



FinCEN

ALERT

FIN-2026-Alert007

October 1, 2026

FinCEN Alert on the A7 Network

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Alert in SAR field 2 ("Filing Institution Note to FinCEN") and the narrative by including the key term "FIN-2026-A7NETWORK".

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to urge financial institutions¹ to be vigilant in detecting, identifying, and reporting suspicious activity, including involving the A7 Network.² The A7 Network is a global wholesale sanctions evasion and money laundering service with ties to Russia, leveraged by a wide range of illicit actors, including Iran and its terrorist proxies.³ The A7 Network's well-established and far-reaching digital asset channels are an appealing tool for a wide range of threat actors. Analysis

of BSA data also indicates that Iranian actors are leveraging the A7 Network, including the Central Bank of Iran and Iran's Islamic Revolutionary Guard Corps (IRGC).

FinCEN is issuing this Alert concurrently with a finding and notice of proposed rulemaking pursuant to section 9714(a) of the Combating Russian Money Laundering Act,⁴ finding transactions involving any company operating outside of the United States that is controlled by the A7 Network to be a class of transactions of primary money laundering concern.⁵

The information contained in this Alert is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, as well as open-source reporting and law enforcement information.

1. See 31 U.S.C. 5312(a)(2); 31 C.F.R. 1010.100(t).
2. On August 14, 2025, Treasury's Office of Foreign Assets Control (OFAC) designated A7 Limited Liability Company, A71 Limited Liability Company, A7 Agent Limited Liability Company, and related actors pursuant to Executive Order (E.O.) 13694. Treasury, Press Release, "[Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals](#)" ("Aug. 2025 Treasury Press Release") (Aug. 14, 2025).
3. For more information about the financing of the Iranian regime and its terrorist proxies, see FinCEN, FIN-2025-A002, "[FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts](#)" (June 6, 2025), and FinCEN, FIN-2024-A001, "[FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations](#)" ("May 2024 FinCEN Advisory") (May 8, 2024).
4. Section 9714(a) of the Combating Russian Money Laundering Act (Public Law 116-283), as amended by section 6106(b) of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81).
5. See generally, 31 CFR Chapter X, Part 1010, "[Proposal of Special Measure Prohibiting the Transmittal of Funds Regarding Transactions Involving the A7 Network's Sub-Agents](#)" (Oct. 2026).

How the A7 Network Operates

The A7 Network provides a financial services infrastructure for customers in Russia and other heavily sanctioned jurisdictions, such as Iran, which enables them to make cross-border payments in both fiat currency and digital assets while obscuring the sanctions nexus from U.S. and foreign financial institutions. Its global ambitions and self-described role as a sanctions-resistant payment service provider have made it a conduit for illicit activity associated with a wide range of threat actors, including North Korea (DPRK);⁶ Iran-backed terrorist organizations;⁷ cybercriminals and ransomware actors;⁸ and the IRGC.⁹ In a typical transaction, an A7 Network customer provides the A7 Network with information necessary to execute the transaction, which may include supplier information and trade documentation. The A7 Network then satisfies its customer's payment obligation through A7 Network-controlled settlement mechanisms, including bills of exchange or promissory notes (referred to as *veksels* in Russian), that record value inside the network.¹⁰ The A7 Network then assigns a Sub-Agent to appear as the contracting or paying party on invoices, sales agreements, and payment instructions. This enables the payment to be executed from non-Russian bank accounts through correspondent banking and Society for Worldwide Interbank Financial Telecommunication (SWIFT) channels.¹¹ In parallel with its fiat settlement mechanism, the A7 Network may use digital assets, including A7A5, a ruble-backed stablecoin developed within the network,¹² to transfer value across A7 Network-linked actors where banking channels are restricted or less dependable.¹³ Through this structure, the origin of payments from Russian or other sanctioned actors is obfuscated and the payments appear to financial institutions as ordinary commercial activity.

The Nodes of the Network

The backbone of the A7 Network, which has been sanctioned by OFAC as a significant transnational criminal organization,¹⁴ includes three Russia-based companies, all of which are sanctioned by OFAC,

6. For more information about DPRK illicit finance, see Treasury, "[2026 National Proliferation Financing Risk Assessment](#)" ("2026 NPFRA") (Mar. 2026), at pp. 5–7.
7. See generally May 2024 FinCEN Advisory, *supra* note 3.
8. For more information about ransomware, see FinCEN, FIN-2021-A004, "[Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments](#)" (Nov. 8, 2021).
9. See generally TRM Labs, "[The A7 Leaks: TRM's On-Chain Analysis of Russia's Cryptocurrency Connections](#)" ("June 2026 TRM Labs Report") (June 12, 2026); see also Centre for Information Resilience, "[A7 in Africa](#)" (Apr. 4, 2026), at p. 4. For more information about IRGC financing, see FinCEN, FIN-2026-Alert002, "[FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds](#)" (May 11, 2026).
10. See Open Source Centre, "[The Big Shor: A7 and the Illusion of Russian Financial Innovation](#)" ("2026 OSC Report") (2026), at pp. 30–31.
11. *Id.*, at pp. 32–34. Several sanctioned Russian financial institutions were removed from the SWIFT system in March 2022 shortly after its full-scale invasion of Ukraine, making it significantly harder for Russian financial institutions to conduct cross-border transactions. See SWIFT, "[An update to our message for the Swift Community](#)" (Mar. 20, 2022).
12. Stablecoins are a type of digital asset for which the value of the token is tied to another asset, typically a fiat currency such as the U.S. dollar. Stablecoins are appealing to illicit actors due to their relative liquidity, ease of settlement, and exchange rate stability. See 2026 NPFRA, *supra* note 6, at p. 16; see also Treasury, "[2026 National Money Laundering Risk Assessment](#)" ("2026 NMLRA") (Mar. 2026), at pp. 52–53.
13. See also Aug. 2025 Treasury Press Release, *supra* note 2.
14. See Treasury, Treasury Press Release, "[Operation Economic Outcast Takes Unprecedented Action Against Sanctions Evasion Network Used by Iran](#)" ("Oct. 2026 Treasury Press Release") (Oct. 1, 2026).

the European Union (EU), and the United Kingdom (UK): A7 Liability Company, and its subsidiaries A71 Limited Liability Company and A7 Agent Limited Liability Company, which are jointly owned by Ilan Shor¹⁵ and Promsvyazbank (PSB).¹⁶ The A7 Network controls Sub-Agents in order to send and receive payments to and from international entities on behalf of the A7 Network and its clients. As a result of OFAC's designation of the A7 Network, all property and interests in property of the A7 Network, including transactions involving Sub-Agents acting for or on behalf of the A7 Network, that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC.¹⁷

The A7 Network has also created and issued a ruble-backed stablecoin called A7A5. Kyrgyz Republic-registered, OFAC-sanctioned digital assets firm Old Vector LLC, which is part of the A7 Network, worked with digital assets exchange Garantex, Garantex's successor exchange Grinex, and others in the creation, issuance, and trading of the A7A5 token.¹⁸ Although A7A5 is issued by a Kyrgyz Republic-based company, each token is advertised to be backed by ruble deposits held at PSB.¹⁹ OFAC has announced that the A7A5 token is to be considered blocked property due to the interest of Old Vector LLC.²⁰

The Kyrgyz Republic plays a central role in both the A7 Network's fiat and digital asset activities. In addition to Grinex and Old Vector LLC, numerous Kyrgyz Republic-registered entities affiliated with the A7 Network maintain bank accounts both in the Kyrgyz Republic and at PSB, serving as critical vehicles for cross-border settlements.²¹ The state-owned Trading Company of the Kyrgyz

15. Ilan Shor was designated by OFAC in October 2022 pursuant to E.O. 14024 for his involvement in Russian malign influence operations in Moldova. He was previously arrested on money laundering and embezzlement charges related to the 2014 theft of \$1 billion from Moldovan banks. Treasury, Press Release, "[Treasury Targets Corruption and the Kremlin's Malign Influence Operations in Moldova](#)" (Oct. 26, 2022). Ilon Shor was also sanctioned by the United Kingdom on December 8, 2022. See UK Sanctions List, "[Shor Ilan](#)" (Apr. 9, 2025).
16. See Aug. 2025 Treasury Press Release, *supra* note 2. PSB was designated by OFAC in February 2022 pursuant to E.O. 14024 for issuing billions of dollars in financial support for Russian defense sector companies in its role as Russia's state defense bank. Treasury, Press Release, "[U.S. Treasury Imposes Immediate Economic Costs in Response to Actions in the Donetsk and Luhansk Regions](#)" (Feb. 22, 2022). PSB was later redesignated in January 2025 pursuant to E.O. 13662 for operating in the financial services sector of the Russian Federation economy. Treasury, Press Release, "[Treasury Disrupts Russia's Sanctions Evasion Schemes](#)" (Jan. 15, 2025).
17. See Oct. 2026 Treasury Press Release, *supra* note 14.
18. Garantex, which had been previously sanctioned as a prolific money launderer for Russian cybercriminals and other illicit actors, executed a scheme to move its funds to a successor exchange, Kyrgyzstan-based Grinex, following disruptive action by U.S. law enforcement in March 2025. Garantex allowed its customers who lost their funds following the law enforcement disruptions to regain access to their accounts using the A7A5 token. See Treasury, Press Release, "[Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex](#)" (Apr. 5, 2026); see also Aug. 2025 Treasury Press Release, *supra* note 2; see also Etherscan, Contract, "[Token A7A5](#)" (accessed Aug. 17, 2026).
19. See A7A5, "[Why A7A5](#)," at p. 1; see also Chainalysis, "[How A7A5 and Grinex Enable The Russian Shadow Crypto Economy](#)" (Aug. 14, 2025), at pp. 2-3.
20. See Oct. 2026 Treasury Press Release, *supra* note 14.
21. For example, OFAC designated Kyrgyzstan-based Keremet Bank in January 2025 for coordinating with PSB to implement a sanctions evasion scheme wherein Keremet Bank would facilitate cross-border transfers on PSB's behalf. Ilan Shor was directly involved in the discussions regarding Keremet Bank's role in this scheme. See Treasury, Press Release, "[Treasury Disrupts Russia's Sanctions Evasion Schemes](#)" (Jan. 15, 2025); 2026 OSC Report, *supra* note 10, at pp. 60-61.

Republic (TKKR) illustrates this typology: the A7 Network used TKKR as a payer entity to appear on external-facing trade documents, hold bank accounts, and send foreign-currency payments to suppliers abroad, obscuring the A7 Network customer's participation in the transaction.²² Through TKKR and other Sub-Agents, the A7 Network accessed the Kyrgyz Republic's financial sector and its banks' access to foreign currencies to indirectly pay suppliers, potentially unbeknownst to certain downstream participants in the relevant funds flows.²³

Use of "Sub-Agents"

As of June 2026, the A7 Network has expanded its operational capacity to facilitate sanctions evasion and money laundering by operating hundreds of companies that have established bank accounts at approximately 435 financial institutions in at least 83 countries. To establish Sub-Agents, the A7 Network forms, acquires, or partners with companies in third countries—such as Hong Kong, Indonesia, Kyrgyz Republic, the Seychelles, Türkiye, and the United Arab Emirates (UAE). Although these companies are typically represented to be owned or managed by non-Russian third-country nationals, they are ultimately controlled by the A7 Network.²⁴

Sub-Agents provide the A7 Network with access to correspondent banking relationships and foreign-currency liquidity, enabling the A7 Network to transmit value through the international financial system without a Russian or other sanctioned customer appearing in the payment chain.²⁵ In essence, this is a form of trade-based money laundering (TBML) that leverages Sub-Agents, falsified trade documents, false import-export records, and misleading goods descriptions. In many cases, funds may be transferred between multiple Sub-Agents to create additional layers of obfuscation before arriving at the final destination.²⁶

While funds are typically moved between these companies by Moscow-based A7 Network personnel, the A7 Network leverages Virtual Private Networks (VPNs) to create the illusion that these individuals are located outside of Russia—obscuring the connection between Russia and the Sub-Agents.²⁷ These VPNs typically depend on infrastructure provided by IT companies controlled by Ilan Shor and have operated on the domains muzpan.com and sodkamus.com and often appear to have IP addresses in Dubai, Hong Kong, or the Kyrgyz Republic.²⁸ Thus, there is often no clear indication of a connection between an A7 Sub-Agent and clients in the heavily sanctioned jurisdiction on whose behalf it is transacting. Sub-Agent transactions, however, are likely to exhibit typical money laundering indicators, including transactions in unusually high volumes shortly after the

22. See 2026 OSC Report, *supra* note 10, at p. 65.

23. *Id.*, at p. 67.

24. *Id.*, at p. 33.

25. *Id.*, at pp. 41–42.

26. See Centre for Information Resilience, "[A7 Abroad: How A7 Sells International Sanctions Evasion as a Service](#)" ("Oct. 2025 CIR Report") (Oct. 2025), at pp. 15–16.

27. See Centre for Information Resilience "[A7A5: Circumventing sanctions with stablecoin cryptocurrency](#)" ("June 2025 CIR Report") (June 25, 2025), at p. 15; see 2026 OSC Report, *supra* note 10, at pp. 28, 68.

28. See 2026 OSC Report, *supra* note 10, at pp. 26, 39. According to information available to FinCEN, customers that access accounts using serving IP ranges fall within 159.100.19.150/152 and 159.100.19.203/214 should warrant additional scrutiny from financial institutions. See June 2025 CIR Report, *supra* note 27, at pp. 13–15.

company is formed, inconsistencies between goods descriptions and supplier business profiles,²⁹ unusual payment routing through apparent shell companies, and falsified or AI-altered invoices.³⁰

Use of Digital Assets

Created by the A7 Network for use by its clients, A7A5 is a ruble-backed stablecoin that operates on the Tron³¹ and Ethereum blockchains.³² FinCEN, through analysis of available financial data, found that more than 180 entities processed A7A5 transactions that totaled at least \$179.1 billion dollars between February 2025 and June 2026. Historically, almost all of these transactions were processed through U.S., EU-, and/or UK-sanctioned entities, including Garantex and Grinex, and likely involved touchpoints with Russian banks.³³ However following an alleged hack of Grinex in April 2026,³⁴ A7A5 has been consolidated into unhosted wallets, suggesting the A7 Network is moving away from using previously named, sanctioned exchanges.³⁵

The token serves as an internal accounting method for the network, moving across internal addresses to maintain a balanced ledger, effectively acting as a mirror system³⁶ to the international payments made by the network.³⁷ According to public and BSA reporting, the tokens are used for transfers within Russia that represent foreign payments, and are made through nested digital asset wallets and financial accounts held in the name of A7 Network Sub-Agents. On the other side of the mirror trading system, the A7 Network employs its Sub-Agents to conduct fiat transactions—including U.S. dollars, yuan, dirhams, and euros—through the international financial system.

-
29. A7 Network payment Sub-Agents are tailored insofar as it is possible to the industries for which they are moving payments to avoid scrutiny from financial institutions. However, there are some indications that the A7 Network at times struggles to match Sub-Agents with specific customer business profiles. *See* Oct. 2025 CIR Report, *supra* note 26, at p. 20.
30. *See* Alexander Osipovich, The Wall Street Journal, “[Russia’s Hottest Startup Is a State-Backed Sanctions Evasion Network](#),” (Aug. 7, 2026). For more information about the use of AI to alter or generate fraudulent documents in furtherance of illicit finance schemes, *see* FinCEN, FIN-2024-Alert004, “[FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions](#)” (Nov. 14, 2024), at pp. 3–5.
31. Through Tron contract address at [TLvfrdym8RojreJ23dAGyfJDygrtiWKBZ](#).
32. Through Ethereum contract address at [0x6fa0be17e4bea2fcfa22ef89bf8ac9aab0ab0fc9](#).
33. *See* June 2026 TRM Labs Report, *supra* note 9.
34. *See* Elliptic, “[The fall of A7A5: how sanctions strangled the ruble stablecoin](#)” (“July 2026 Elliptic Report”) (July 29, 2026).
35. *See* Hannah Curtis, Crystal Intelligence, “[One wallet now holds 94.5% of A7A5’s supply](#)” (July 30, 2026).
36. The term “mirror transactions” or “mirror transfer” is used by U.S. law enforcement to describe a money laundering typology involving foreign currency exchange. The process typically happens within Chinese underground banking and black-market peso exchange schemes and usually involves a money broker or an accountant who conducts two equal, but separate, transactions involving at least two parties who often are unaware of each other. In this scheme, the broker or accountant makes payments to each party using the other parties’ currency, “mirroring” or balancing the transactions. In the instance of the A7 Network, transactions within Russia using the A7A5 token “mirror” movements of fiat currency through “Sub-Agents,” balancing the transactions while ensuring that the counterparties remain completely firewalled from one another. *See* Treasury, “[2024 National Money Laundering Risk Assessment](#)” (Feb. 2024), at pp. 29–30. For more information about Chinese underground banking and the black-market peso exchange, *see* FinCEN, FIN-2025-A003, “[FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds](#)” (Aug. 28, 2025).
37. *See* June 2026 TRM Labs Report, *supra* note 9.

In general, U.S. financial institutions are unlikely to directly see A7A5 transactions, as they primarily move between sanctioned entities.³⁸ The A7 Network has most often used the A7A5 tokens as a non-freezable, bridging asset to convert into other, more widely accepted digital assets, such as the stablecoin Tether (USDT), and which may then be converted to the fiat currency of the customer's choosing as another means of settling payments internationally.³⁹ In order to maintain the necessary liquidity to operate, the A7 Network uses its Sub-Agents or other trusted intermediary entities such as digital asset exchanges. This includes over-the-counter digital asset brokers (OTCs)⁴⁰ outside of Russia operating in jurisdictions of concern for A7 Network activity—especially firms that are newly created or dramatically expanding their stablecoin trading operations—which could serve as A7 Network liquidity providers.⁴¹ In addition, FinCEN analysis indicates that U.S. financial institutions may encounter use of derivative or “wrapped” tokens distinct from but “pegged” to the A7A5 token that serve as a representation of the A7A5 token on a blockchain to which A7A5 is not native;⁴² wrapped tokens are often accessed through decentralized finance applications.⁴³

Red Flag Indicators for A7 Activity

FinCEN has identified the following red flag indicators to help detect, prevent, and report potential suspicious activity related to sanctions evasion and other illicit activities using the A7 Network. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the totality of available facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags before determining that a behavior or transaction is suspicious.

38. See Aug. 2025 Treasury Press Release, *supra* note 2.

39. See Elliptic, “[A7A5: The ruble-backed stablecoin crosses \\$100 billion in transactions](#)” (Jan. 21, 2026); see also July 2026 Elliptic Report, *supra* note 32; June 2025 CIR Report, *supra* note 27, at p. 9.

40. OTCs are money services businesses (MSBs) that conduct peer-to-peer exchanges of digital assets for fiat currency, or digital assets for digital assets, between two parties without the use of a centralized digital asset exchange and usually involving large volumes. As part of the money laundering process, illicit actors often seek to convert digital assets, specifically stablecoins, into fiat currency via diffuse networks of OTCs brokers in third countries. These OTCs can receive substantial fees from illicit actors for providing cash-out services that leverage proxy accounts to circumvent digital asset service providers' Customer Due Diligence (CDD) processes or exploit providers with weaker AML/CFT controls, among other tactics. See 2026 NMLRA, *supra* note 12, at p. 50.

41. The A7A5 token is only available for purchase on a small number of exchanges, most of which are sanctioned by the UK, United States, or the EU; however, it is also traded using peer-to-peer exchangers and decentralized exchanges. See June 2025 CIR Report, *supra* note 27, at pp. 12–13.

42. A “wrapped” token is a digital asset that represents another digital asset on a non-native blockchain where the original asset is not offered. For example, a “wrapped” A7A5 token may offer trading of a representation of A7A5 on a blockchain other than A7A5's native blockchains. Wrapped tokens maintain a peg to the original asset, which is traditionally locked by a smart contract or maintained in a digital vault. See Securities and Exchange Commission and Commodity Futures Trading Commission, 17 CFR Parts 231 RIN 3235-AN56 and 241 and 17 CFR Part 1 RIN 3038-AF67, “[Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets](#)” (Mar. 23, 2026). Wrapped tokens may also be created on the same blockchain as the original token to make them compatible with decentralized exchanges. See June 2025 CIR Report, *supra* note 27, at p. 13.

43. See Ethereum Foundation, “[Wrapped ether \(WETH\)](#),” (last accessed Aug. 20, 2026).

Use of “Sub-Agents”

-  1 A customer conducts transactions with suspected or previously identified A7 Network Sub-Agents.
-  2 A customer conducts transactions with suspected shell companies⁴⁴ located in Kyrgyz Republic or other jurisdictions of concern for A7 Network activity.
-  3 A customer routes payments through several potential shell companies in multiple jurisdictions for no clear economic purpose before the funds arrive at their final destination.
-  4 A customer’s recently-formed company begins engaging in unusually high volumes of large transactions that occur over a short period of time and do not appear to be indicative of consistent business relationships with recurring counterparties.
-  5 A customer conducts a large volume of transactions with entities in disparate lines of business, or documentation related to a customer’s business transactions reveals inconsistencies between the descriptions of goods or services and the supplier’s business profile.
-  6 A customer accesses a financial account or conducts transactions from an IP address that resolves to identified VPN infrastructure known to be affiliated Ilan Shor and the A7 Network, such as the domains muzpan[.]com or sodkamus[.]com, and runs on servers based in jurisdictions known to host A7 Network digital infrastructure, such as Dubai, Hong Kong, or Kyrgyz Republic.
-  7 A customer provides an email address to register an account or communicate with their financial institution with a domain that resolves to mail servers affiliated with the domains muzpan.com or sodkamus.com.
-  8 A customer’s purported business website has a blank or minimally active website whose serving IP ranges fall within 159.100.19.150/152 and 159.100.19.203/214.

Mis-invoicing and Invoice Falsification

-  1 Documentation associated with a customer’s transactions include shipping invoices that use templates that differ from previously observed standards.
-  2 Documentation associated with a customer’s transactions contain overly simplified or vague product details, financially unlikely total dollar value prices for listed trade goods, or dates that do not make sense based on type of goods and/or services purportedly being purchased.
-  3 Shipping invoices and other documentation associated with a customer’s activities exhibit an analog “company stamp” affixed to an otherwise seemingly entirely digitally produced document.

44. Indicators of possible shell companies include opaque ownership structures, individuals/entities with obscure names that direct the company, or business addresses that are residential or co-located with other companies, especially companies that have been previously sanctioned.

-  Shipping invoices or other documentation for a customer's transactions contain out-of-place Cyrillic characters in otherwise English language documents.
-  Documentation associated with a customer's transactions appears to have been modified or wholly created using AI, for example displaying incorrectly formed letters, garbled wording, and malformed seals or other iconography.

Digital Asset Abuse

-  A customer offers, has traded in, or has historic direct or indirect exposure to trades denominated in the A7A5 token or in derivative, or "wrapped," tokens based on the A7A5 token.
-  A customer provides digital assets, especially stablecoins, to identified or suspected A7 Network Sub-Agents.
-  A customer engaged in international trade, import/export, or shipping using stablecoins to make large purchases or engage in a high volume of transactions, especially to pay for commodities not usually traded using digital assets, including military or dual-use goods or oil and petroleum products.
-  A customer operating a digital asset firm—including a firm that purports to be engaged in "over the counter," "OTC," or "block trading" services with a primary focus on stablecoin/fiat trading pairs—or suspected to be engaged in unregistered MSB activity involving digital assets sees a sudden, unexplainable growth in activity in jurisdictions with known touchpoints to A7 Network operations, especially if they have a minimal online presence or limited operating history.

FinCEN requests that financial institutions reference this Alert by including the key term "FIN-2026-A7NETWORK" in SAR field 2 (Filing Institutions Note to FinCEN) and the narrative.

Financial institutions wanting to expedite their report of suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

FinCEN's website, at www.fincen.gov, contains information on how to register for FinCEN Updates. FinCEN welcomes any feedback from financial institutions on this Alert, its utility, or other best practices or control limitations in addressing the typologies or red flag indicators described herein. Questions or comments regarding the contents of this Alert should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.