National Crime Agency

Office of Financial Sanctions Implementation HM Treasury

Foreign, Commonwealth & Development Office

NECC NATIONAL ECONOMIC CRIME CENTRE

10 YEARS PUBLIC PRIVATE PARTNERSHIPS

A7 Sanctions Evasion Mechanism

Date: August 2026

Reference: 0808-NECC

This Flash Alert is issued by the United Kingdom's National Crime Agency (NCA) and its National Economic Crime Centre (NECC), working in conjunction with OFSI and FCDO and financial sector partners as part of the Joint Money Laundering Intelligence Taskforce (JMLIT). The JMLIT was established to ensure a more collaborative approach between law enforcement and the private sector.

The subject matter contained within represents activity which has been identified as a current potential risk, such as a specific new or emerging typology or changing trend in activity, but has not been analysed or evaluated in the same way as a Red or Amber Alert. Therefore, this Flash Report should be read as highlighting a particular matter of potential concern for recipients to consider in line with existing anti-money laundering controls, and not a statement that the activity within is definitively of an illicit nature.

FLASH ALERT

Overview

In November 2025, the NCA published information pertaining to Operation DESTABILISE, which targeted a global money laundering network operating here in the UK. It highlighted that parties affiliated with DESTABILISE had attempted to acquire a stake in the Kyrgyz-based Keremet Bank, a major building block, designed to facilitate cross-border payments on behalf of Promsvyazbank (PSB), a sanctioned Russian state-backed bank supporting its military-industrial base[1].

In collaboration with PSB, the Russian-Moldovan oligarch and convicted fraudster Ilan Shor has established A7, a complex web of financial structures and tools hosted between Kyrgyzstan and Russia, with state-level backing. This alert details the risk A7's operations pose to the integrity of the international financial system and the considerable scale of its activities.

The NCA are issuing this alert to promote awareness and complement existing knowledge on A7 and its attempts to circumvent financial and trade sanctions on Russia. This alert forms part of ongoing collaboration between the NCA, NECC, JMLIT, HM Treasury's Office of Financial Sanctions Implementation (OFSI), Foreign Commonwealth and Development Office (FCDO) and private sector stakeholders to understand and counter the evolving sanctions threat presented by A7.

What We Would Like You to Do

The National Crime Agency (NCA) is a national law-enforcement agency which leads the UK's fight to cut serious and organised crime. The NCA Alerts process is the way in which we provide information to non-law enforcement bodies including the private sector to combat and disrupt serious crime. To help us to improve this service, we would welcome any feedback you have on both the Alert itself and the information provided to you. Please email all feedback to NECC.PPP@nca.gov.uk and include the reference 0808-NECC in the subject line.

If you identify activity which may be indicative of the activity detailed in this report, and your business falls under the regulated sector, you may wish to make a Suspicious Activity Report [SAR]. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include XXJMLXX within the text and the reference 0808-NECC for this alert within the relevant field on the NCA SAR Portal.

The NCA would also welcome any information identified as a result of this alert which does not constitute a SAR, including any information on action taken by you which you believe has or could have a disruptive impact on serious organised crime. Please email all such information to NECC.PPP@nca.gov.uk. Any information received in this way will be treated in confidence and will be handled in line with the data protection principles.

OFSI is the UK's competent authority for the implementation of financial sanctions. If you identify information that is indicative of either a frozen asset or of a breach of financial

[1] Op DESTABLISE press release, November 2025

sanctions, such as dealing with frozen assets or funds involving a designated person, then you must report this to OFSI. Please email all such information to OFSI@hmtreasury.gov.uk.

Feedback

The NCA would welcome any feedback in relation to this Alert to help us assess the impact this information has had on your organisation and inform updates and enhancements to future products. Please scan the QR code to our feedback form, or alternatively you can access this link from any internet enabled device.

Information Report

Established in 2024, A7 is a commercial enterprise backed by PSB and VEB.RF, a Russian state-owned development corporation and investment company. PSB describes A7 as offering an "unique mechanism" for Russian individuals and companies, and their foreign counterparts, to complete trade settlements "in the face of anti-Russian sanctions pressure". Within its first year of operating, A7 claims to have settled more than USD 86 billion. Fundamentally, A7 represents an alternative value transfer system, moving value across borders for clients in need of an obfuscation service[2]. Although A7 is known to use cryptoassets, as outlined further below, the network is engaged in the extensive exploitation of traditional fiat-currency payments, including using correspondent banking relationships, to circumvent sanctions on Russia and gain access to the global financial system. A7 and its affiliates have been sanctioned by the UK, USA and EU.

How does A7 illicitly use the international financial system?

A7's ability to complete cross-border transactions relies on third-country financial institutions, SWIFT, and, in turn, the illicit use of the international financial system. It has successfully created pools of liquidity outside Russia, which it uses to complete transactions on behalf of clients[3]. This A7-controlled liquidity has been introduced into the international financial system via a number of mechanisms, with the most historically significant being through its links to Kyrgyzstan and the Trading Company of the Republic of Kyrgyzstan (TKKR), liquidated in February 2026[4]. Crucially, when introduced, the liquidity bears no association with its Russian origin. Instead, it is linked to shell companies or so-called 'sub-agents' registered in jurisdictions across the globe. These 'sub-agents' hold local bank accounts connected to the wider banking system. Funds can be moved between the accounts and used to complete transactions with international suppliers on behalf of A7's clients, many of whom are Russian-based and/or sanctioned[5]. These transactions are also accompanied by false invoices manufactured and issued by A7 to provide a façade of legitimacy masking the predicate offences it commits, adhering to well-known practices used in trade-based money laundering[6].

Despite ostensibly being located in multiple foreign jurisdictions, the 'sub-agents' are controlled by individuals inside Russia. A7 manufactures an online presence for its shell companies by creating websites and email addresses which its staff use when communicating with banks. They also maintain a number of Virtual Private Networks (VPNs) so staff can masquerade as being located in the same jurisdiction as the banking services they seek to access[7]. This enables A7 to avoid traditional anti-money laundering regulations and know-your-customer checks.

[2] 'A7 Abroad', Centre for Information Resilience (CIR) (October 2025), p. 2-3
[3] 'The Big Shor', Open-Source Centre (OSC) (June 2026), p. 46-54
[4] Ibid, p. 62-76
[5] Ibid, p. 32-6
[6] Ibid, p. 40-1
[7] Ibid, p. 38-9

To date, A7's financial instrument of choice has been the promissory note or 'veksel'. Customers purchase these bills of exchange, which then act as credit and cover the value of transactions they want executed abroad. They allow A7 to track their obligations and are provided to customers to help ensure compliance with Russian regulations[8]. While linking A7's domestic and international activities in Russia, the note obfuscates A7's involvement in the international financial system as, when redeemed, there is no correspondent bank transfer from Russia. Instead, a shell company completes a seemingly separate transaction accompanied with false documentation for the financial system.

A7 directs payments through shell companies incorporated in numerous intermediary jurisdictions. These companies exploit complex, multi-layered correspondent banking arrangements to obscure their activities and avoid detection. OFSI's analysis of suspected A7 activity has identified transactions between A7 shell companies and UK-incorporated beneficiaries, routed through banks in several intermediary jurisdictions.

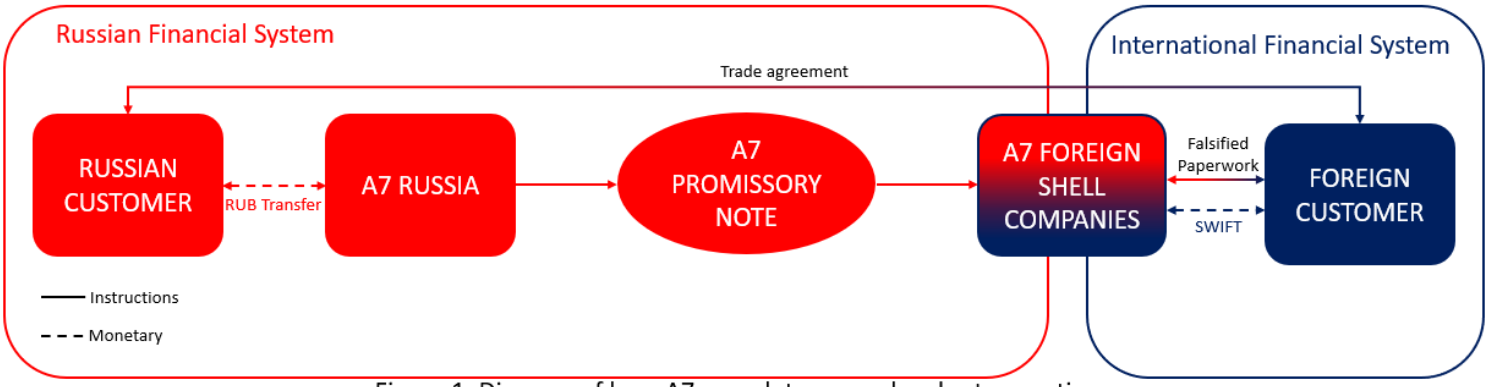


Figure 1. Diagram of how A7 completes cross-border transactions

Although A7 has primarily used a variety of Kyrgyz entities to facilitate its access to the international financial system, with one estimate suggesting around USD 8 billion flowed through the now liquidated TKKR by April 2025] more recently A7 has sought to diversify its access both geographically and technically. 78% of A7 transactions went through Chinese jurisdictions in August 2025. A7 is also expanding into Africa, with the opening of offices in Nigeria and Zimbabwe[9]. In the former it has established a relationship with local payments service provider (PSP) Pilot Finance Limited, now UK sanctioned, which had connectivity with British, Spanish and Ugandan financial entities[10]. Access to PSPs would provide A7 with the ability to further obfuscate the origin and purpose of transactions within the international financial system as a PSP can act as an intermediary between the 'sub-agent' and bank.

Given the extent of A7's activity, jurisdictions which permit A7 to use their financial systems are at increased risk of abuse for money-laundering and sanctions evasion purposes at scale. Analysis conducted on A7's clients found they represented "some of Russia's most important players in the military-industrial complex"; consequently, it may additionally be involved in

[8] Ibid, p.30-1
[9] 'A7 Abroad', Centre for Information Resilience (CIR) (October 2025
[10] Ibid, p. 108-10

proliferation financing[11]. Furthermore, its backer PSB is focused on supporting Russia's military industry[12]. As such, supervisors, financial institutions, virtual assets service providers and designated non-financial businesses and professions may wish to consider incorporating this particular threat into risk assessments and mitigation plans, for which cross-border collaboration on information sharing will be essential.

Red Flag indicators

No single red flag is indicative of illicit activity associated with the A7 network and all surrounding facts and circumstances should be considered before determining whether specific transactions or customers are associated with the A7 network.

- Companies with a limited history completing large volumes of transactions with established entities in ostensibly different industries;
- Invoices detailing goods or services which are distinct from the suppliers' usual products;
- Multiple transfers completed between obscure companies operating ostensibly in different industries;
- Limited information on ownership, directors or beneficiaries;
- Companies registered or operating in known jurisdictions of high risk;
- Companies with a limited online presence with websites containing generic stock photos and minimal to no details on individuals operating the company;
- Use of VPNs to conduct banking, including companies or their representatives using VPNs that may match the jurisdiction in which they seek banking services but do not match their profile. For example, differing locations within the same jurisdiction, or at locations not associated with their address.

[11] Ibid, p. 95

[12] 'A7 Abroad', p. 24

Suspicious Activity Reporting [SARs]

If you know or suspect that there has been money laundering or terrorist financing activity (including as a result of information provided to you by the NCA) and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the NCA under Part 7 Proceeds of Crime Act 2002 and the Terrorism Act 2000. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the reference 0808-NECC within the specified field on the NCA Portal. This reference is specific to the Alerts process; where appropriate, we would ask that this is used *in addition* to the ongoing use of the Glossary Codes. Guidance on making suspicious activity reports is available at www.nationalcrimeagency.gov.uk.

Alert Markings

The Flash Alert is intended to promptly inform the private sector of emerging trends and/or typologies of suspected money laundering or economic crime that may be of immediate interest or concern to their institutions. We recommend you use this Flash Report to complement existing knowledge and support on-going improvements to your business processes and procedures.

NCA Alerts

Recognising that the private sector is often the victim of serious organised crime and is engaged in its own efforts to prevent, deter, and frustrate criminal activity, the NCA seeks to forge new relationships with business and commerce that will be to our mutual benefit – and to the criminals' cost. By issuing Alerts that warn of criminal dangers and threats, NCA seeks to arm the private sector with information and advice it can use to protect itself and the public. For further information about this NCA Alert, please contact the NECC PPP team by email NECC.PPP@nca.gov.uk. For more information about the National Crime Agency go to www.nationalcrimeagency.gov.uk.

Protecting the Public – Providing Information Back to the NCA

Section 7(1) of the Crime and Courts Act 2013 allows you to disclose information to the NCA, provided the disclosure is made for the purposes of discharging the NCA's functions of combating serious, organised, and other kinds of crime. The disclosure of such information to the NCA will not breach any obligation of confidence you may owe to a third party or any other restrictions (however imposed) on the disclosure of this information. The disclosure of personal information about a living individual by you to the NCA must still comply with the provisions of the Data Protection Act 2018 (DPA). However, you may be satisfied that the disclosure by you of such personal information to the NCA in order to assist the NCA in carrying out its functions may be permitted by Schedule 2, Part 1 of the DPA 2018. This allows a data controller to be exempt (by means of a restriction or adaption) from provisions of the GDPR, if the personal data is processed for the following purposes:

a) the prevention or detection of crime,
b) the apprehension or prosecution of offenders, or
c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions of the GDPR would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).
(DPA 2018, Schedule 2, Part 1).

Any Section 7(1) information should be submitted to NECC.PPP@nca.gov.uk.

The NCA's Information Charter is published on our external website at www.nationalcrimeagency.gov.uk.

Handling Advice – Legal Information

This information is supplied by the UK's NCA under Section 7(4) of the Crime and Courts Act 2013. It is exempt from disclosure under the Freedom of Information Act 2000. It may be subject to exemptions under other UK legislation. Except where permitted by any accompanying handling instructions, this information must not be further disclosed without the NCA's prior consent, pursuant to schedule 7, Part 3, of the Crime and Courts Act 2013.

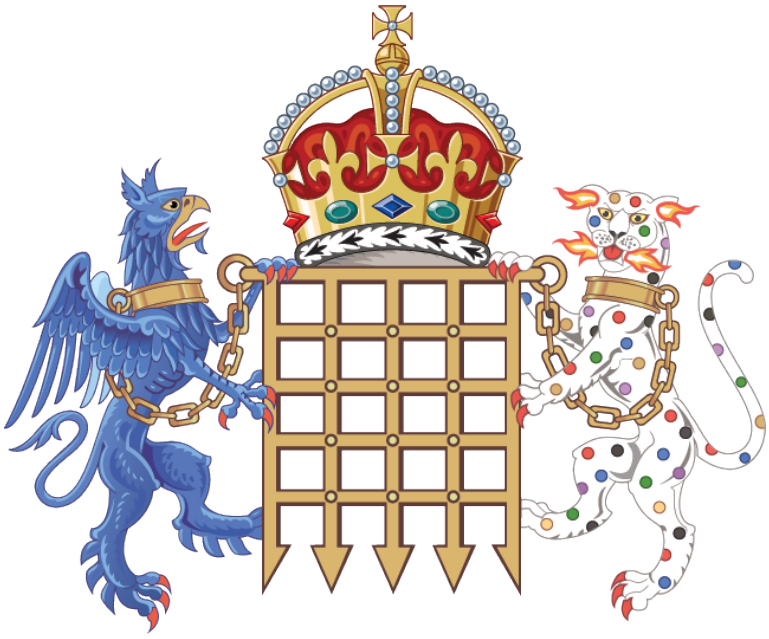
This report may contain 'Sensitive Material' as defined in the Attorney General's guidelines for the disclosure of 'Unused Material' to the defence. Any sensitive material contained in this report may be subject to the concept of Public Interest Immunity. No part of this report should be disclosed to the defence without prior consultation with the originator.

Requests for further disclosure which are not permitted by any handling instructions or handling code must be referred to the NCA originator from whom you received this information, save that requests for disclosure to third parties under the provisions of the Data Protection Act 2018 or the Freedom of Information Act 2000 and equivalent legislation must be referred to the NCA's Statutory Disclosure Team by e-mail on statutorydisclosureteam@nca.gov.uk.

Disclaimer

While every effort is made to ensure the accuracy of any information or other material contained in or associated with this document, it is provided on the basis that the NCA and its staff, either individually or collectively, accept no responsibility for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any such information or material.

Any use by you or by any third party of information or other material contained in or associated with this document signifies agreement by you or them to these conditions.



NCA
National Crime Agency

nca.gov.uk

NECC
NATIONAL ECONOMIC CRIME CENTRE

10 YEARS
PUBLIC PRIVATE PARTNERSHIPS

Follow us on LinkedIn:
@National Economic Crime Centre (NECC)