 660-II of 26 August 2004 applies to banks, payment organisations, crypto-asset service providers and other reporting entities. It requires customer due diligence, internal controls, risk assessment, monitoring and reporting of suspicious transactions to the authorised body. It is therefore the principal channel through which institutional detection of a suspected pyramid reaches the state [21].

The Laws on Banks and Banking Activity, the Central Bank, and Payments and Payment Systems establish the licensing perimeter and the Central Bank's supervisory powers over banks and payment providers. This matters in two ways: unauthorised collection of repayable public funds may create an earlier regulatory ground for intervention, and licensed providers are the principal real-time observers of mass collection [22].

Crypto-asset services are regulated by the National Agency of Perspective Projects. Official materials state that licensed service providers must be resident legal entities and that, from 1 January 2023, citizens and legal entities should conduct crypto-asset purchase, sale and exchange through national service providers. The Advertising Law prohibits improper and misleading advertising, while consumer law protects access to accurate information and remedies for loss. These regimes can support preventive action below the threshold of proven criminal advertising [23].

Responsibility is distributed. The financial intelligence function receives and analyses suspicious-transaction reports; investigative bodies and prosecutors establish criminal liability and trace assets; the Central Bank supervises banks and payment providers; the National Agency of Perspective Projects licenses crypto-asset services; advertising and consumer-protection authorities address misleading promotion and redress; and courts determine liability, confiscation and civil claims. Effective prevention depends on rapid coordination among these mandates [24].

Documented practice shows both that Article 188 is applied and that the response consistently arrives late.

The best-known adjudicated example is the case of Ahmad Tursunbaev (“Ahmadbay”). A contemporaneous report states that the Tashkent Regional Criminal Court sentenced him to 13 years’ imprisonment in February 2018 and left compensation issues for later determination. Because no published judgment was identified, the article relies only on this limited procedural account and does not repeat unverified estimates of participants, losses or recovery [25].

A more recent example is available only as investigative reporting. In June 2026 Kun.uz described the “Seven Jade” project as recruiting through Telegram, promising daily returns and directing payments to an individual’s bank card. The report is evidence of an alleged operating pattern, not a judicial finding, and no procedural outcome was identified at the time of research [26].

The available material illustrates recurring risks: personal payment instruments may be used for mass collection; online promotion can expand faster than institutional response; and conviction does not by itself guarantee timely compensation. Public warnings also remain dispersed across regulators and media rather than consolidated in a single official verification source [27].

No consolidated official statistics on Article 188 investigations, prosecutions, convictions or victim recovery were identified. The article therefore makes no quantitative claim about enforcement volume. The data gap itself limits evidence-based supervision and legislative review.

Kazakhstan criminalises the creation and management of a financial pyramid under Article 217 of its Criminal Code and separately regulates promotion. Official public guidance also emphasises characteristic indicators and the need for legal assessment of the whole model. Academic analysis nevertheless reports continuing qualification and coordination challenges, showing that a specific offence does not remove the need for consistent guidance and financial investigation.

Russia combines Criminal Code Article 172.2 with an administrative offence in Article 14.62 of the Code of Administrative Offences. The two-tier structure offers a comparator for proportionate treatment of promotion or collection conduct that does not meet the criminal threshold.

The United States contributes a strong investor-alert and civil asset-recovery practice. SEC and FTC guidance provides accessible public tests for Ponzi, pyramid and recruitment-driven models, while FATF guidance stresses prompt tracing, restraint and victim-oriented asset recovery. The transferable mechanisms are public warning lists, supervisory typologies, judicially controlled freezing and recovery systems designed to preserve value for victims.

Five gaps emerge in Uzbekistan. No public pyramid-specific monitoring typology for banks and payment organisations was identified; there is no single official warning list; published arrangements for real-time inter-agency coordination are limited; asset restraint and victim distribution typically begin after the investigative threshold is

crossed; and the law does not provide a proportionate intermediate response for promoters whose conduct falls below provable criminal intent. Where public information was insufficient, the article treats the point as a transparency gap rather than asserting that no internal mechanism exists.

CONCLUSION

Fundamental Finding: Uzbekistan's criminal law identifies the core mechanism correctly. Article 1881 covers unlawful collection, management, operation and advertising, with liability rising for aggravated forms. It is a sound foundation, but its effect is limited by the point at which criminal procedure normally intervenes. Banks and payment providers can identify clustered inflows from unrelated payers, rapid redistribution, activity inconsistent with the customer profile and extraction into cash or crypto-assets. **Implication:** The appropriate reform is integration rather than greater severity: connect criminal law to AML/CFT reporting, monitoring to supervisory expectation, detection to judicially controlled restraint, confiscation to victim distribution and enforcement to a public verification source. This would move the national response from prosecuting collapses toward interrupting collections while recoverable value remains. **Limitation:** The central limitation is temporal. By the time complaints accumulate and an investigation begins, contributions may have been withdrawn, converted or transferred. The publicly documented record shows that a custodial sentence and the separate problem of compensation can coexist. **Future Research:** Prevention depends on institutions that observe collection in real time. They already have due-diligence, monitoring and reporting duties; the missing elements are published typologies, defined escalation expectations, supervisory feedback and coordinated action.

REFERENCES

- [1] Republic of Uzbekistan, Criminal Code, Law No. 2012-XII, Sep. 22, 1994, art. 1881, as amended. [Online]. Available: <https://lex.uz/docs/-111453>. Accessed: Jul. 23, 2026.
- [2] Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations, Paris, France, updated Jun. 2026. [Online]. Available: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>. Accessed: Jul. 23, 2026.
- [3] U.S. Securities and Exchange Commission, "Ponzi schemes," Investor.gov. [Online]. Available: <https://www.sec.gov/fast-answers/answersponzihtm.html>. Accessed: Jul. 23, 2026.
- [4] U.S. Securities and Exchange Commission, "Beware of pyramid schemes posing as multi-level marketing programs," Investor Alert. [Online]. Available: <https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/investor-30>. Accessed: Jul. 23, 2026.
- [5] U.S. Federal Trade Commission, "Multi-level marketing businesses and pyramid schemes." [Online]. Available: <https://consumer.ftc.gov/articles/multi-level-marketing-businesses-and-pyramid-schemes>. Accessed: Jul. 23, 2026.

- [6] U.S. Federal Trade Commission, "Business guidance concerning multi-level marketing." [Online]. Available: <https://www.ftc.gov/business-guidance/resources/business-guidance-concerning-multi-level-marketing>. Accessed: Jul. 23, 2026.
- [7] U.S. Securities and Exchange Commission, "Ponzi schemes using virtual currencies," Investor Alert, Jul. 2013. [Online]. Available: https://www.sec.gov/files/ia_virtualcurrencies.pdf. Accessed: Jul. 23, 2026.
- [8] C. E. R. Heyman, "A red flag checklist for cryptocurrency Ponzi schemes," *Journal of Financial Crime*, vol. 31, no. 3, pp. 711–747, 2024, doi: 10.1108/JFC-05-2023-0118.
- [9] S. Bosley and M. Knorr, "Pyramids, Ponzis and fraud prevention: Lessons from a case study," *Journal of Financial Crime*, vol. 25, no. 1, pp. 81–94, 2018, doi: 10.1108/JFC-10-2016-0062.
- [10] Republic of Uzbekistan, Law No. 660-II, "On combating legalization of proceeds from criminal activity, financing of terrorism and financing of proliferation of weapons of mass destruction," Aug. 26, 2004, as amended. [Online]. Available: <https://lex.uz/docs/-283717>. Accessed: Jul. 23, 2026.
- [11] Financial Action Task Force, Guidance for a Risk-Based Approach: The Banking Sector, Paris, France, Oct. 2014. [Online]. Available: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach-banking-sector.html>. Accessed: Jul. 23, 2026.
- [12] Financial Action Task Force, Guidance for a Risk-Based Approach for Money or Value Transfer Services, Paris, France, Feb. 2016. [Online]. Available: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-money-or-value-transfer.html>. Accessed: Jul. 23, 2026.
- [13] Republic of Uzbekistan, Law No. ZRU-580, "On banks and banking activity," Nov. 5, 2019. [Online]. Available: <https://lex.uz/docs/-4581969>. Accessed: Jul. 23, 2026.
- [14] Republic of Uzbekistan, Law No. ZRU-582, "On the Central Bank of the Republic of Uzbekistan," Nov. 11, 2019. [Online]. Available: <https://lex.uz/docs/-4590452>. Accessed: Jul. 23, 2026.
- [15] Republic of Uzbekistan, Law No. ZRU-578, "On payments and payment systems," Nov. 1, 2019. [Online]. Available: <https://lex.uz/docs/-4575786>. Accessed: Jul. 23, 2026.
- [16] National Agency of Perspective Projects of the Republic of Uzbekistan, "Service providers in the sphere of crypto-assets turnover." [Online]. Available: <https://napp.uz/en/pages/service-providers>. Accessed: Jul. 23, 2026.
- [17] National Agency of Perspective Projects of the Republic of Uzbekistan, "Information statement," Dec. 29, 2022. [Online]. Available: <https://napp.uz/en/news/axborot-xabar>. Accessed: Jul. 23, 2026.
- [18] Republic of Uzbekistan, Law No. ZRU-776, "On advertising," Jun. 7, 2022. [Online]. Available: <https://lex.uz/docs/6052633>. Accessed: Jul. 23, 2026.
- [19] Republic of Uzbekistan, Law No. 221-I, "On consumer protection," Apr. 26, 1996, as amended. [Online]. Available: <https://lex.uz/docs/14643>. Accessed: Jul. 23, 2026.
- [20] UzDaily, "Ahmadbay sentenced to 13 years of jail," Feb. 22, 2018. [Online]. Available: <https://www.uzdaily.uz/en/ahmadbay-sentenced-to-13-years-of-jail/>. Accessed: Jul. 23, 2026.
- [21] Kun.uz, "New financial pyramid emerges in Uzbekistan, using official documents to gain public trust," Jun. 22, 2026. [Online]. Available: <https://kun.uz/en/news/2026/06/21/new-financial-pyramid-emerges-in-uzbekistan-using-official-documents-to-gain-public-trust-9effe6>. Accessed: Jul. 23, 2026.

- [22] Republic of Kazakhstan, Criminal Code No. 226-V, Jul. 3, 2014, art. 217, as amended. [Online]. Available: <https://adilet.zan.kz/eng/docs/K1400000226>. Accessed: Jul. 23, 2026.
- [23] Government of the Republic of Kazakhstan, "What is a financial pyramid and how not to become a victim?" [Online]. Available: <https://www.gov.kz/situations/236/intro?lang=en>. Accessed: Jul. 23, 2026.
- [24] G. Kaiyrbekova, "Criminal legal measures to counteract the activities of financial pyramids in the Republic of Kazakhstan," *Pakistan Journal of Criminology*, vol. 16, no. 3, pp. 153–170, 2024.
- [25] Russian Federation, Criminal Code, art. 172.2, "Activities for attracting money and/or other property." [Online]. Available: https://www.consultant.ru/document/cons_doc_LAW_10699/f495e538cbd830549504e85df0c84f27001900de/. Accessed: Jul. 23, 2026.
- [26] Russian Federation, Code of Administrative Offences, art. 14.62, "Activities for attracting money and/or other property." [Online]. Available: https://www.consultant.ru/document/cons_doc_LAW_34661/78c33211b5186947de7f9ed8ed24b5eb746144b8/. Accessed: Jul. 23, 2026.
- [27] Financial Action Task Force, Asset Recovery Guidance and Best Practices, Paris, France. [Online]. Available: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Asset-Recovery-Guidance-Best-Practices.pdf.coredownload.pdf>. Accessed: Jul. 23, 2026.

*** Sardor Khushvaktov (Corresponding Author)**

Tashkent State University of Law, Uzbekistan

Email: s.khushvaktov@tsul.uz; sardorkhushvaktov0301@gmail.com
