



A7 UNDERCOVER

A7's Undeclared Links to International Payment
Platforms

A7 UNDERCOVER

A7's Undeclared Links to International Payment Platforms

28 October 2026

Table of Contents

EXECUTIVE SUMMARY.....	3
Disclaimer.....	7
1 INTRODUCTION.....	8
1.1 WHAT IS A7?.....	8
1.2 STRUCTURE OF THIS REPORT.....	8
2 A7 INTERNATIONAL: NEW A7 SERVICE TARGETS INTERNATIONAL CUSTOMERS.....	10
3 TRUE CODE AND BACKEND'S WORK LINKED TO A7.....	13
3.1 WHOIS REGISTRATION DATA FOR BACKEND ON A7-LINKED DOMAINS.....	13
3.2 TRUE CODE AND BACKEND SUBDOMAINS REFER TO A7.....	15
3.3 TRUE CODE'S FINTECH AND TREASURY PROJECTS MATCHING A7'S DESCRIPTION.....	16
4 PAYMENT PLATFORMS WITH TECHNICAL LINKS TO A7 AND TRUE CODE/BACKEND.....	18
4.1 INDICATOR 1: MIRRORED DOMAIN ARCHITECTURE.....	18
4.2 INDICATOR 2: CONNECTED AND/OR MATCHING API DOCUMENTATION.....	20
4.2.1 SPECIFIC CONNECTIONS BETWEEN AMANI.BOT, QBANQ.NZ AND FINANCE-BOT.DEV.....	22
4.3 INDICATOR 3: HIGHLY SIMILAR USER INTERFACE AND EXPERIENCE.....	23
4.4 INDICATOR 4: IP ADDRESSES LINKING BACKEND TO THE FOUR PAYMENT PROJECTS.....	27
4.5 WEIGHT OF EVIDENCE SUPPORTS A STRONG CONNECTION.....	28
5 AMANI AI: TARGETING AFRICA, ASIA, UAE, BRAZIL.....	29
5.1 MAISON DU COMMERCE DU TOGO (MCT) AND THE A7 CONNECTION.....	29
5.2 AMANI AI'S TERMS OF USE AUTHORED ON BEHALF OF MAISON DU COMMERCE DU TOGO BY LAWYER LINKED TO A7 NIGERIA.....	32
5.3 LUVERTA TRADE LLC DRAWS LINK TO KYRGYZSTAN.....	32
5.4 ADDITIONAL SERVICES: BANK CARDS AND TRON WALLET GENERATION.....	33
5.5 WEBSITES REDIRECTING INTERNATIONAL USERS TO AMANI AI.....	34
6 QBANQ.NZ: A NEW ZEALAND-BASED INTERNATIONAL PAYMENTS PLATFORM.....	36
6.1 QBANQ LIMITED AND AUSNZ TECH LIMITED.....	37

7	FINANCE BOT	40
8	THE PAYMENT PLATFORMS ARE USING THIRD-PARTY SERVICES AND PAYMENT PROVIDERS.....	41
8.1	UNDISCLOSED LOCAL PAYMENT PROVIDERS	41
8.2	THIRD PARTY FINTECH PROVIDERS: TERRAPAY, SYMPLEPAY, AND BRIDGE.....	45
8.3	INTERNATIONAL AI PLATFORMS MAY BE USED BY A7	47
9	DISCUSSION: EVOLVING THREAT CALLS FOR INCREASED VIGILANCE AND AGILE RESPONSE.....	49

EXECUTIVE SUMMARY

Russia's A7 network appears to have taken a significant and concerning new step: open-source evidence suggests A7 is offering cross-border payment services to unwitting international customers through at least one possible front company without disclosing any connection to A7 or to Russia. A7 also appears to be using unknowing third-party service providers to facilitate its operations.

Key Findings:

- A7 International was publicly launched by A7 on 13 October 2026 as a cross-border payments service targeting non-Russian users. It offers USDT-to-fiat transfer via the SWIFT system.
- **Two further payment platforms appear to run a version of the same bespoke AI-enabled payment system as A7 International.** Amani AI is operated by a company claiming to be wholly owned by the government of Togo. Qbanq is operated by a New Zealand-registered company. An additional two linked payment projects appear to be in development but not publicly operational.
- **There is evidence linking these payment platforms to Russian software developers who appear to have worked for A7:** The bespoke AI-enabled payments system appears to have been developed by True Code and Backend, two Russian software companies owned by the same individual, Artem Shelengovskiy. Domain registration records and the companies' own subdomains indicate they have worked on A7 products since at least May 2025.
- **There are multiple technical indicators linking A7 International, Amani AI, and Qbanq:** These include mirrored website structures (including distinctive shared subdomains); near-identical technical documentation carrying the internal project name "A7T"; near-identical user interfaces, each with an "AI Concierge" chatbot; and server addresses shared only by Backend and the payment projects. No single indicator is conclusive, but together the weight of evidence that these sites are technically connected is very strong.
- **Further evidence links Amani AI to A7:** The website of Amani AI's stated operator, Maison du Commerce du Togo, was registered using details previously used for A7's infrastructure and linked to a house owned by Ilan Shor. It shares its security certificate with the website of a known A7 shell company. An individual with the same name as a lawyer at Pilot Finance, a Nigerian company sanctioned by the UK and Ukraine for its ties to A7 Nigeria, appears to have authored Amani AI's Terms of Use. Amani AI is also linked to a Kyrgyz company, Luverta Trade.

- **API specifications further link Amani AI and Finance-bot.dev to Qbanq.nz:** API specifications for amani.bot, qbanq.nz, and finance-bot.dev mutually reference both Amani AI and Qbanq. For example, Qbanq’s API appears to utilise references to Amani AI’s Bank Directory, while Amani AI uses ‘qbnq’ and “Qbank” as masked rail codes, among multiple other such examples. The sites appear to be actively maintained at the same time. This appears to reflect a strong connection between the platforms at the technical level. When contacted by the Financial Times, the **owner of Qbanq Limited denied any knowledge of A7** or these technical connections, stating that the platform has been built by third-party contractors.
- **Amani AI targets users in Africa, Asia, the UAE, and Brazil:** Nine websites funnel businesses in Nigeria, Ghana, the UAE, India, the Philippines, and Brazil towards Amani AI, again without mentioning A7 or Russia. This mirrors public announcements that A7 has made about its intended geographical expansion.
- **The platforms are reliant upon third-party services:** This includes a network of largely unknown payment service providers that funnel payments via the fiat banking system. CIR has also found the names, although not the definitive identities, of several providers. These third-party providers may be unaware of A7’s apparent use of their services.
- **The possible purpose for using international payment platforms is to develop a source of ‘clean’ USDT for A7:** A7 makes heavy use of USDT in its operations. However, USDT, which has been publicly linked to A7, Russia, or other entities associated with sanctioned activities, is at risk of being frozen by Tether. One motive behind the use of A7 International and Amani AI may be to develop a reliable source of ‘clean’ USDT from customers with no link to Russia, which can then be used in A7’s operations (notably, as of 15 October 2026, neither allowed payouts to Russia itself). It is not possible from the open-source evidence to determine the motive for building Qbanq based on the same technology.
- **If this motive is correct, this marks a worrying escalation:** it would suggest that A7 has moved from supplying knowing Russian clients to targeting businesses and individuals in other countries into unwittingly supplying liquidity to A7’s wider scheme.

Implications and Response

- **Need for increased vigilance:** A7’s use of covert tactics such as shell companies is not new, but the possible creation of fully fledged front entities that conceal their links to Russia and target international customers reflects the need for ongoing monitoring of A7’s expanding activities and tactics.
- **Cross-border cooperation essential to tackling cross-border risk:** The cross-border, decentralised nature of this network underlines the importance of

regulators, law enforcement, and governments, especially in the targeted regions, sharing information and raising collective awareness of A7's methods.

- **An important role for cryptocurrency companies:** Because USDT remains central to A7's operations, Tether in particular may have an important role to play alongside law enforcement. Other cryptocurrency exchanges and services could also contribute.
- **Tracking A7's use of technical enablers and the private sector:** A7 still depends on Western payment providers, fintechs, AI companies, software tools and other businesses, who are possibly unwittingly enabling A7 operations. Identifying these entities and preventing that facilitation could significantly impact A7 operations.
- **Enhanced public awareness increases resilience:** Increasing public awareness about A7 and its tactics, especially among users of cross-border payment services, could help to combat their expansion and prevent any exploitation of unwitting customers looking for international payment services. This includes developing an understanding of potential red flags to be wary of.

Points of Note

A7 has stated in previous public statements that it was created to ensure uninterrupted settlements for the Russian market, against which illegal restrictive measures have been imposed. It has also stated that it serves third countries not related to sanctions, providing legal export-import operations with consumer goods and raw materials. It has stated that it operates a modern multi-level compliance system, and all clients undergo screening that makes it possible to identify risks and excludes the servicing of individuals and organisations whose activities violate requirements.

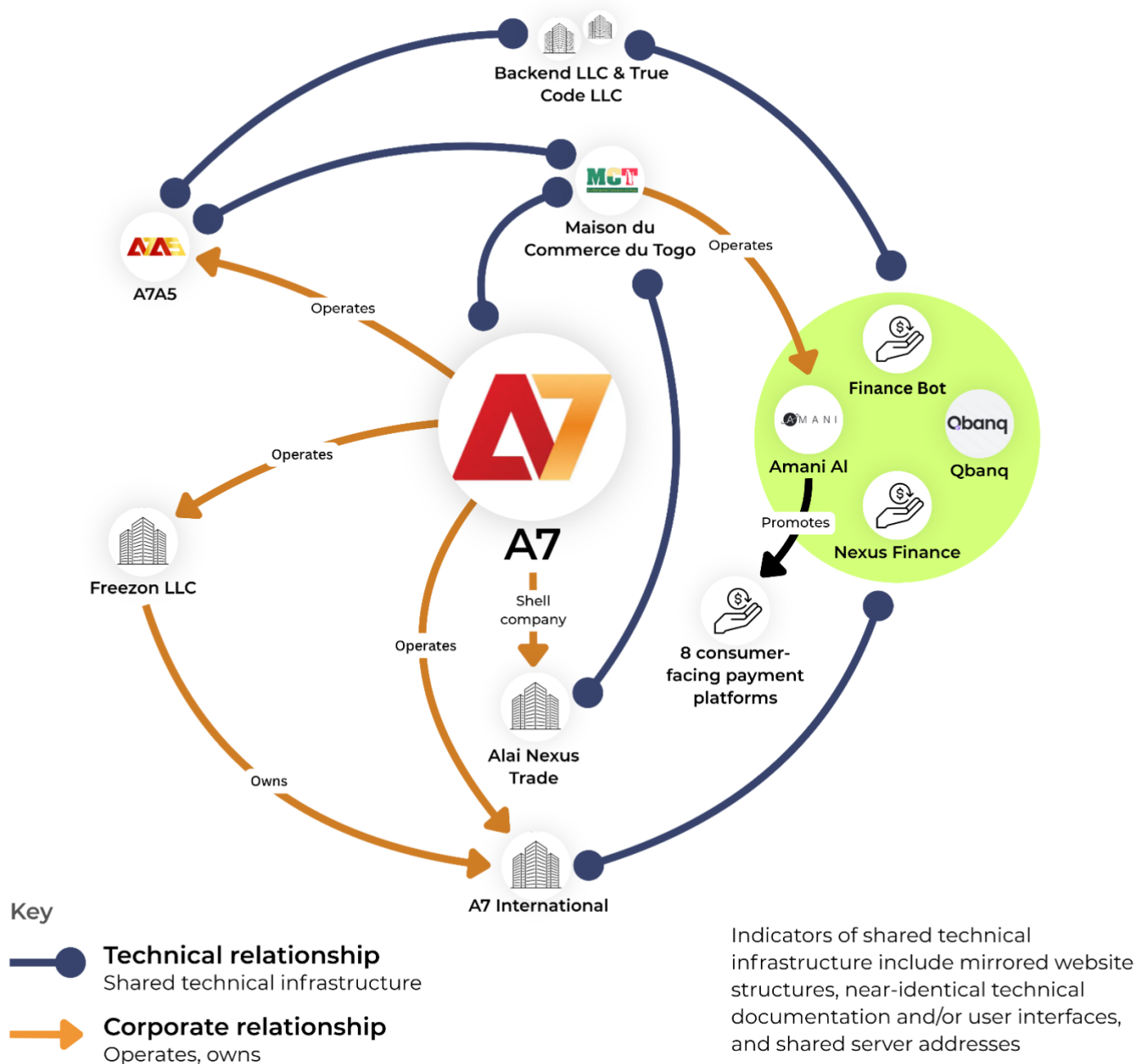
When contacted by the Financial Times in connection with this report, the owner and registered Director of Qbanq denied any knowledge of A7 or awareness of his platform's deep technical connections to Amani AI. He stated that the Qbanq.nz platform has been built for him by subcontractors contacted through an associate in New Zealand, with whom he had not dealt directly, and that he was unaware of whether they have any connections to Russia.

CIR did not attempt to send any payments via the platforms discussed in this investigation.

Nothing in this report is intended to allege, and it should not be read as alleging dishonesty, wrongdoing, or improper conduct by any individual or organisation, save as expressly stated and based on the evidence identified.

A7's undeclared links to payment platforms

Platforms connected to A7 through corporate or technical relationships



Disclaimer

This report has been prepared in good faith on the basis of open-source data available to CIR at the date of, and as documented in, this report. We believe the facts stated in this report to be true and the opinions expressed to be honestly held, based on those facts.

Where a statement of fact relies on information from third parties, this is indicated, and that information has not been independently corroborated unless stated.

Opinions, conclusions and potential implications are identified as such and represent the author's honest assessment; they are not statements of established fact.

Nothing in this report is intended to allege, and it should not be read as alleging, dishonesty, wrongdoing or improper conduct by any individual or organisation, save as expressly stated and based on the evidence identified.

1 INTRODUCTION

1.1 WHAT IS A7?

A7 is a Russian network which facilitates sanctions evasion and transnational money laundering. As of 1 October 2026, [US authorities](#) have designated it as a significant transnational criminal organisation, and it is subject to sanctions in multiple jurisdictions, including the US, UK, and EU.

A7 is 51% owned by sanctioned businessman and convicted fraudster Ilan Shor and 49% owned by Promsvyazbank (PSB), a Russian state-owned bank geared to servicing Russia's defence sector. The connection between A7 and the Kremlin has become increasingly overt and direct over the course of 2025 and 2026. The company has repeatedly been publicly endorsed by Russian President Vladimir Putin and Foreign Minister Sergei Lavrov. On 15 October 2026, Russian news agency [Interfax](#) reported that Finance Minister Anton Siluanov, Energy Minister Sergei Tsivilev, and First Deputy Prime Minister Denis Manturov had joined A7's board, underscoring the increasingly close ties between A7 and the Kremlin. As of July 2026, A7 claims to be facilitating roughly 20% of Russia's overall foreign trade, as reported by [The Wall Street Journal](#).

A7 has been the subject of multiple investigations by CIR beginning in June 2025, including its [network of shell companies](#), its [cryptocurrency A7A5](#), its [expansion into Africa](#), and its [facilitators in Kyrgyzstan](#).

A major problem that has confronted A7 throughout its operations is the need to access large amounts of 'clean' USDT. USDT plays a major role in A7's laundering operations, but USDT tokens which have previously been linked to criminal or sanctioned entities (including A7 itself as well as many of its Russian customers) also pose a significant risk. Tether, the organisation which controls USDT, has previously cooperated with US and international law enforcement to freeze funds, including in the [Garantex](#) case, which directly impacted A7 early in its existence.

One purpose behind A7's push to target international customers with USDT-to-fiat payment services may be to resolve this issue by developing an international stream of 'clean' USDT not connected to either A7 or to Russia, which they can then use for other purposes. Notably, as of October 2026, neither A7 International, or any other service covered in this report appear to allow payouts to Russia itself.

1.2 STRUCTURE OF THIS REPORT

This investigation examines the international expansion of A7's payment infrastructure to target unwitting consumers in multiple jurisdictions.

[Section 2](#) covers A7 International, A7's publicly launched cross-border payment platform and its digital infrastructure.

[Section 3](#) examines the linkages connecting Russian software companies True Code and Backend with the relevant payment platforms.

[Section 4](#) unpacks OSINT evidence indicating that the A7 International platform, domains, and the other identified platforms are related.

[Section 5](#) focuses on Amani AI, one of the platforms identified, and provides additional OSINT findings that connect the platform to A7, including A7's presence in Togo and Nigeria (see CIR's [April 2026 report](#) for more information on A7's expansion into Africa). It also discusses nine websites identified by CIR which promote Amani AI's cross-border payment services specifically to customers in Ghana, Nigeria, the UAE, Brazil, India, and the Philippines.

[Section 6](#) focuses on Qbanq, another of the platforms identified with technical links to A7.

[Section 7](#) focuses on Finance Bot.

[Section 8](#) discusses the role which third-party service providers appear to play in the platforms' operations. It is highly possible that these service providers are unaware that their tools are being used by entities linked to A7.

[Section 9](#) considers the implications and potential responses to the investigation's findings.

Additional details, including a related entity and an in-depth analysis of platform API specifications, are included in the report's Appendix.

2 A7 INTERNATIONAL: NEW A7 SERVICE TARGETS INTERNATIONAL CUSTOMERS

A7 has built a business model around the use of covert tactics and deception. Previously, these tactics have been aimed primarily at deceiving banks, regulators, and enforcement bodies to enable A7 to evade sanctions levelled against Russian entities. New evidence strongly suggests A7 is expanding its operations to target ordinary non-Russian businesses and consumers across the world.

On 13 October 2026, [A7's Telegram channel](#) reported the launch of A7 International, a cross-border payments service targeting non-Russian users. It advertises cross-border transfers in which the payer submits funds in USDT via the TRON blockchain, and the recipient receives fiat currency via SWIFT.¹

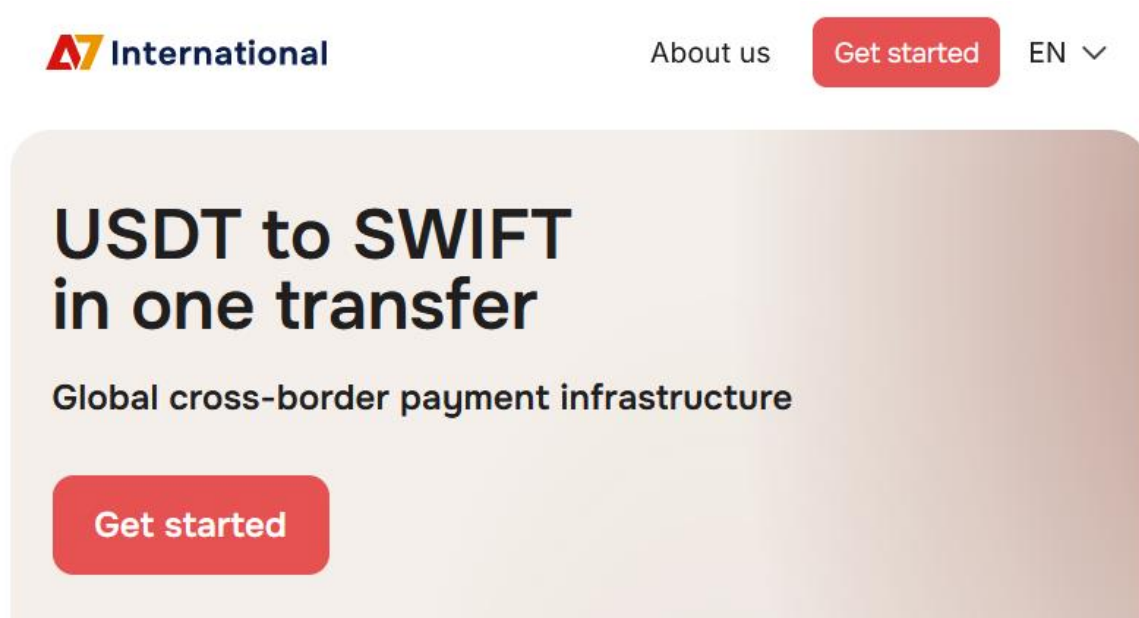


Figure 1: Screenshot of the A7 International homepage captured on 14 October 2026.

[A7 International](#) says it is “trusted by over 10,000 clients worldwide”, has coverage of over 100 countries, and offers payouts in USD, EUR, CNY, and AED² (although transfers can only be paid in using USDT). Processing takes one day. The domain is available in English and Russian.

¹ The TRON Network is a decentralised, open-source layer-1 blockchain platform. It is designed for high-speed, low-cost smart contracts and decentralised applications (DApps), and it serves as the largest host network for Tether (USDT) stablecoins globally. Fiat currency is Government-issued money that is not backed by a physical commodity like gold or silver, deriving its value instead from government decree and public trust.

² CNY - Chinese yuan renminbi; AED - Emirati dirham

A7 International

Trusted by over 10,000 clients worldwide

Get started



Global coverage of 100+ countries



Payments in USD, EUR, CNY, AED.
Other currencies available on request



Legal compliance and fast invoice processing



Reliable and secure payment corridors

Send USDT — your recipient gets a SWIFT transfer

1+ business day

Payment processing time



From 0.5%*

Service fee for individuals



From 0.3%*

Service fee for legal entities



*Rate depends on currency and jurisdiction

Figure 2: Screenshot of the a7.biz homepage (Source: a7.biz).

The homepage (a7.biz) explains how to use the service: users upload invoices and recipient details, and A7's system analyses them and automatically extracts key data. They then connect their crypto wallets, confirm the USDT transfer, and receive confirmation from an unspecified "respective financial network." It is not clear from the evidence available in open source how exactly the internal mechanics of this payment process work.

How to pay a supplier with USDT using A7 International



1

Register

Sign up in your
A7 International
personal account



2

Upload your invoice

The system
automatically
recognizes and
extracts the required
data



3

Upload recipient documents

Provide beneficiary's
Certificate of
Incorporation



4

Connect your crypto wallet

Link your wallet and
confirm transaction
on blockchain



5

Done

You will receive
payment
confirmation from
respective financial
network

Figure 3: Screenshot of the a7.biz homepage (Source: [A7 International](https://a7.biz)).

The homepage footer and [Terms of Use](#) state that the A7 International platform is owned by Kyrgyz company Freezon LLC ("Фризон" ЖЧК, 327393-3301-ООО, INN

00104202610504).³ Registered on 1 April 2026 to an address in Bishkek, its registered purpose is non-specialised wholesale trade.

CIR has identified at least two further domains associated with A7 International. One, core-bny.com, contains identical content to a7.biz on some pages and may be an early or test version for the platform. Appendix 1 contains further details on A7 International's web infrastructure.

CIR has identified evidence suggesting that the technical infrastructure behind these entities, and possibly the A7 International-branded projects as well, was likely created by one of two software companies owned by the same individual and working for A7. These companies are **True Code** and **Backend**.

³ Core-bny.com's [Terms of Use](#) state, "The text of this document is being updated and will be published later", which appears to support the hypothesis that core-bny.com is at least partially a test site for A7.biz.

3 TRUE CODE AND BACKEND'S WORK LINKED TO A7

Artem Vladimirovich Shelengovskiy⁴ is a Russian software developer. He is the owner of two software development companies registered in Irkutsk: **True Code LLC** (ООО "Верный Код"), registered in 2015 and **Backend LLC** (ООО "Бэкенд"), registered in 2024. In practice, these two companies appear to operate somewhat interchangeably, with True Code as the public face and the aptly named Backend as the more backend operational arm of the collective organisation.

In 2022, Shelengovskiy moved to New Zealand, where Shelengovskiy told Russian-language business and technology platforms [VC.ru](#) and [Habr](#) that his company, True Code, engaged in projects for New Zealand-based clients. This included registering a separate [New Zealand website](#) and [Facebook presence](#) for its New Zealand work.

In the months immediately following Russia's full-scale invasion of Ukraine in 2022, True Code, according to its [Telegram channel](#), continued working with Russian government clients while also expanding its services to the UAE, Kazakhstan, and Indonesia.

Strong open-source evidence shows that Shelengovskiy and his companies appear to have worked on A7 products since at least May 2025. This includes: i) Whois registration data, ii) subdomains on Backend and True Code's own domains referring to A7 and its products A7A5 and StablePay and iii) multiple similarities between projects described by Shelengovskiy and his companies and publicly available data on A7 operations.

CIR has not identified and does not impute any evidence of criminal wrongdoing by True Code and Backend. The following sections simply document open-source evidence indicating connections between these entities and the A7 network.

3.1 WHOIS REGISTRATION DATA FOR BACKEND ON A7-LINKED DOMAINS

Historical Whois records show that Shelengovskiy and Backend registered the domain a7a5-wallet.com in May 2025. The same Whois details, including Shelengovskiy's name and the backendgroup.ru support email address, were also later used to register a7a5-wallet.dev. As of October 2026, both domains use Whois privacy protection.

[Whois](#) records also show that Shelengovskiy and Backend are the current registered owners of stable-pay.tech, a domain created on 1 February 2026.

⁴ Sometimes transliterated as Shelengovskii.

The three domains, a7a5-wallet.dev, a7a5-wallet.com, and stable-pay.tech, appear to have been linked to the StablePay card project. Multiple a7a5-wallet.dev [subdomains](#) displayed a [StablePay login page](#), whereas dev-admin.a7a5-wallet.dev displayed a [login page](#) featuring the A7A5 logo.

According to a [Radio Liberty](#) report, StablePay was a relatively short-lived effort by A7A5 to launch a payment card that users could top up with A7A5 tokens and use to pay for various online services. The project appears to have encountered several hurdles and petered out in late 2025.

Backend appears to have begun an effort to revive the project in February 2026. However, all three domains appear defunct as of October 2026. Instead, the project appears to have ultimately re-emerged on the [stable-pay.cards](#) domain. This domain was registered one day after Shelengovskiy registered the stable-pay.tech domain. It has used Whois privacy protections from the start; however, it shares a key IP address with stable-pay.tech and Backend subdomains referring to A7A5.⁵

While not definitive, on the balance of probabilities, it seems highly likely that this domain was also developed by Backend. However, this remains an inference rather than an established fact and cannot be confirmed definitively.

⁵ When two domains resolve to the same IP, they may sit on the same machine or account, indicating that they may have been created by the same actor. This is not always the case, as many domains use shared hosting services. A shared IP is a stronger signal when the IP appears to be dedicated, such as a private server hosting only a handful of sites.



Date resolved	Detections	Resolver	Domain
2026-09-30	0 / 91	VirusTotal	www.stable-pay.cards
2026-06-02	0 / 91	VirusTotal	admin.stable-pay.cards
2026-06-02	0 / 91	VirusTotal	api.stable-pay.cards
2026-06-02	0 / 91	VirusTotal	op.stable-pay.cards
2026-04-03	0 / 91	VirusTotal	sms.stable-pay.cards
2026-04-03	0 / 91	VirusTotal	vip.stable-pay.cards
2026-04-03	0 / 91	VirusTotal	alertbot.stable-pay.cards
2026-02-17	0 / 91	VirusTotal	stable-pay.cards
2026-02-03	0 / 91	VirusTotal	wallet.stable-pay.cards
2026-02-01	0 / 91	VirusTotal	admin.stable-pay.tech
2026-02-01	0 / 91	VirusTotal	alertbot.stable-pay.tech
2026-02-01	0 / 91	VirusTotal	www.stable-pay.tech
2026-02-01	0 / 91	VirusTotal	vip.stable-pay.tech
2026-02-01	0 / 91	VirusTotal	sms.stable-pay.tech
2026-02-01	0 / 91	VirusTotal	op.stable-pay.tech
2026-02-01	0 / 91	VirusTotal	wallet.stable-pay.tech
2026-02-01	0 / 91	VirusTotal	proxy-a7a5-prod.backendgrou...
2026-02-01	0 / 91	VirusTotal	stable-pay.tech
2026-02-01	0 / 91	VirusTotal	api.stable-pay.tech
2026-02-01	0 / 91	VirusTotal	proxy--a7a5-prod.backendgrou...

Figure 5: VirusTotal resolutions for IP address 45.10.42.203.

3.2 TRUE CODE AND BACKEND SUBDOMAINS REFER TO A7

Both True Code (t-code.ru) and Backend (backendgroup.net, backendgroup.ru) have subdomains that appear to reference A7 or related products.

The subdomain a7-support.t-code.ru was created on 14 July 2025. As of October 2026, the subdomain still exists, but the ISPmanager Hosting Control Panel, which previously appeared to be there, has been [disabled](#).

Backendgroup.net has at least nine subdomains which appear to reference A7A5 or StablePay.⁶ These subdomains suggest that Backend/True Code was building and testing elements of the A7A5 and StablePay products on their own domains, presumably with the intention of later deploying them on separate domains.

Taken together, these indicators provide strong evidence that True Code, Backend, and Shelengovskiy appear to have worked on behalf of A7 on its payment technologies, including during the period when they also developed the payment projects discussed below. CIR does not allege wrongdoing by True Code, Backend, or Shelengovskiy.

3.3 TRUE CODE'S FINTECH AND TREASURY PROJECTS MATCHING A7'S DESCRIPTION

In 2025, True Code and Shelengovskiy published website content and blog posts discussing a project they undertook for an unnamed client.

CIR cannot definitively confirm that the client was A7. However, the description of the client, their business processes, and the technology that Shelengovskiy's companies developed for them closely match A7 and the payment projects investigated in this report. A full analysis of the similarities between True Code's description of the project and A7 operations is contained in Appendix 5. This includes:

- Hacked and leaked files from 2025 showing internal operations at A7 at that time closely matched True Code and Shelengovskiy's description of their client
- A plausible timeline for the project aligning with Shelengovskiy and Backend's registration of relevant A7 domains
- Numerous similarities between the systems described on the website and blog post and Ilan Shor's description of A7 International

If the project described by True Code and Shelengovskiy is indeed A7, it suggests that the picture painted by the 2025 hacked files about A7's internal processes, which has formed the basis of much recent reporting about A7, is likely now out of date. A7 may now function significantly differently internally, at least when it comes to payment processing. This has ramifications beyond the current investigation.

Two of the systems described – “digital assistants” for processing payments and an automated method for parsing differently formatted invoices – bear an extremely

⁶ dozzle-a7a5-prod.backendgroup.net; dozzle-a7a5-prod2.backendgroup.net; dozzle-stablepay-prod2.backendgroup.net; jenkins-a7a5-prod.backendgroup.net; jenkins-stablepay-prod2.backendgroup.net; kafka-ui-a7a5-prod.backendgroup.net; portainer-a7a5-prod.backendgroup.net; portainer-stablepay-prod2.backendgroup.net; proxy-a7a5-prod.backendgroup.net

strong resemblance to the technology underpinning the USDT-to-SWIFT payment services offered by the payment projects discussed in this investigation. In a report on the Russian specialist financial news and analysis platform, [Finversia](#), Shelengovskiy described using AI to determine optimal international payment pathways, another service the payment projects advertise and that A7's representatives have publicly boasted about in [Russian media](#). This similarity is an observation and not a statement of fact.

4 PAYMENT PLATFORMS WITH TECHNICAL LINKS TO A7 AND TRUE CODE/BACKEND

In February 2026, while True Code and Backend Group were actively working on StablePay and the A7A5-wallet domains, they also appear to have been involved in the development of a suite of at least two and up to four payment projects under other names and domains. These projects do not state that they have any link to A7 or Russia. However, multiple technical indicators suggest they are variants of the same bespoke platform underlying A7 International.

These four projects are:

- Amani AI (amani-ai.com, amani.bot)
- Qbanq (qbanq.nz)
- Finance Bot (financebot.pro, finance-bot.pro, finance-bot.dev) - Non public⁷
- Nexus Finance (nexusfinance.pro, nexusfinance.dev)- in development⁸

The technical indicators are:

- i. Mirrored domain architecture
- ii. Connected or matching API documentation
- iii. Highly similar user interface (UI) and user experience (UX)
- iv. Shared IP addresses linked to Backend

In documenting evidence of these linkages, CIR does not allege or impute any evidence of wrongdoing by any of these entities.

In a statement to the Financial Times, the registered owner of Qbanq Limited Tehmus Mistry denied any knowledge of A7 and said that the qbanq.nz platform had been built by subcontractors found for him by an associate in New Zealand (as discussed above, True Code and Shelengovskiy have a history of operating in New Zealand). He stated that he did not deal with the subcontractors directly and was unaware of qbanq.nz's technical links to Amani AI. See the below section on Qbanq for more details.

4.1 INDICATOR 1: MIRRORED DOMAIN ARCHITECTURE

CIR has identified a pattern of at least 15 matched subdomains across all six payment projects (with 34 matched across multiple, but not all, of the projects). As

⁷ According to its site, Financebot appears to have been launched in January 2026, then pulled down again, and may now be serving some kind of support function for Amani AI and Qbanq.

⁸ Nexus Finance does not appear to have been fully developed. As of 13 October 2026, like a7int.kg, the [domain host](#) is not set up.

some of these projects appear to be actively under development as of 13 October 2026, this number may rise as more subdomains are added.

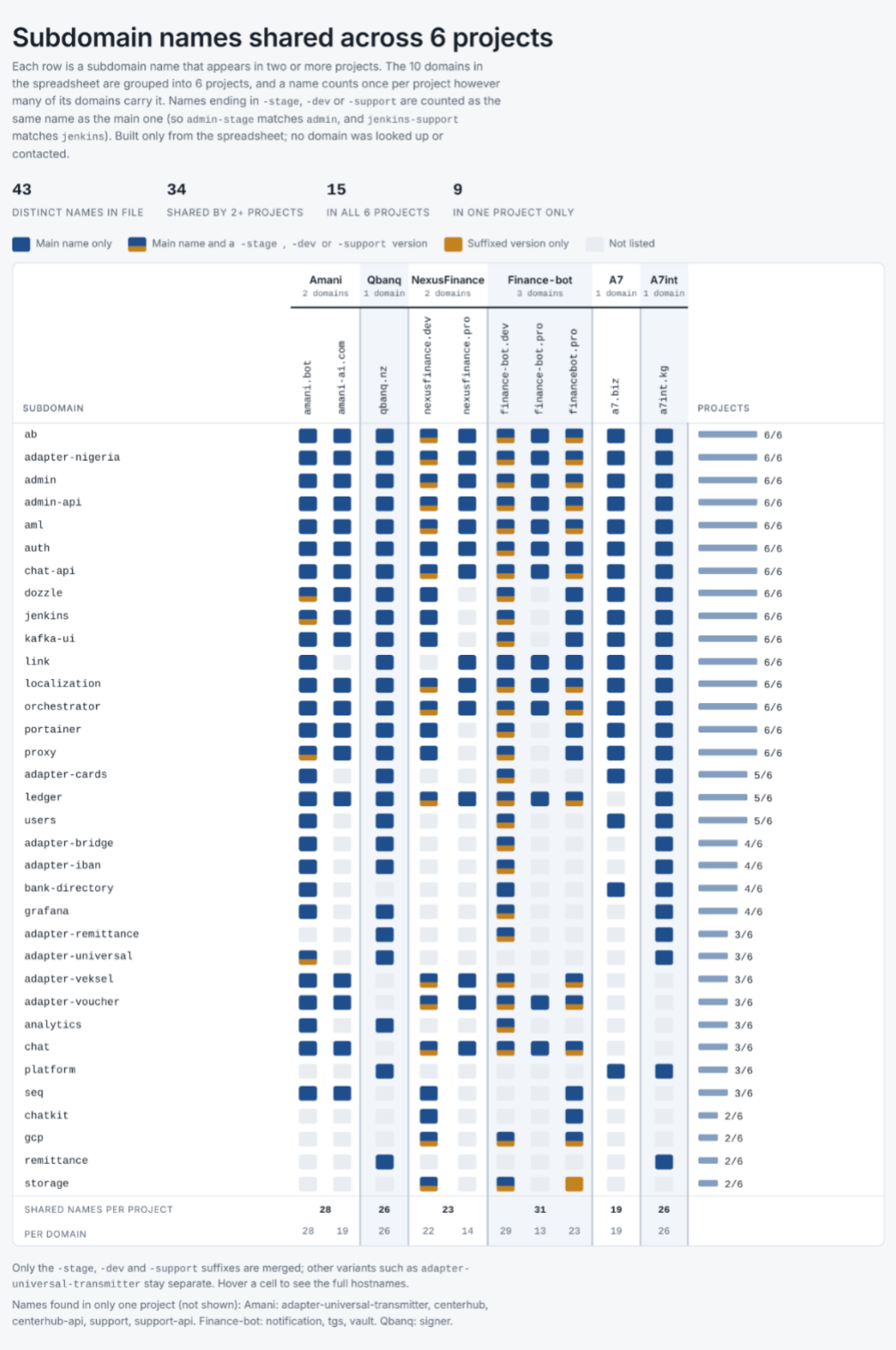


Figure 6: Matching subdomains across the six projects. Subdomains analysed by CIR in the week of 5-10 October 2026. Graphic generated by CIR using Claude.

While some of these subdomains are generic (e.g. 'auth', 'admin'), others are highly distinctive. For example, the 'adapter-nigeria' and 'adapter-veksel' subdomains are each relatively unusual on their own, but together they appear likely to be unique

to this set of domains. 'Veksel' (вексель) is the Russian word for promissory notes or bills of exchange, a payment instrument used extensively by A7, according to [Kommersant](#). It is questionable what other organisations might tailor their payment platforms for both Russian promissory notes and Nigerian users.

4.2 INDICATOR 2: CONNECTED AND/OR MATCHING API DOCUMENTATION

CIR identified Swagger UI instances containing API specifications, which had been left publicly accessible across the domains for the overtly A7 International branded projects, a7.biz, core-bny.com, and for the projects amani.bot, qbanq.nz, and finance-bot.dev. CIR's internal technology team conducted a manual review of the API documentation. This was supplemented with a separate analysis using Claude AI, a publicly available Large Language Model.

CIR's manual analysis found that the documentation was highly similar across the A7 International and other Backend platforms. The API files are nearly identical in structure, with only minor variations, strongly suggesting a common source or shared backend framework rather than independent development.

There is no indication that the implementation was copied from an open-source project or standard backend template. The specifications contain substantial business-specific logic, particularly in the orchestrator and ledger, further suggesting a shared, purpose-built architecture. Both sets of documentation also included many references to 'A7T', a code which appears in multiple places across the projects and may serve as an internal project name or signifier.

The apparent use of **ASP.NET Core**, a Microsoft framework commonly employed in high-performance, transaction-intensive enterprise systems, is noteworthy. While not conclusive, its use alongside substantial business-specific logic and design consistency suggests deliberate technical design and experienced backend development.

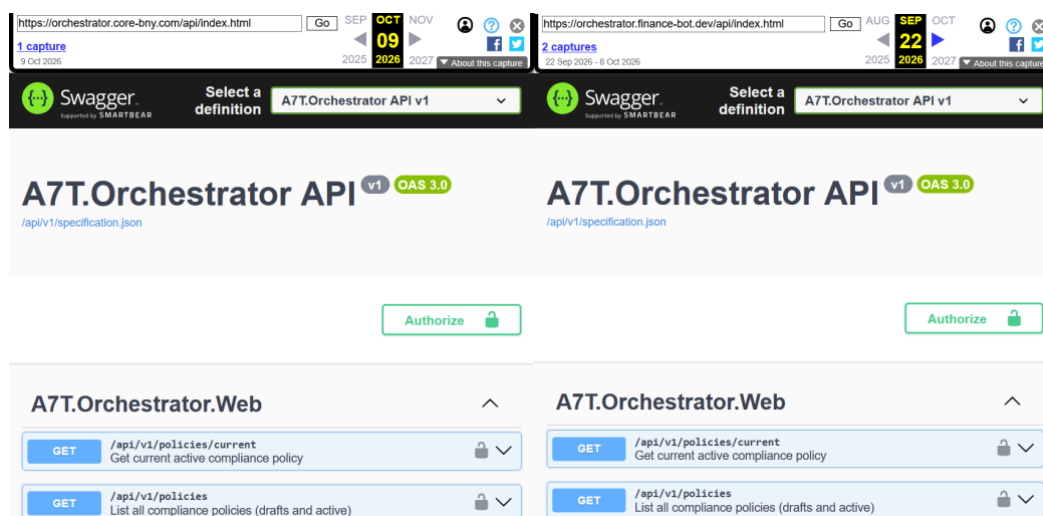


Figure 7: Screenshots of API documentation on [Left] core-bny.com and [Right] finance-bot.dev.

Claude AI's analysis similarly concluded that the API specifications from the two A7 International branded domains and three covert domains were versions of the same platform, based on multiple indicators detailed below.

A simplified version of Claude's findings is included here. A more in-depth version is available in Appendix 5. CIR does not specialise in programming or software development and encourages interested parties to verify all findings based on Claude's analysis with a human expert.

Indicators

- **Shared product names.** Every spec carries one of two internal names, "A7T" (A7T.Ledger, A7T.Orchestrator, A7T.Remittance, A7T.ChatBFF) or its successor "Platform" (Platform.Ledger, Platform.Orchestrator). "A7T" also matches the a7.biz domain.
- **Identical code across domains.** Where specs overlap, endpoint paths, operation names, descriptions, and data models match word for word, including quirks, like listing both "200 OK" and "201 Created" for one call.
- **A consistent version pattern.** Across the ledger, orchestrator, and chat services, amani.bot carries the oldest build, finance-bot.dev a later one (including staging and demo addresses), and core-bny.com, a7.biz, and qbanq.nz the newest.
- **Shared ticket numbers.** Internal tickets with the same "BAC-" prefix (BAC-2495, BAC-2621, BAC-3360, BAC-3469, BAC-3470) appear in ledger, remittance, and chat specs on different domains.
- **Services that call each other by name.** The ledger registers its actions with "Orchestrator", the remittance gateway names "ChatBFF" as its caller, and the chat API proxies the ledger, orchestrator, and remittance services. They form one connected system, not separate products.
- **Brand names tying domains together.** The remittance gateway on qbanq.nz and finance-bot.dev is titled "Amani", matching amani.bot, and the chat API calls an "Amani.BankDirectory" service. Payout partners are masked as "QBank" rails (codes qbnq1, qbnq2...), matching qbanq.nz.
- **The same tenant and business model.** The remittance module's example tenant is "amani", and the ledger, remittance, and chat services all centre on USDT balances, with fees, exchange-rate markup, and KYT/AML screening handled the same way.
- **Payout partners named despite masking.** The remittance service hides partners behind QBank codes, but the chat specs name TerraPay, Bridge

and an "AdapterNigeria" exchange-rate service, which links the masked rails to identifiable providers.”⁹

4.2.1 SPECIFIC CONNECTIONS BETWEEN AMANI.BOT, QBANQ.NZ AND FINANCE-BOT.DEV

The API specifications for Amani AI, Qbanq.nz and the finance-bot.dev domain contain multiple specific references to one another.

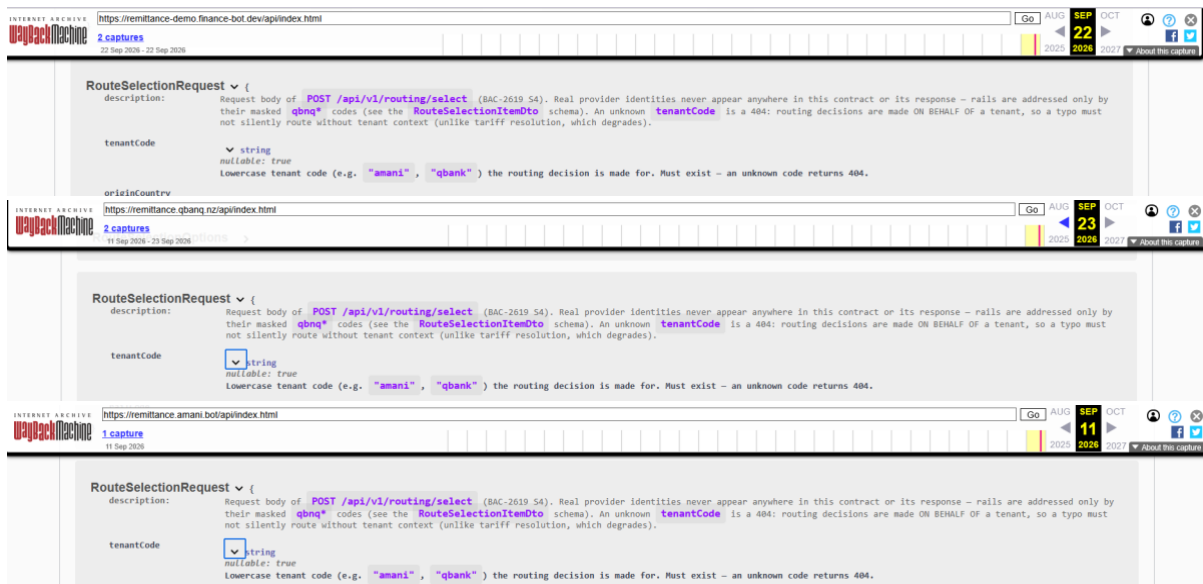
For example, the [adapter-remittance.qbanq.nz](#) API specification is titled "Amani.AdapterRemittance API", with the description "Anti-corruption-layer proxy from the Amani platform to A7T.Remittance's routing/select and providers/catalog runtime contracts (BAC-2621).". This matches the exact title and description from [adapter-remittance.amani.bot](#). Both sets of specs use “qbnq” as the masked rail code.

In another example, the [remittance.amani.bot API](#) similarly makes direct references to “qbnq*”, “qbanq1” and “Qbank 1” as the masked rail code and “neutral, operator-facing label... safe to show to end users” respectively. In a chat with CIR’s test account, the Qbanq chatbot also referenced “Qbanq1” as an option for payment methods (see Fig. 19).



The [remittance-demo.finance-bot.dev](#) [remittance.amani.bot](#) and [remittance.qbanq.nz](#) API specs all reference both ‘amani’ and ‘qbnq’ as ‘tenant codes’

⁹ Claude also noted one instance of Cyrillic in the API spec documentation for qbanq.nz, “...delivery asset/network (USDT→TRON, USDC→BASE; null until persisted per plan **n.2c**), rail, status...” “n.” is the standard abbreviation of *пункт* (“item” or “clause”), used in Russian, Ukrainian, and some other languages. The note therefore reads “per plan item 2c”, apparently referring to an internal planning document.



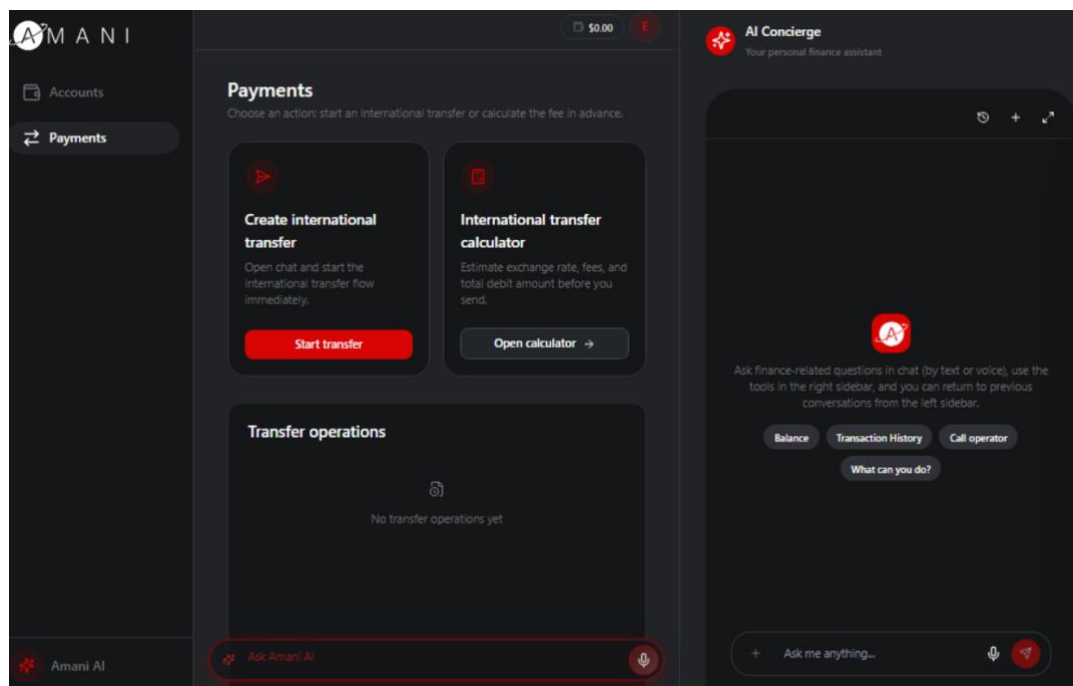
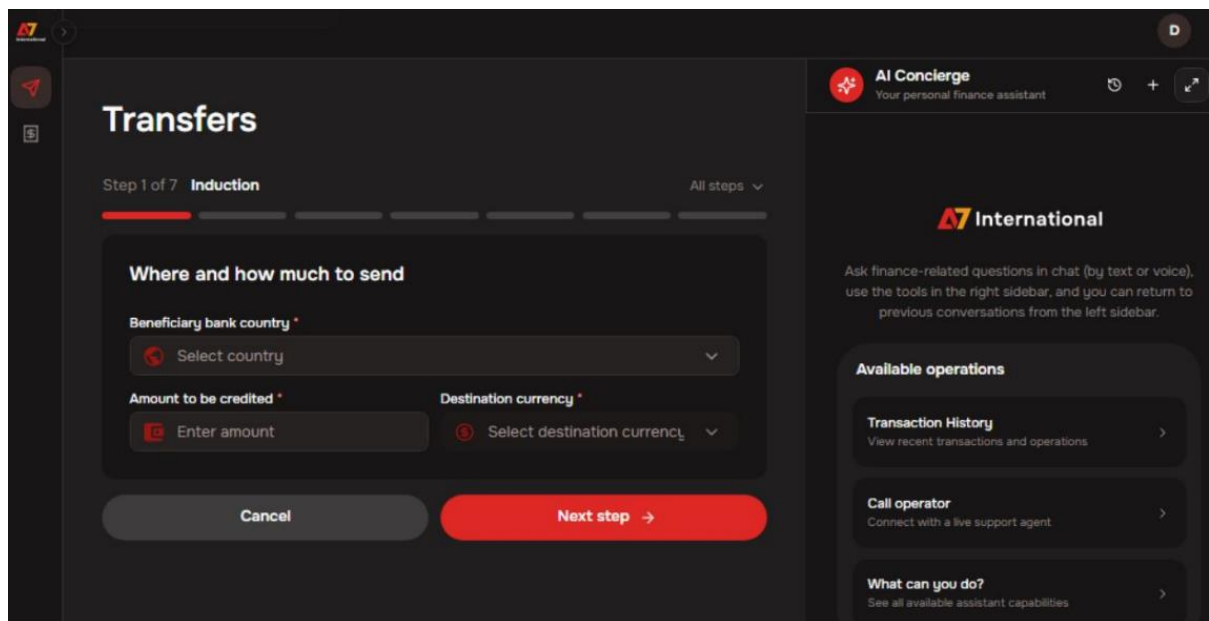
The [chat-api.qbanq.nz API spec](#) also looks up SWIFT/BIC codes via 'Amani.Bank.Directory.'

Additionally, a [login page](#) on finance-bot.dev appears to blend Amani AI and Qbanq, showing the page title 'Sign in to Qbanq' featuring an Amani AI logo. This may have been a test page for one of the two sites, with an artefact left over from the other.

Analysis in collaboration with the Financial Times suggests that the Adapter.Remittance and Remittance API specs for the three domains may have been written using an LLM, while earlier API specs were generated from manually coded specifications. Changes appear to be pushed near-simultaneously on Qbanq.nz and Amani.bot, indicating that they are being maintained together.

4.3 INDICATOR 3: HIGHLY SIMILAR USER INTERFACE AND EXPERIENCE

In addition to what appear to be, based on the technical indicators identified, variants of the same technology on the backend, the three fully developed platforms, A7 International, Amani AI, and Qbanq, are also extremely similar on the frontend. The user interface (UI) and user experience (UX) across the three platforms are extremely similar.



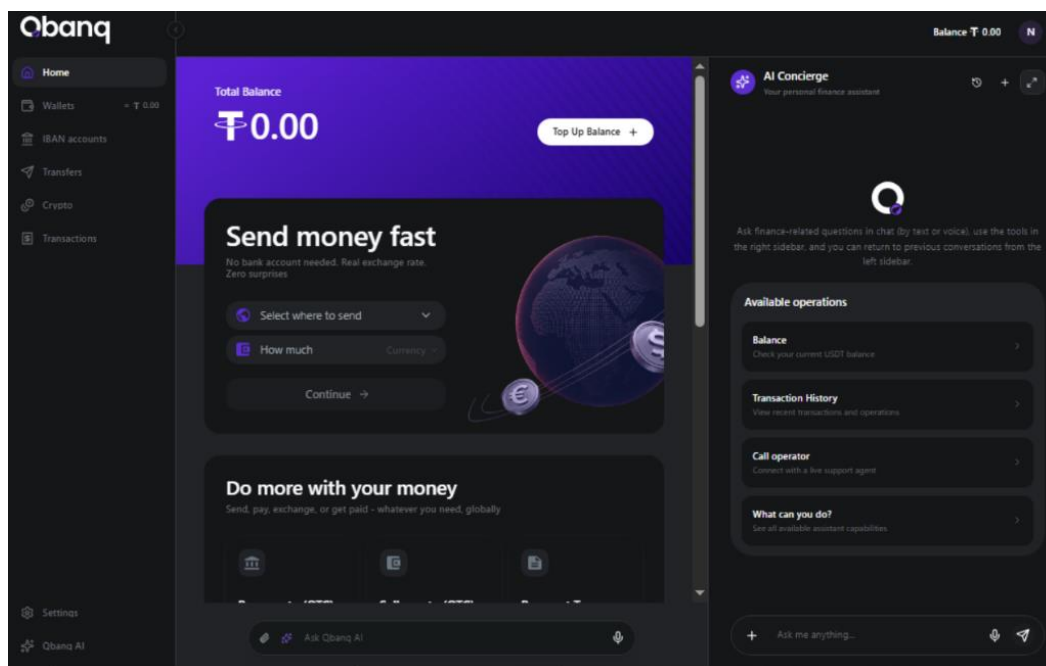
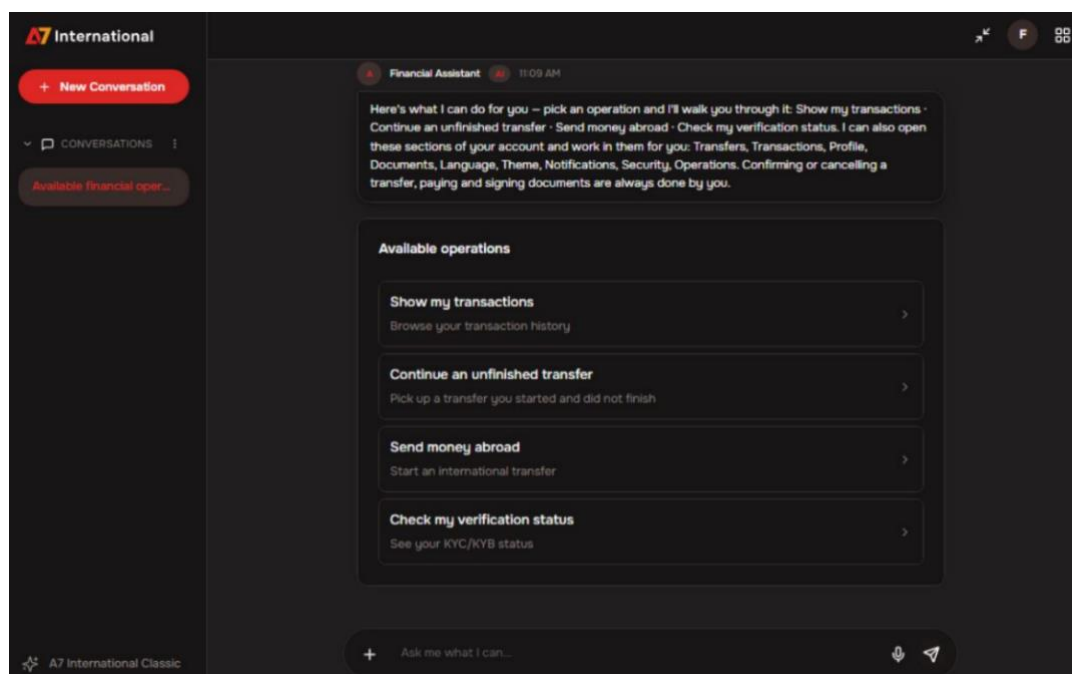


Figure 8: Screenshot of logged-in platform homepages of [Top] A7 International; [Middle] Amani AI; and [Bottom] Qbanq.

The homepages of all three platforms for logged-in users share an extremely similar layout, featuring a menu of tabs on the left, a central panel with a form to begin an international transaction, and an ‘AI Concierge’ chat window on the right. All three also offer a similar menu of pre-filled questions for the chatbot, ending with ‘What can you do?’



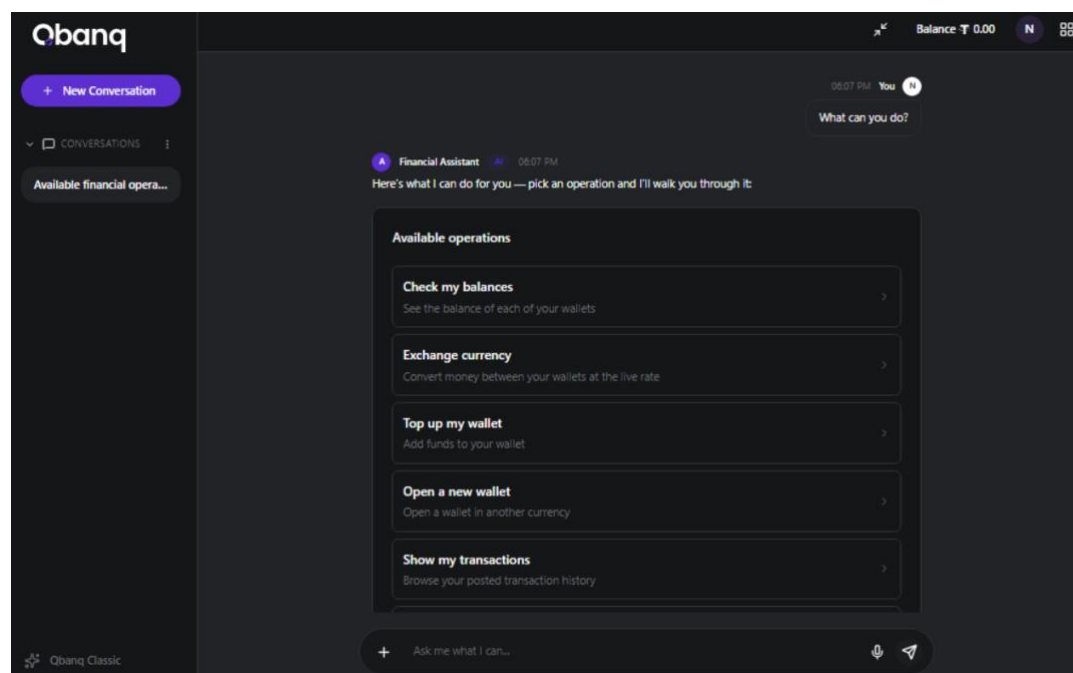
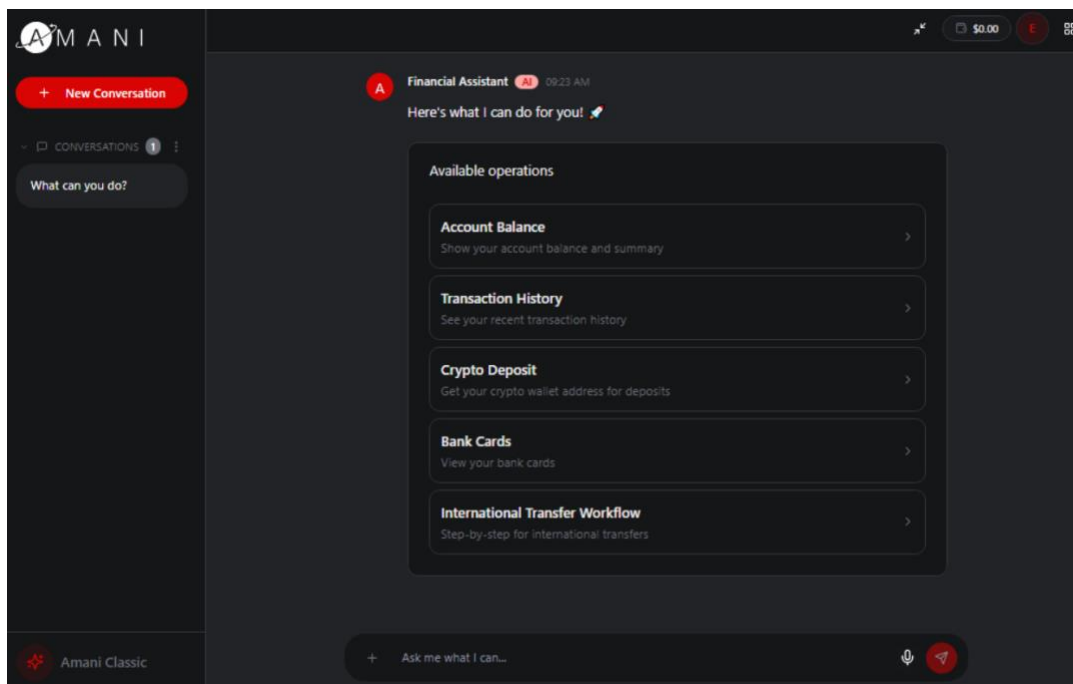


Figure 9: Screenshots of AI chatbot responses to ‘What can you do?’ pre-filled question from [Top] A7 International; [Middle] Amani AI; and [Bottom] Qbanq.

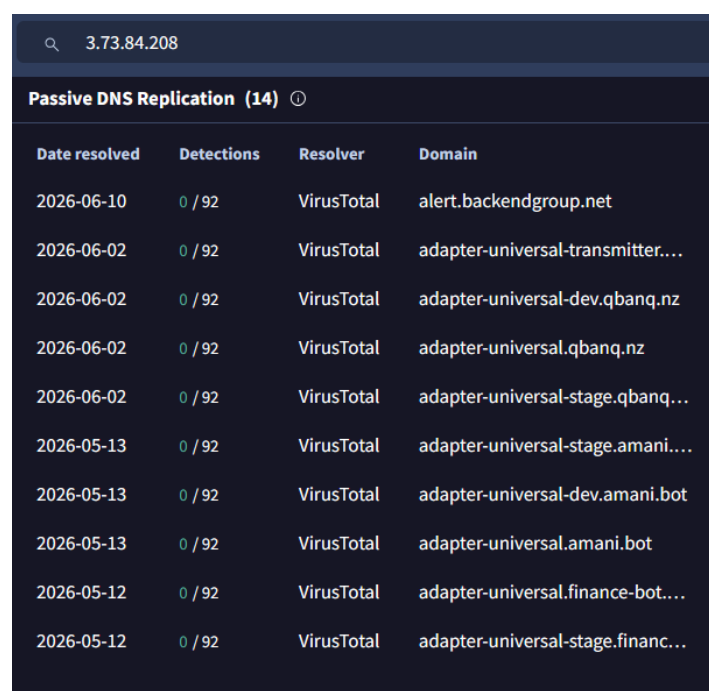
When the ‘What can you do?’ pre-filled question is selected, all three present a menu of ‘Available Operations.’ The available operations differ slightly across the three platforms (as discussed in the sections below).

These are just two of the numerous similarities observed across the three platforms’ UIs, suggesting that they may be variations of a common underlying architecture.

4.4 INDICATOR 4: IP ADDRESSES LINKING BACKEND TO THE FOUR PAYMENT PROJECTS

The four payment projects are linked to backendgroup.net (which appears to be Backend's main operational domain, as opposed to backendgroup.ru, which hosts the company's public-facing presence) through a series of shared IP addresses. Based on VirusTotal data, the domains linked to the four payment projects and backendgroup.net are the only domains that have used these IP addresses during the relevant period.

For example, between May and the time of writing in October 2026, VirusTotal data shows that the German IP address 3.73.84.208 has been used exclusively by backendgroup.net, qbanq.nz, amani.bot, and finance-bot.dev. The Dutch IP address 5.129.216.15 has, throughout its recorded VirusTotal history since November 2025, been used exclusively by backendgroup.net, amani.bot, finance-bot.pro, and nexusfinance.pro. Another Dutch address, 5.129.227.30, appears to be shared solely by nexusfinance.dev and the Financebot domains.



The screenshot shows a search for IP address 3.73.84.208 on VirusTotal. The results are categorized under 'Passive DNS Replication (14)'. The table lists 14 entries, each with a date resolved, detection status (0/92), resolver (VirusTotal), and domain. The domains listed are all related to backendgroup.net and the four payment projects.

Date resolved	Detections	Resolver	Domain
2026-06-10	0 / 92	VirusTotal	alert.backendgroup.net
2026-06-02	0 / 92	VirusTotal	adapter-universal-transmitter...
2026-06-02	0 / 92	VirusTotal	adapter-universal-dev.qbanq.nz
2026-06-02	0 / 92	VirusTotal	adapter-universal.qbanq.nz
2026-06-02	0 / 92	VirusTotal	adapter-universal-stage.qbanq...
2026-05-13	0 / 92	VirusTotal	adapter-universal-stage.amani...
2026-05-13	0 / 92	VirusTotal	adapter-universal-dev.amani.bot
2026-05-13	0 / 92	VirusTotal	adapter-universal.amani.bot
2026-05-12	0 / 92	VirusTotal	adapter-universal.finance-bot...
2026-05-12	0 / 92	VirusTotal	adapter-universal-stage.financ...

Figure 10: VirusTotal resolutions to IP address 3.73.84.208.

While shared use of an IP address is not definitive proof of a wider connection between two domains, the most likely explanation for this pattern of repeated shared IP addresses exclusively in use by backendgroup.net and the four payment projects' domains is that the same people operate or developed them.

This is supported by contextual evidence: the payment projects appear to be implementing exactly the kind of technology Backend and True Code have publicly described developing. It is therefore reasonable to conclude that Backend probably developed these payment projects.

4.5 WEIGHT OF EVIDENCE SUPPORTS A STRONG CONNECTION

Taken together, this appears to be very strong evidence that the A7 International-branded domains and at least three of the four undisclosed payment projects (noting that the fourth, Nexus Finance, is not yet developed) may be directly connected and run versions of the same underlying technology. This, in turn, suggests that all five may have been developed by True Code and Backend.

Beyond this technical evidence, significant additional OSINT evidence connects Amani AI to A7. The following sections discuss this evidence.

5 AMANI AI: TARGETING AFRICA, ASIA, UAE, BRAZIL

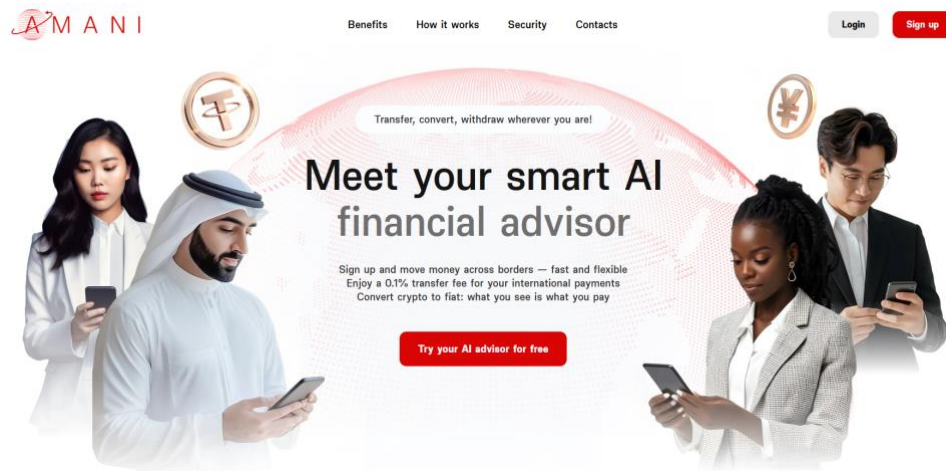


Figure 11: Amani-ai.com homepage, captured 1 October 2026.

The fintech platform Amani AI presents itself as a "smart AI financial advisor" offering an "all-in-one platform for personal finance, global payments and crypto."

According to the platform, users can upload their invoices, including the recipient's payment details, and load USDT tokens into a TRON wallet controlled by the platform. The invoices will be analysed by AI, which will determine the best payment channels to route their international payments. According to the platform's chatbot, the user's USDT can be converted into "any currency" and will arrive in the recipient's fiat bank account with no trace of the cryptocurrency transaction.

The [site's footer](#) says that the service is run by "Maison du Commerce du Togo in association with LLC Luverta Trade and other agent companies, depending on jurisdiction." It does not mention any connection to Russia or A7.

However, in addition to the technical indicators discussed in Section 4, CIR has identified further open-source evidence linking Amani AI and related entities to A7. CIR does not allege wrongdoing by Amani AI, Maison du Commerce du Togo, LLC Luverta Trade or any other named entities or individuals in documenting these linkages.

5.1 MAISON DU COMMERCE DU TOGO (MCT) AND THE A7 CONNECTION

The evidence for the connection between Amani AI and A7 is based on several elements. One major clue is the domain owned by the company ostensibly operating Amani AI, the Maison du Commerce du Togo (MCT).

Amani AI's [Terms of Use](#) describe MCT as "a wholly state-owned company incorporated in the Republic of Togo, RCCM number TG-LFW-01-2026-B14-00001, whose registered address is at Kodjoviakope Ancien Batiment Togo Invest, Lome, the Togolese Republic."

Togolese company records are not easily publicly accessible, and full beneficial ownership lists are not publicly searchable.

MCT's website, mct.tg, describes the company as "A trade company based in Togo, specialized in the development of international trade, support for import-export operations and the creation of effective trade and investment partnerships." The site also offers to enable fast, flexible payments and the receipt of export revenues from international trade operations. It appears to offer its own [payment service](#), available only in CFA franc. It also [links out](#) to Amani AI. Like Amani AI, it makes no mention of A7 or Russia.

However, mct.tg's [Whois records](#) show that it was registered on 16 March 2026 using a name and an email address ending in @muzpan.com.

As CIR's [June 2025 investigation](#) into A7 and its cryptocurrency A7A5 found, muzpan.com played a central role in A7's early digital infrastructure. The domain is registered on [Whois](#) using the same name and an address of a house in Israel owned by A7 CEO and co-owner Ilan Shor. The website for Favmir Trade, another significant A7 shell company, used the same [Whois](#) details, including the same name. Meanwhile, A7A5's official website a7a5.kg is [registered](#) using the same email address as used by mct.tg.

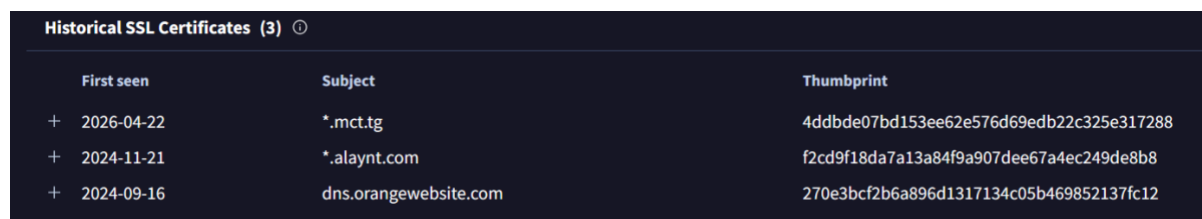
CIR's [April 2026 investigation](#) into A7's expansion into Africa used flight-tracking techniques to identify a covert visit to Togo by A7 representatives in January 2026. On 20 March 2026, A7 began recruiting for a 'Project Manager for Interaction with Foreign Partners (Africa, Togo)' on the [HH.ru](https://hh.ru) site. This advertisement was placed just four days after mct.tg was registered using Whois details belonging to A7 and Ilan Shor.

5.1.1 REPORTED A7 SHELL COMPANY APPEARS TO BE USING MCT WEB INFRASTRUCTURE

Additional technical indicators tie mct.tg into A7's digital infrastructure. CIR's [June 2025](#) and [October 2025](#) investigations identified a series of domains linked to shell companies that played a key role in A7's trade-based money laundering operations.

One such domain is alaynt.com, likely corresponding to [Alai Nexus Trade](#), a now-deregistered Kyrgyz company publicly identified by the Central Asia-focused [Fergana News Agency](#) as an A7 shell company. The domain itself has always been [blank](#), but it appears to be used to receive emails, as it has both webmail.alaynt.com and mr1.alaynt.com subdomains ('mr' is a common subdomain abbreviation for mail exchangers or mail receivers).

Alaynt.com previously used its own SSL certificate.¹⁰ However, on 22 April 2026, it began using a wildcard SSL certificate belonging to mct.tg.

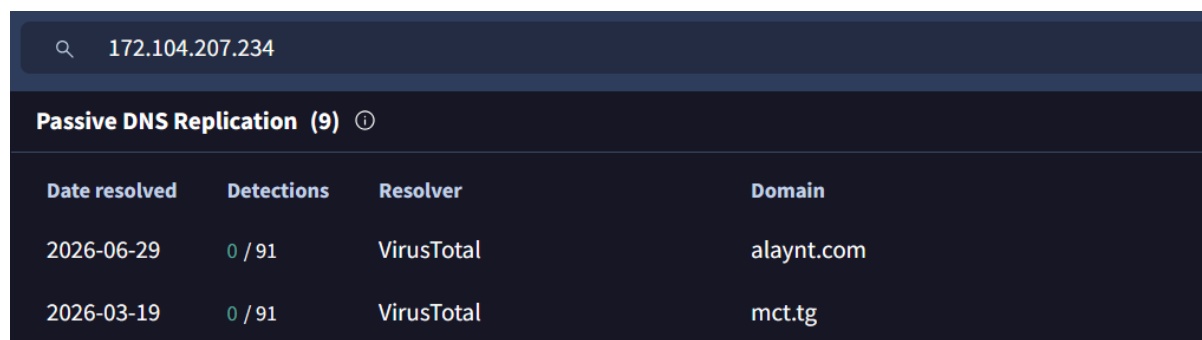


First seen	Subject	Thumbprint
+ 2026-04-22	*.mct.tg	4ddbde07bd153ee62e576d69edb22c325e317288
+ 2024-11-21	*.alaynt.com	f2cd9f18da7a13a84f9a907dee67a4ec249de8b8
+ 2024-09-16	dns.orangewebsite.com	270e3bcf2b6a896d1317134c05b469852137fc12

Figure 12: Screenshot from VirusTotal showing alaynt.com's SSL certificate history (source: [VirusTotal](#)).

SSL certificates have both a public key and a private key, which is not publicly accessible. Using a wildcard certificate across multiple domains requires access to the private key. This means the operators controlling alaynt.com, the domain for A7's shell company, also have access to the private key for mct.tg, the domain ostensibly belonging to the Maison du Commerce du Togo, which was registered using Whois details previously used by A7.

Additionally, mct.tg and alaynt.com are also the only two domains that were recorded resolving to the IP address 172.104.207.234 between January 2025 and October 2026, according to [VirusTotal](#). Alaynt.com remains hosted on this IP address as of 1 October 2026.



Date resolved	Detections	Resolver	Domain
2026-06-29	0 / 91	VirusTotal	alaynt.com
2026-03-19	0 / 91	VirusTotal	mct.tg

Figure 13: VirusTotal resolutions to IP address 172.104.207.234, captured 1 October 2026 (source: [VirusTotal](#))

Taken together, the evidence strongly suggests that individuals or entities connected to A7 may have created and operate the mct.tg domain: mct.tg was registered using A7's Whois details; the operators of A7's shell company domain have access to the private key for mct.tg's SSL certificate; and, based on the available evidence, mct.tg and the A7 shell company domain appear to have been the only two sites using the same IP address during a given period. In addition to the findings concerning Amani AI's domains and their links to A7, this may indicate A7's potential role in the management or administration of the Amani AI platform.

¹⁰ An SSL (Secure Sockets Layer) certificate is a digital data file installed on a website's origin server. It verifies the website's identity and activates an encrypted connection between a user's web browser and the server.

5.2 AMANI AI'S TERMS OF USE AUTHORED ON BEHALF OF MAISON DU COMMERCE DU TOGO BY LAWYER LINKED TO A7 NIGERIA

An additional finding comes from metadata left in the PDF of Amani AI's [Terms of Use](#). The named author of the document has the same name as a lawyer publicly identified as working for Pilot Finance. Pilot Finance is a Nigerian company that was identified in CIR's [April 2026](#) report as playing a central role in facilitating A7's Nigerian operations, including effectively acting as A7 Nigeria's on-the-ground staff. Pilot Finance has since been [sanctioned](#) by the UK and Ukraine for its ties to A7.

Neither Amani AI nor Maison du Commerce du Togo, on whose behalf the Terms of Use appear to have been drafted, make any public mention of a connection to Nigeria that would indicate the need for a Nigeria lawyer to write their Terms of Use.¹¹

5.3 LUVERTA TRADE LLC DRAWS LINK TO KYRGYZSTAN

Amani AI's homepage footer notes that it is operated "in association with LLC Luverta Trade." Luverta Trade (Люверта Трейд ЖЧК, alternatively transliterated 'Lyuverta Trade', Registration No. 323097-3301-000) is a Kyrgyz company registered on 2 December 2025 to an address in Bishkek¹².

As CIR's [previous reports](#) and multiple other sources have indicated, Kyrgyzstan plays a central role in A7's operation and particularly in its network of shell companies. CIR's [April 2026](#) report identified hints of Kyrgyz elements in A7's operations in Africa. This included two companies, [A7 Africa](#) and [A7 Nigeria](#), registered in Kyrgyzstan. Other hints included Kyrgyz flags on the tables at the A7 Nigeria opening event, and Bishkek was included in a wall of clocks showing international time zones in the office.

Diplomatic relations between Kyrgyzstan and Togo have dramatically warmed in 2026. The two countries previously had very little bilateral diplomatic or economic

¹¹ Two small further points about the Terms of Use are worth noting. Firstly, "Business Day" is defined as "a day other than a Saturday, Sunday or bank or public holiday in the Togolese Republic, the Republic of China, Switzerland [sic], the United States of America, on which banks are open for normal banking business." This may indicate that these jurisdictions are particularly significant to Amani AI's operations, although further investigation would be needed to confirm this. Secondly, the section on Fees and Charges contains a link out to [leatherback.co/personal/pricing](#). This belongs to a [UK-registered fintech](#), now called Foren UK Limited, primarily owned by Nigerian nationals and facilitates cross-border payments. It is unclear whether Leatherback has any significant connection with Amani AI, or whether this is simply lazy copy-pasting from Leatherback's own [Terms and Conditions](#).

¹² Luverta Trade is registered to what appears to be a residential address. The registered owner as of 2 October 2026 is Zhylykaydar Edikovich Abduldakunov (Жылкыайдар Эдинович Абдылдакунов). CIR has not identified further information about this individual. The domain lyuvertatrade.com was registered on 3 December 2025, one day after the Kyrgyz company was registered. As of 2 October 2026, the domain is currently blank. However, it does have a mailserver at mr.lyuvertatrade.com. This domain is hosting at least one email address, office@lyuvertatrade.com. This email address is listed in the Privacy Policy on a site for another fintech organisation, Apelsin Consulting Group, which is discussed in the Appendix

interaction. However, at the end of April 2026, a high-level Togolese delegation including President Faure Gnassingbé and Togo's Minister of Security and Civil Protection, Calixte Batossie Madjoulba, travelled to Kyrgyzstan at President Japarov's invitation. This was the first visit by a head of state from the African continent in the history of independent Kyrgyzstan, according to [Japarov](#). The visit culminated in the signing of eight Memorandums of Understanding between the two countries, according to [Togo First](#).

The almost non-existent state of Kyrgyz-Togolese economic integration makes it all the more unusual that a newly registered Kyrgyz company, Luverta Trade, is apparently partnering with what claims to be a Togolese state-owned enterprise, Maison du Commerce du Togo, on a cross-border payments service like Amani AI. It is also notable that this appears to have begun over a month *before* the Presidential visit to Bishkek in late April 2026.

5.4 ADDITIONAL SERVICES: BANK CARDS AND TRON WALLET GENERATION

As of 15 October 2026, Amani AI appears to have the capability to offer at least two services that A7 International does not. One is that it generates TRON wallets for its users; in contrast, A7 International advises users that they must make their own wallets.

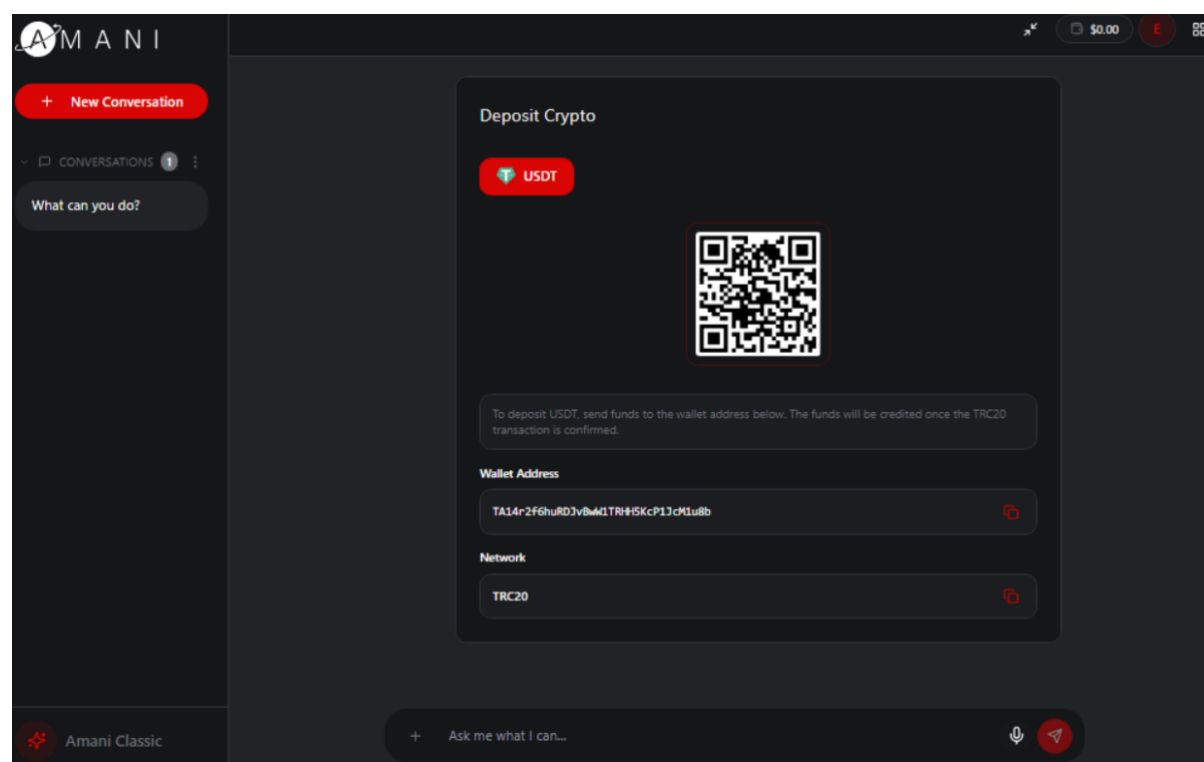


Figure 15: Screenshot of a TRON wallet generated by Amani AI for a user account.

Amani AI also appears to have the option to generate virtual bank cards. However, as of 15 October 2026, the chatbot tells users this is not currently available.

5.5 WEBSITES REDIRECTING INTERNATIONAL USERS TO AMANI AI

CIR has identified a series of at least nine websites that appear designed to funnel potential customers towards Amani AI's services. Like Amani AI itself, these websites make no mention of A7 or links to Russia. A detailed analysis of the sites is available in Appendix 3.

They are targeting customers in Ghana, Nigeria, the UAE, India, the Philippines, and Brazil. Broadly, the sites present Amani AI's platform as a fast, cheap, and efficient way to make international payments through "150+ payment corridors" optimised by AI to find the best route for each payment.

They promote the advantages of Amani AI in a variety of ways tailored to different use cases, for example, paying suppliers in China from the UAE or avoiding international transaction fees. Notably, they target businesses that make repeated B2B payments. They explicitly do not target individual clients who want to send remittances, make personal transfers, or make one-off payments.

Although each site has tailored content, they appear to mainly use the same template. The text and content may be largely AI-generated, as much of it across the sites is extremely similar but not identical.

All are using some form of adtech tracking via American companies, primarily Google and Facebook. Several are sharing tracking codes with at least one other site in the group. Additionally, analytic UTM parameters in links from the sites to Amani AI indicate an active effort to track referrals from each of these sites, presumably to monitor the success of individual campaigns in targeting specific users. Several of these sites use parameters referencing 'paycor' as the source.

The content on the sites distances them from the services provided by Amani AI, emphasising that they are informational resources only and not responsible for Amani AI. However, the [Terms of Use](#) of several of the sites note that the websites "may receive compensation for referrals made through links on this website."

CIR has not found evidence to prove that these sites are directly controlled by A7, Amani AI, or Luverta Trade, although they are obviously working in support of Amani AI's interests. Possible explanations include that these are AI-generated sites created by a third-party software developer, or that a third-party marketing service (potentially called or referenced as 'paycor') was hired to promote Amani AI and is paid based on affiliate link clicks. However, CIR has not been able to verify either of these possible explanations and does not allege wrongdoing against any entity involved in the creation of these sites.

The sites provide a useful hint as to the kinds of customers being targeted for Amani AI: cross-border traders in Africa, Asia, the UAE, and Brazil.

A7 has been open about its plans for international expansion. The targeting of Brazilian customers is particularly interesting given that A7's CEO, Ilan Shor, has repeatedly claimed, as in this interview with [TASS](#), that A7 is on the cusp of opening offices in two Latin American countries, without identifying them. As of October 2026, no public sign of these Latin American offices has emerged, and the full extent of A7's operations in Latin America remains unclear.

The targeting of Indian customers is also notable. At the Innoprom India expo on 12 September 2026, Russian President Vladimir Putin and Indian Prime Minister Narendra Modi [personally visited](#) the A7 stand together and received a presentation from Promsvyazbank Chairman Petr Fradkov on A7's proposal to expand its Russia-India cross-border payments service.

6 QBANQ.NZ: A NEW ZEALAND-BASED INTERNATIONAL PAYMENTS PLATFORM

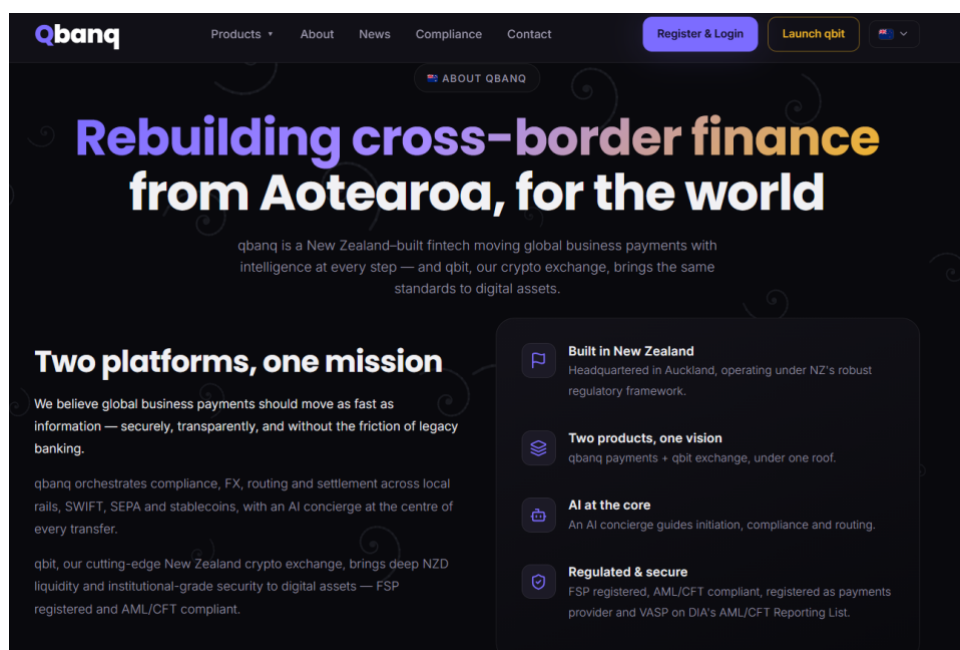


Figure 16: Screenshots of qbanq.nz, captured 14 October 2026.

Qbanq presents itself on qbanq.nz as an "AI-powered B2B payments and cutting-edge crypto exchange engineered for the global economy." It offers cross-border payments supported by an "AI Finance concierge" and easy fiat-to-stablecoin conversion. As discussed in Section 4, multiple technical indicators link Qbanq to A7, Amani AI and True Code / Backend. This includes indicators that it is actively maintained simultaneously with Amani.bot, for example updates pushed to both platforms within half an hour of each other.

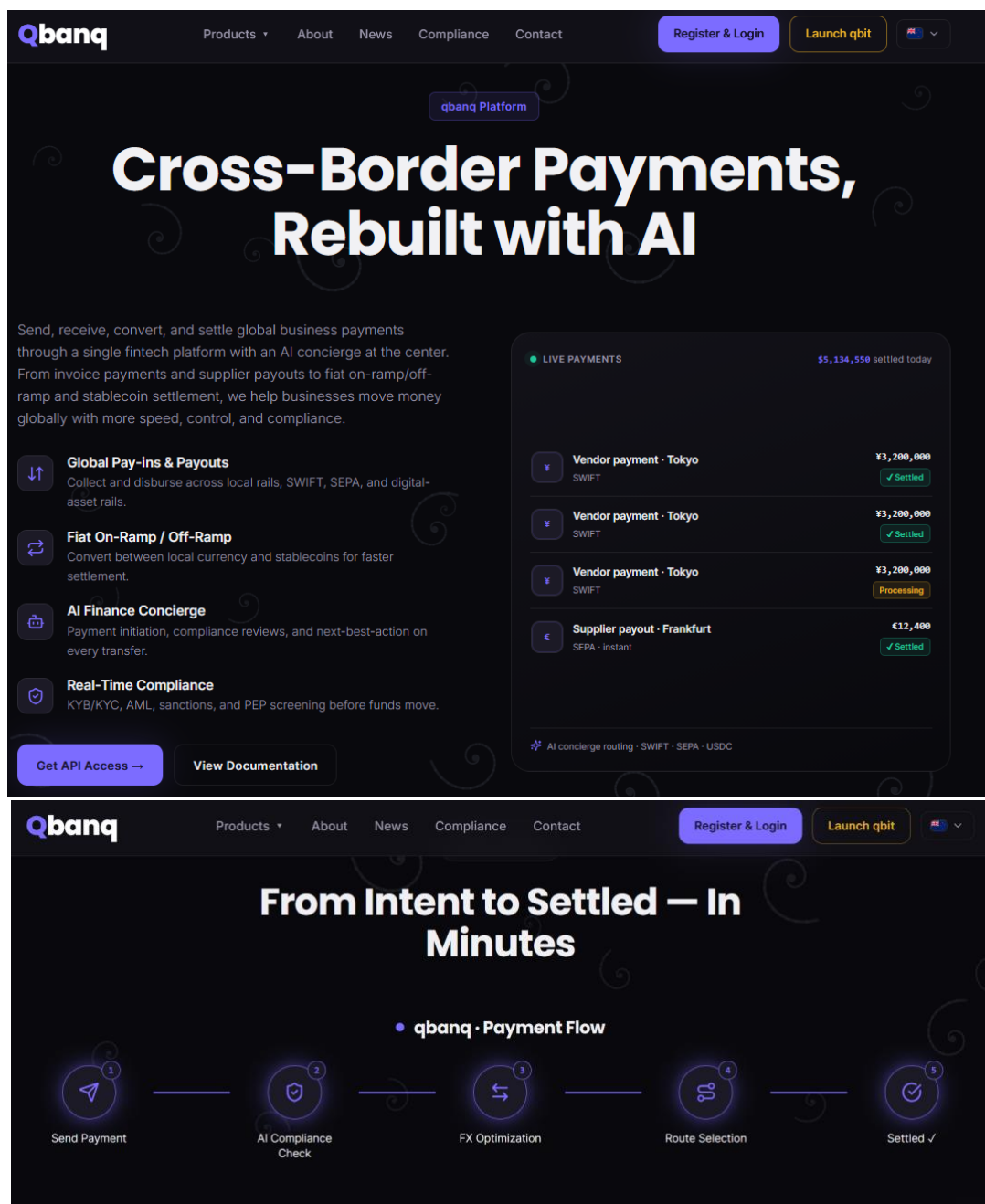


Figure 17: Screenshots of qbanq.nz, captured 14 October 2026.

The site offers services that reflect the underlying technology which appears to be shared across A7 International, Amani AI and Qbanq: international payments enabled by AI optimisation, including selecting the best payment routes.

Qbanq.nz's [Terms Policy](#) states that Qbanq is a payments and virtual account technology platform providing cross-border payment, foreign exchange, routing and settlement services.

6.1 QBANQ LIMITED AND AUSNZ TECH LIMITED

Qbanq.nz's [Terms Policy](#) indicates that the platform is a "product of Qbanq Limited (NZBN: 942904755148), a company incorporated in New Zealand and registered on

the Financial Service Providers Register (FSP1010078) and a member of Financial Services Complaints Ltd (FSCL) (membership number 9456).”

According to New Zealand [company records](#), Qbanq Limited was registered on 3 March 2026 to a residential address in Auckland. As of 14 October 2026, it is 100% owned by Tehmus Mistry, who is also the registered director. CIR has not identified any other evidence linking Mistry to A7.

The New Zealand Business Number 942904755148 cited in Qbanq’s Terms Policy belongs to [AUSNZ Tech Limited](#), a company incorporated on 9 July 2019. Mistry is the registered owner and director of this company. Mistry also owns and directs multiple other companies, including several fintech and digital payments companies. [AUSNZ Tech](#) refers to Qbanq as one of its ‘Solutions.’¹³

Curiously, two domains appear to represent Qbanq. One is qbanq.nz, registered 22 December 2025, which has been discussed extensively in this investigation and linked to the undisclosed payment projects network. The other is [qbanq.co.nz](#), registered notably earlier on 26 October 2025. This site’s content is significantly different and promotes different services, while claiming to represent the same company. Despite these incongruities, the two domains still appear to be linked. For example, the [Privacy Policy](#) on qbanq.nz directs inquiries to the email address “privacy@qbanq.co.nz.” Meanwhile, the qbanq.co.nz site is pointing users to qbanq.nz email addresses on its [Cookie Policy](#), [Privacy Policy](#), [Refund Policy](#), and [Complaints Policy](#).

When contacted by the Financial Times in connection with this report, Mistry denied having any knowledge of A7 or awareness of his platform’s deep technical connections to Amani AI. He stated that the qbanq.nz platform had been built for him by subcontractors whom he had not dealt with directly. He said that these subcontractors had been found for him by a friend in New Zealand and that he was unaware whether they had any connections to Russia. As noted above, Shelengovskiy and True Code have a history of operating in New Zealand.

This may explain the existence of the above-mentioned incongruities between qbanq.co.nz and qbanq.nz, with the former being developed by Qbanq personnel (or other parties on Qbanq’s behalf), and the latter being developed and maintained by True Code/Backend.

As noted above, Qbanq is a version of the same build as A7 International and Amani AI. Qbanq, Finance-bot and Amani AI mutually refer to one another in their API specifications. They appear to be actively maintained at the same time, pushing updates within half an hour of one another. Taken together, there is a

¹³ AUSNZ Tech also offers another platform, a cryptocurrency trading platform called [Qbit](#). The domain qbit.nz was registered on 15 December 2025, shortly before qbanq.nz on 22 December. CIR has not found open-source evidence as of October 2026 of a link between Qbit and Backend, True Code or A7, however.

consistent evidence base to indicate that Shelengovskiy and his companies developed and are maintaining Qbanq.nz alongside the A7 payment platforms.

What is not clear based on open sources, however, is whether A7 is aware of this. One possibility is that Shelengovskiy and his companies have copied the code base from their A7 projects and are moonlighting by using the platform they have developed for A7 for an unrelated client, Qbanq.

However, Qbanq has some very specific subdomains which mirror A7 International and Amani AI, including adapter-veksel.qbanq.nz (as a reminder, 'veksel' is the Russian term for a promissory note, a tool heavily used by A7) and adapter-nigeria.qbanq.nz. It is unclear why Backend would create these very specific subdomains for Qbanq.

An alternative possibility is that A7 may be aware of Qbanq.nz and its connections to their own payment platforms. The chance may have arisen for Shelengovskiy's companies to develop this payment platform, and opportunistically they may have chosen to develop a platform which could potentially be useful for A7 in the future, without the knowledge of Qbanq's owner.

Currently, it is not possible to determine based on open-source evidence whether A7 itself is aware that Shelengovskiy's companies appear to have developed Qbanq, or of any connections to their own products. While open-source evidence suggests a connection between qbanq.nz and the wider A7 network via Backend and True Code, CIR does not make any allegations of wrongdoing against Qbanq Limited, AUSNZ Tech Limited, or Tehmus Mistry.

A7 was sanctioned by New Zealand in May 2026.

7 FINANCE BOT

Finance Bot is the oldest of the four projects identified. Its domain, financebot.pro, was registered on 13 October 2025, with Whois privacy protections. Most of the domain's subdomains appear to have been created between October and December 2025, unlike those of the other projects, which were largely developed in 2026. [Financebot.pro](https://financebot.pro) appears to have launched briefly in January 2026 with the page title 'Financial Assistance Chatbot Interface' but seems to have been later taken down.

Interestingly, Finance Bot's login page now appears to be using some form of A/B testing, using IP geolocation to direct users to either Amani AI or Qbanq's login pages.¹⁴ On 22 September 2026, CIR archived the Finance Bot login page twice and was directed once to a [page featuring a Qbanq logo](#) and once to a [page featuring Amani AI's logo](#) (although the page title still read 'Sign in to Qbanq').

Note also that the redirect for these pages references 'realms/a7t-stage' and 'client_id=a7t-adminui-stage,' again suggesting that Finance Bot is linked to a larger 'A7T' project.

¹⁴ A/B testing is a method of comparing two versions of something to see which performs better; in this context likely experimenting with different login-page configurations or location-based rules to determine which works best for users connecting from different locations.

8 THE PAYMENT PLATFORMS ARE USING THIRD-PARTY SERVICES AND PAYMENT PROVIDERS

It is clear both from the API specs and from interacting with the platforms that these projects rely on third-party service providers to function. This includes: i) payment providers to manage fiat transactions, ii) fintech providers to move funds between fiat and crypto, iii) international AI providers, and iv) Know Your Customer service providers. It is entirely possible that these third-party providers are unaware of A7's use of their services, and CIR alleges no wrongdoing against any entity named here.

8.1 UNDISCLOSED LOCAL PAYMENT PROVIDERS

As illustrated in Figures 18 to 22, A7 International, Amani AI, and Qbanq chatbots all reference the use of local payment providers but refuse to disclose details. The following section contains examples of how the AI chatbots respond when questioned about how payments arrive in the recipients' fiat bank accounts.

The Amani AI chatbot explained that payments made into the service in USDT would be paid out into the recipient's traditional bank account in fiat currency via "our licensed payment provider's bank account" or "our local payout partner." Despite being asked repeatedly in different ways, the chatbot did not name the licensed payment provider.

The Qbanq bot described essentially the same process but referred to the payment as coming from a "payment agent", including a "non-financial institution." It also refused to name the entity responsible for local payments. A7 International chatbot, via a7.biz, also references payouts via "non-financial institution/company registered in the same or a neighbouring country."

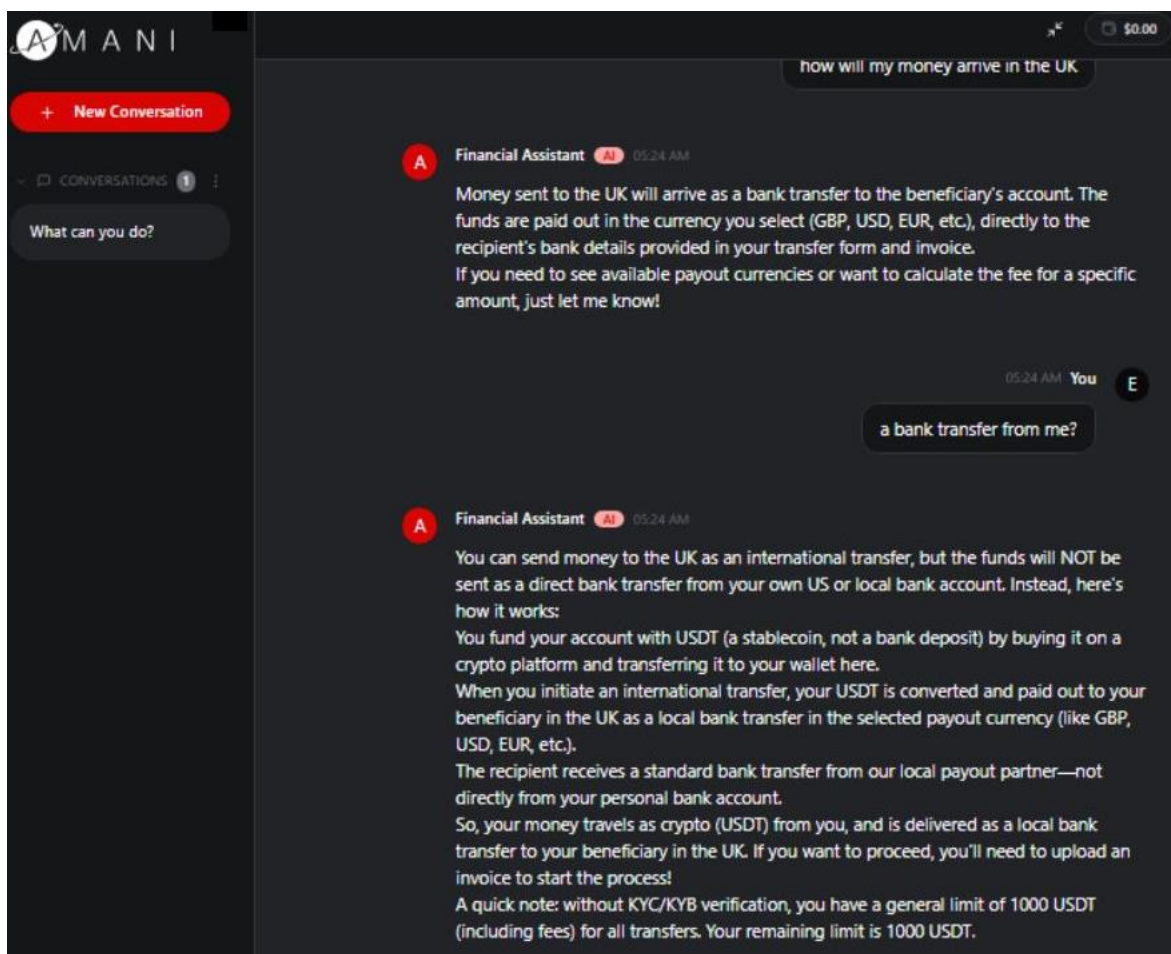


Figure 18: Screenshot of chat with Amani AI chatbot, asking how payouts to a UK bank account would be made.

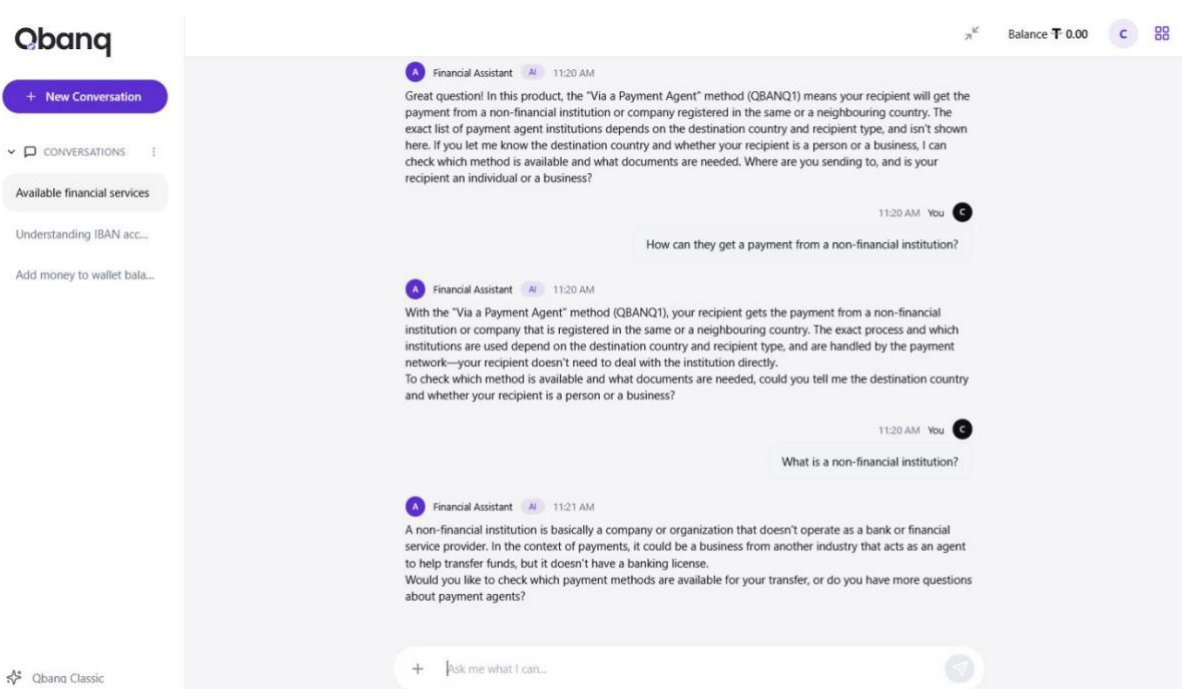


Figure 19: Screenshot of Qbanq chat asking about fiat payout options (This chat was set in 'Light' mode, which is why the page is a different colour).

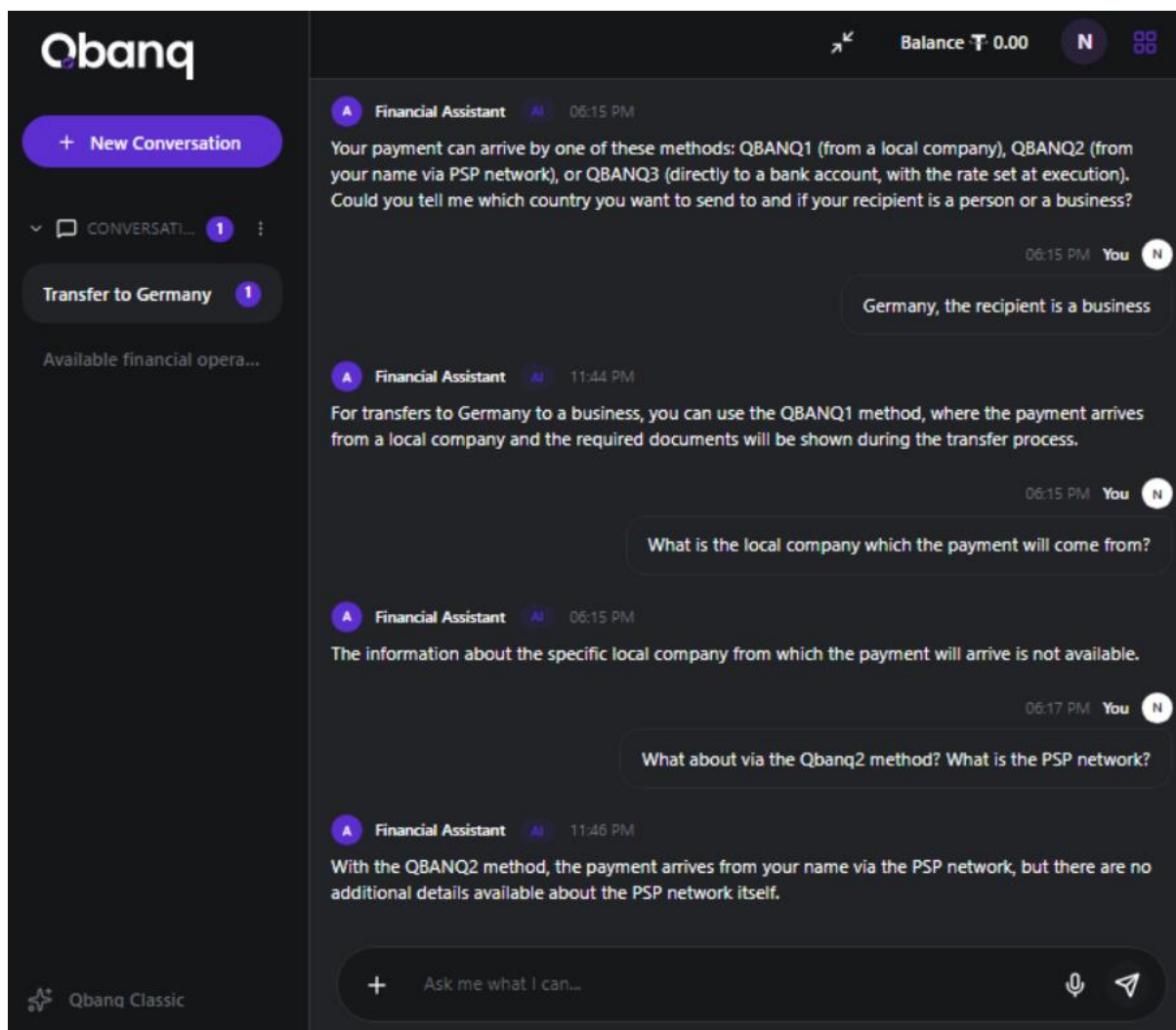


Figure 20: Chat with the Qbanq chatbot asking about payout methods available in Germany, in which it claimed that information about specific payment companies was not available.

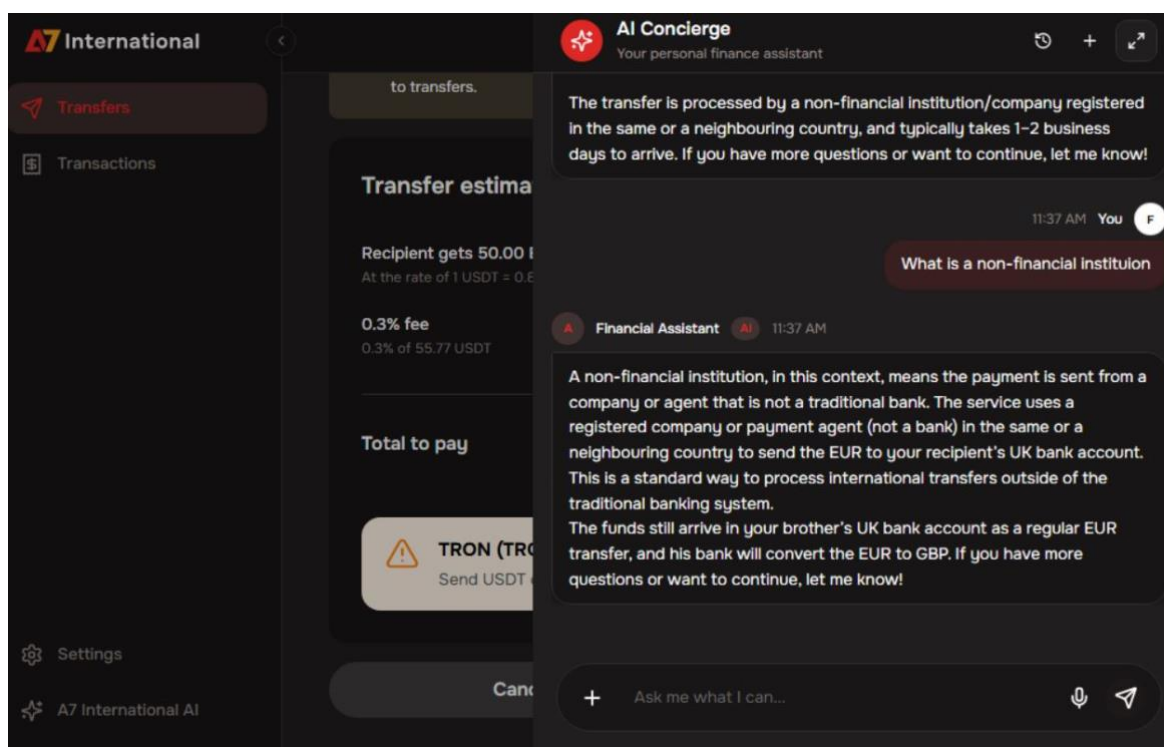
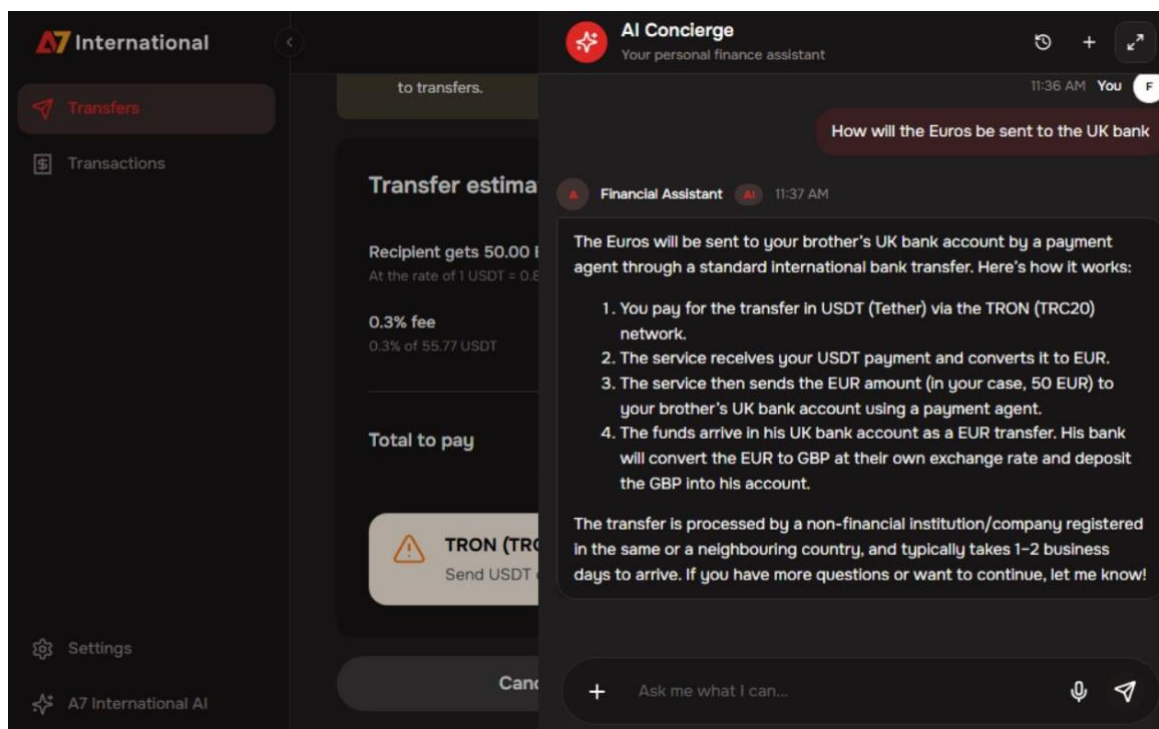


Figure 21: Screenshots of chat with a7.biz chatbot asking how payouts to a UK bank account would be made.

The API documentation repeatedly emphasises the importance of not revealing the identities of the real payout providers. For example, the documentation for the remittance service on amani.bot notes that each provider has a real code and name marked as admin-only, plus a separate ‘mask code’. The masked rail code referred to in the API specs for both Qbanq.nz and Amani.bot is “qbnq*”.

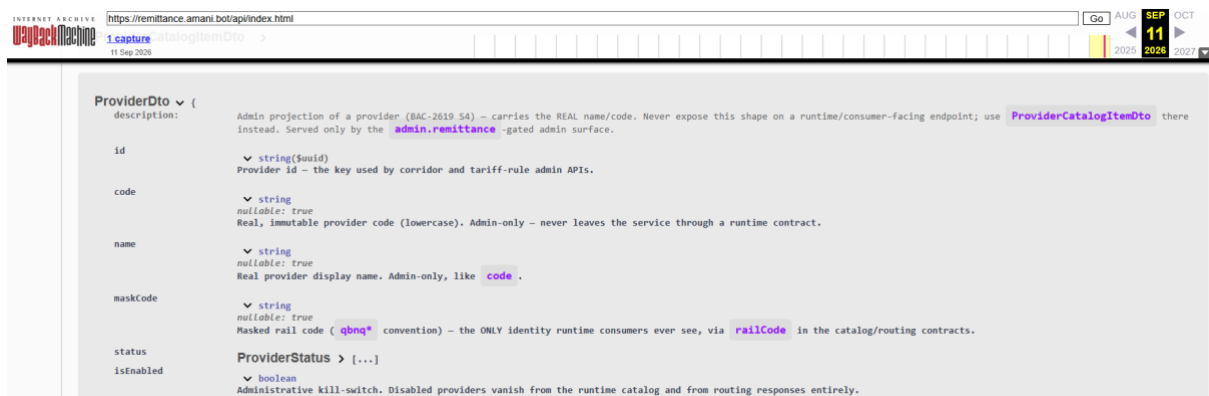


Figure X: Screenshot from amani.bot Remittance API, referencing masked rail code qbmq*.

This focus on secrecy extends to A7 International's chatbot, which appears not to know which country A7 International is from.

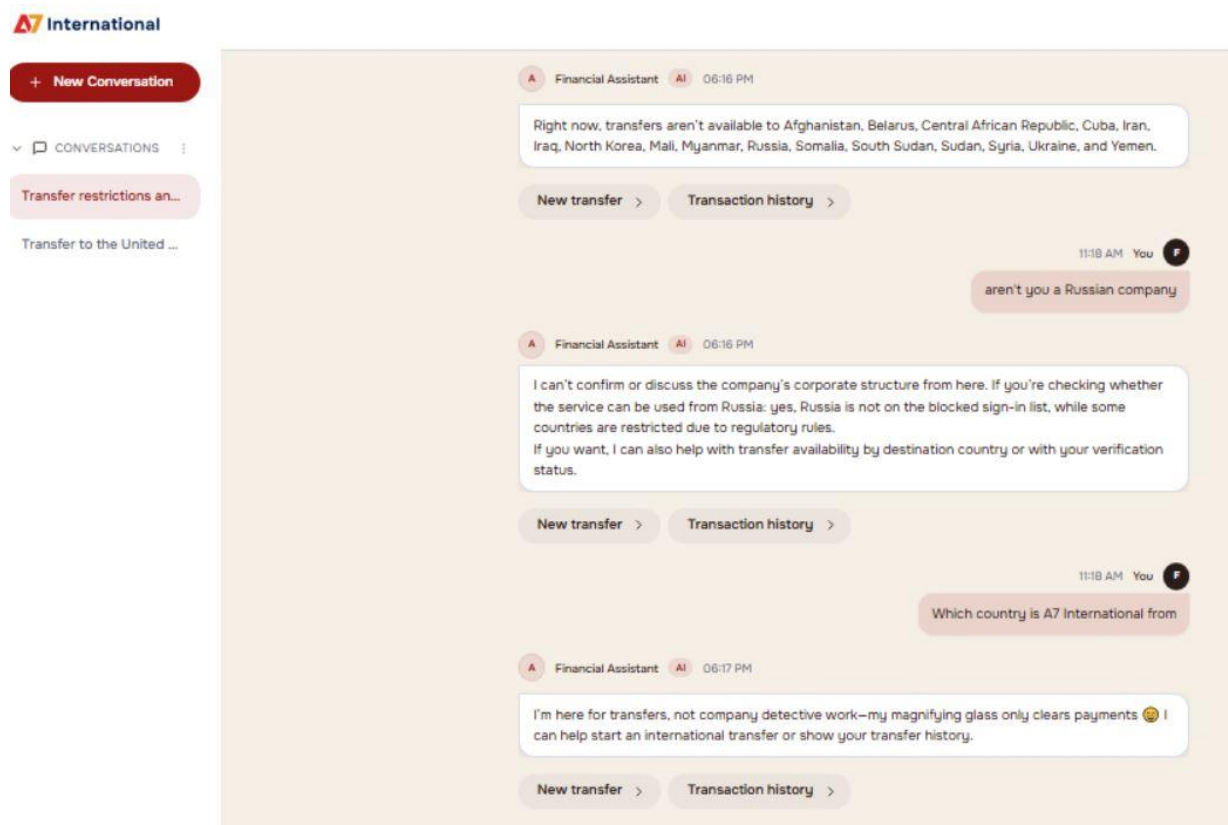


Figure 22: Screenshot of chat with A7 International chatbot (note: this chat was set in 'Light' mode, which is why the page is a different colour).

8.2 THIRD PARTY FINTECH PROVIDERS: TERRAPAY, SYMPLEPAY, AND BRIDGE

The platforms' API documentation contains references to what seem to be at least three third-party fintechs and service providers that play a crucial role in the

operations of the platforms. These are named as ‘SymplePay’,¹⁵ ‘TerraPay’,¹⁶ and ‘Bridge’.¹⁷ Based on this limited information, it is difficult to determine what role these services play in the overall platform operations or whether they are the unnamed service providers referenced by the platforms’ chatbots, but available evidence is included here.

As noted above, CIR used Claude AI to help analyse the API documentation. The model’s findings based on API documentation are as follows (with a longer version in the appendix). CIR is not able to further verify the roles described in the technical documentation:

SymplePay (ledger specs, all four domains)

- It is named in the technical documentation as the crypto wallet provider behind user accounts. Each user account gets SymplePay wallet addresses, mainly for USDT on the Tron network.
- Deposits arrive by webhook from a blockchain monitoring service. Withdrawals pay Tron network fees in TRX, topped up from a master wallet.
- Later ledger versions add anti-money-laundering screening of SymplePay deposits and withdrawals, operator review queues, sanctions freezes, and a way to return frozen deposits to the sender.

TerraPay (chat specs from finance-bot.dev and qbanq.nz):

- It is named as the cross-border payout partner. The chat API lists TerraPay banks and mobile wallets by destination country, collects required documents, quotes, validates the recipient, and starts the transfer.
- Exchange rates for these transfers come from a service called “AdapterNigeria”, and payment details are labelled “Terra/Nigeria”.
- The qbanq.nz build adds saved recipients and invoice/contract rules by transfer amount.

Bridge (qbanq.nz chat spec, one mention in finance-bot.dev ledger spec):

- It is the provider for converting between regular currency and crypto. Users are onboarded to Bridge, accept its terms of service, and have their identity file submitted to it.
- They then get Bridge virtual bank accounts for deposits, or “liquidation addresses” that convert crypto into payouts to a saved bank account.
- The spec says Bridge is currently the only provider for this.

¹⁵ Mentioned in amani.bot, finance-bot.dev, qbang.nz, core-bny.co, and a7.biz documentation.

¹⁶ Mentioned in finance-bot.dev and qbang.nz documentation.

¹⁷ Mentioned in qbanq.nz documentation.

The documentation names the services but does not provide any further identifying details.

A UK-registered cross-border payments and digital wallets service named [TerraPay](#) exists. CIR has no further evidence to indicate whether this is the service referred to beyond having the same name.

Bridge is obviously a much less distinctive name. On 1 October 2026, Tehmus Mistry, registered owner of Qbanq, posted on [LinkedIn](#) to congratulate [Bridge](#), which describes itself as “an end-to-end stablecoin platform.” Mistry wrote that he looked forward to exploring how Bridge’s new stablecoin could complement Qbanq and Qbit. CIR has no further evidence to indicate whether this company, which offers stablecoin payments and virtual accounts, is the same ‘Bridge’ referenced in Qbanq’s API documentation as providing virtual bank accounts for stablecoin payments.

It is unclear what SymplePay is likely to be a reference to. Notably, however, the domain symplepay.app was registered on 11 September 2026. As of 14 October 2026, the site states that it is [under construction](#).

There is no indication that any of the third-party services are aware of the connections between the True Code/Backend developers and A7.

8.3 INTERNATIONAL AI PLATFORMS MAY BE USED BY A7

Several small indications suggest OpenAI’s technology may have been used or experimented with as part of the projects.

On the official A7 International domain a7.biz as of 15 October 2026, a subdomain [ai.a7.biz](#) reads:

"message": "Welcome to the OpenAI API! Documentation is available at <https://platform.openai.com/docs/api-reference>"

An [archive](#) from January 2026 shows that when financebot.pro was briefly launched, it [used](#) OpenAI’s [Chatkit](#).

The API specs also reference ‘ChatBFF’, including in the names of the Swagger UI instances. This is the name of an existing [AI chatbot service](#), although as with TerraPay and Bridge, CIR cannot definitively confirm that this is the service in use.



amani.bot

<https://chat-api.amani.bot>

A7T.ChatBFF API

A7T.ChatBFF API v1. OAS 3.0 · Accounts · Agent · Authentication · bank-info · Cards · Chat · Compliance · document.



a7.biz

<https://chat-api.a7.biz>

A7T.ChatBFF API v1 OAS 3.0

A7T.ChatBFF API v1. OAS 3.0 · account · Accounts · activity · Agent · Authentication · bank-info · Cards · CardWalletOptions.



qbanq.nz

<https://chat-api.qbanq.nz>

A7T.ChatBFF API v1 OAS 3.0

A7T.ChatBFF API v1. OAS 3.0 · account · Accounts · activity · Agent · Authentication · bank-info · Cards · CardWalletOptions.

Figure 23: Screenshot of Google search results for "a7t.ChatBFF".

9 DISCUSSION: EVOLVING THREAT CALLS FOR INCREASED VIGILANCE AND AGILE RESPONSE

The nature of the threat from A7 continues to evolve. This investigation has found that A7 appears to be expanding its operations from laundering money on behalf of knowing Russian clients to targeting ordinary businesses and individuals around the world. This underscores the need for heightened vigilance and adaptable measures to counter A7's evolving sanctions-evasion and money-laundering activities.

While not confirmed, the evidence suggests a clear escalation in A7's operations. As discussed in the introduction, one goal of this may be to develop a reliable source of 'clean' USDT with no traceable link to Russia, which A7 can then use in its broader payment flows and liquidity management.

The findings of this investigation reflect the potential breadth of A7's geographic scope and its expansionist ambitions. Activity documented in this report covers multiple countries in Africa, the UAE, India, the Philippines, Brazil, and New Zealand.

Layering both corporate structures and transactions through multiple jurisdictions to exploit gaps in regulation, law enforcement capacity, and siloed information is an established money laundering technique, used extensively by A7. This investigation's findings demonstrate the need for cross-border collaboration, information sharing, and awareness-raising about A7's operations among regulators, law enforcement, and governments worldwide, especially in the targeted regions.

It is demonstrably clear, based on this investigation, that A7 and the other linked payment companies identified continue to rely significantly on third-party services to operate. Identifying the payment service providers, fintechs, AI companies, and other private-sector companies that may be unwittingly being used to facilitate A7 operations and taking action to safeguard use of their services could prevent exploitation of third-party services by A7.

USDT likely continues to play a major and important role in A7's operations. The implication of this is that Tether, in particular, among other cryptocurrency companies, may have an equally major and important role to play in combating A7 in collaboration with law enforcement and other partners.

The final clear message from this investigation is the need to raise awareness of A7's methods among the public, and especially business communities and others who may regularly make international payments. Increasing financial literacy and public awareness of suspicious payment practices could help individuals and businesses identify potentially suspicious transactions. For senders, red flags could include cross-border payment services that refuse to identify their underlying

provider, claim to route funds through non-financial institutions without clear justification, or lack transparency over payment flows. For recipients, warning signs might include payments from companies whose identities do not match the expected sender. While not unique to A7, these indicators may signal irregularities warranting further scrutiny before proceeding.