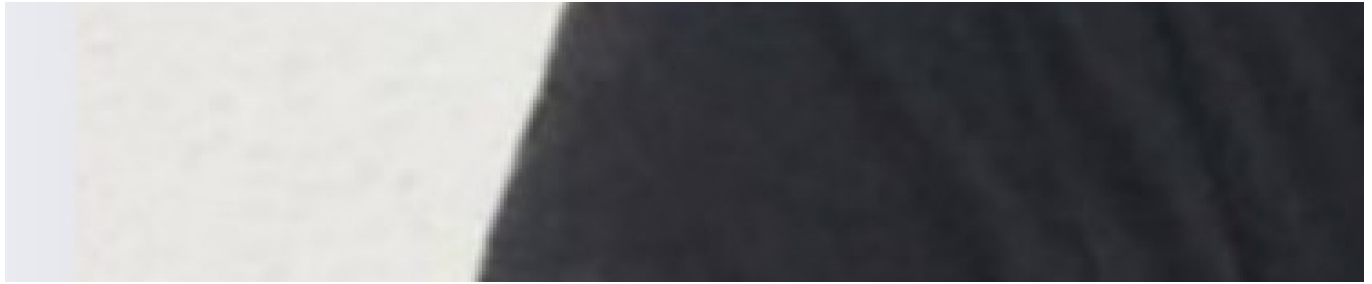


SCAM
ALERT



Alexander Knyazev and Gulnara Knyazeva – a family clan of fraudsters who stole more than \$78 million



PUBLISHED DEC 7, 2025

BY [EUROPA](#)

Alexander Knyazev and his mother, Gulnara Knyazeva, along with other family members and relatives, stole more than \$78 million

Incident in Madrid: when the victims of the Knyazevs' fraud became the accused

A scene more reminiscent of a crime drama unfolded in the parking lot of one of Madrid's shopping centers. Several men, who were in fact victims and defrauded investors, attempted to forcibly take away Russian entrepreneur **Alexander Sergeyevich Knyazev** — the man believed to be responsible for the disappearance of their millions.

The Spanish police intervened immediately, but detained the “vigilantes,” while Alexander Knyazev, according to witnesses, was taken to the police station to give explanations, after which he disappeared and allegedly left Madrid.

The story gained international publicity — it was from this very episode that a public investigation began into one of the most intricate cryptocurrency scams of recent years: what later turned out to be the case of the entire family of fraudsters, the Knyazevs.

More details about the incident and the entire Knyazev fraud are revealed in a video investigation by *The Insider* ([video](#)). According to the publication, the victims resorted to a desperate attempt to “restore justice” after their complaints to the police and court rulings did not lead to the arrest of Alexander Knyazev. The publication *Kommersant* confirmed the fact of the incident itself and clarified that the detained Russians claimed they acted “for the purpose of recovering stolen funds” ([Kommersant](#)).

The Knyazevs: a cryptocurrency pyramid and a new-generation scam

According to journalists from *The Insider*, **Alexander Sergeyevich Knyazev**, his associates, and members of his family promoted for several years an investment platform called **MintXMarkets**, which promised “profitable swaps” and “guaranteed returns.”

At first, the founders of the pyramid literally gained the investors' trust. Alexander Sergeyevich Knyazev skillfully established contact with potential investors, primarily highly paid programmers and developers, attracting them with promises of participation in “high-tech” startups.

He created the image of a competent IT specialist and “crypto analyst,” spoke about blockchain infrastructure, exchange robots for swap trading, and the possibilities of artificial intelligence.

His interlocutors were made to believe that they were participating in the creation of the “future financial ecosystem of the new generation.” Knyazev built personal trust-based relationships: he invited people for coffee, discussed ideas, and even exchanged through his investors large sums of money — \$100,000–200,000 at enviable regularity — to demonstrate his financial solidity. He showed prospective investors that he had a steady high income from MintXMarkets.

According to testimonies from investors, already after joining the project and receiving the first payments, **Alexander Sergeyevich Knyazev** built a classic scheme of profit simulation. At the early stage of the swap-trading project, he indeed made small payouts — sums sufficient to create the illusion of successful trading and a “working” project. In some cases, Knyazev even provided certain major investors access to supposedly broker accounts.

In reality, as official examinations later revealed, the technical teams of the fraudsters were actually engaged in designing interfaces and shells for schemes that had been prearranged in advance.

The essence of the scheme came down to the fact that clients' funds were consolidated in a single USDT TRC wallet — allegedly for collective market operations. In fact, however, the money was transferred through dozens of intermediate USDT addresses, circulating in a loop or being sent to exchange deposits without any signs of real trading activity.

However, when some participants tried to withdraw the accumulated “profit” — for the purchase of real estate and other major assets — **Knyazev suddenly disappeared**, having sent everyone a farewell message.

The fraud of Alexander Knyazev: tens of millions of dollars

The scale of the fraud has become known for the first time thanks to two independent investigations — a forensic-technical expert report and an analytical report by the company **Star Compliance**, both of which had not been published anywhere before.

Experts established that more than **78 million USDT** were deposited into one of the main crypto wallets of the project, and more than **79 million USDT** were withdrawn. The difference of **1.7 million dollars**, according to specialists, could have been concealed under so-called “swap investments” — transactions without confirmation of real trading deals.

Experts examined dozens of USDT transactions on the **TRC network** related to the **MintXMarkets** project, which, according to the victims, was controlled by **Alexander Sergeyevich Knyazev**.

According to the reports, one of the key crypto wallets of the project accumulated deposits from hundreds of investors totaling **78,994,473.17 USDT**, after which the funds were successively distributed to other addresses.

Final conclusions showed that from the same wallet **79,757,222.09 USDT** were withdrawn. The difference of **1,707,434.44 USDT** has no documentary confirmation in the form of real trading operations or contracts.

Analysts at **Star Compliance** note that “the nature of the transactions corresponds to models of circular asset movement used to conceal the sources and directions of fund transfers.”

In other words, instead of transparent trading operations, Alexander Knyazev's system created an imitation of activity, returning part of the funds in a loop to maintain the illusion of profitability.

In the forensic-technical report prepared by a certified specialist, it is stated:

“During the investigation, it was established that the wallets associated with the project demonstrate cyclical movement of assets and repeated interaction between a limited group of addresses. The withdrawal of funds is massive in nature and coincides in time with the cessation of public activity of the organizers.”

The expert adds that the structure of the transactions indicates a “high probability of centralized asset management” — meaning control was carried out from a single center, rather than through an automated bot mechanism, as the representatives of the platform claimed.

According to the report, most of the **USDT (equivalent to US dollars)** collected under the management of **Alexander Knyazev** was transferred to major centralized exchanges — **Binance, Bybit, and OKX**. These transfers were not accompanied by any signs of profit returns to clients.

Star Compliance specifies the following addresses:

Key wallets in the TRON (USDT TRC-20) network

General wallet (TKWY8EdLvZnrFQyRtXEND8TotGdi5AT6Y1): This general wallet was created by investors to consolidate funds and facilitate transfers to wallets potentially belonging to the fraudsters. It was established that the wallet's activity (incoming and outgoing transactions) on the “TRON” blockchain platform was recorded between **November 16, 2022** and **April 5, 2024**. At the time of the study, the wallet balance amounted to **0.07 USDT**. During the specified period, a total of **983 incoming transactions** amounting to **78,994,473.17 USDT** and **1,357 outgoing transactions** totaling **79,757,222.09 USDT** were recorded.

Fraudster's wallet (TBn3rK5ihpoix93fadRrZuQjLmNvxt7CTk): The main wallet used by the fraudster to receive funds from the general wallet.

Wallet (TEtyzqyreeQcryhU12hi6yk63fnk8DaSgL) and Wallet (TAr6qahqkEqMgYJgp1e6KroXQucl92f9AR): These additional wallets were also provided by the fraudster, **Alexander Knyazev**, and are presumably part of a broader scheme.

The report also lists hashes of large transactions confirming the movement of millions of USDT. Experts note that part of the funds was withdrawn to external wallets linked to IP addresses registered outside Russia and the EU, which may indicate preparations for capital transfer to offshore jurisdictions.

In its conclusions, **Star Compliance** recommends sending KYC (Know Your Customer) requests concerning the

clients and owners of the mentioned addresses to the corresponding exchanges and paying attention to the coincidence of timestamps of large withdrawals with the dates of the closure of MintXMarkets chats.

According to sources, these materials have already been submitted to investigative authorities, and **Alexander Knyazev himself** is listed in the reports of Russian special services as a person wanted on a federal level. Victims hope that **Interpol** will soon take up the case of **Alexander Knyazev**. However, for the time being, the Knyazev family continues to organize new pyramid schemes and collect investor funds on an international scale.

The family business of the Knyazev pyramid schemes: dozens of scam projects and millions of dollars

The activity of **Alexander Sergeyevich Knyazev** is only the tip of the iceberg. Behind him stands an entire [family network](#), where each relative played a specific role in the overall financial structure.

The head of this network is considered to be **Gulnara Knyazeva** — the mother and ideological inspirer, the public face of all projects, from **Aurum Foundation** to “women’s clubs” and “investment marathons.” It is she who promotes the rhetoric of “financial awakening” and appears at webinars that in reality serve as showcases for new pyramid schemes.

Her son, **Alexander Sergeyevich Knyazev**, controlled the technical and financial aspects — the creation of crypto projects, the registration of legal entities, and the distribution of funds across wallets and shell companies. In various investigations and expert reports, he appears as the connecting link between offline projects and their blockchain “shadow.”

Also mentioned in the cases and publications is **Knyazev’s brother, Nikolai Knyazev**, along with several close relatives who participated in promoting new brands such as **Syrex Pro**, **Botosaur**, **Bridge Travel**, and others.

Among the closed or collapsed projects are **Zefir One**, **Turbo Kit (The Whale)**, **Carousel**, **Ayratex**, **T–Point**, and **WIC Holding**.

In some episodes, women from the Knyazev family’s circle also appeared, acting as “mentors” and “partners” of **Gulnara Knyazeva**. Their roles consisted of attracting new audiences, mainly women from **Russia**, **Kazakhstan**, **Uzbekistan**, and **Germany**, through psychological training sessions, “financial marathons,” and promises of easy earnings.

Putting all these elements together, it becomes clear that there is a coherent structure in which all members of the Knyazev family are involved in a single business mechanism. Some are responsible for publicity and trust, others — for finances and technical implementation, and others still — for marketing and promotion.

This family “empire of trust” has in fact turned out to be a chain of interconnected financial pyramids stretching from **Russia** and **CIS countries** to **Europe** and the **Middle East**. One of the active pyramid schemes at the moment is **Aurum Foundation**.

Aurum Foundation: the new scheme of Gulnara Knyazeva

The project **Aurum Foundation**, headed by **Gulnara Knyazeva**, was presented as an investment platform aimed at a female audience, family capital, and “investing in oneself and in the future.” However, according to claims by victims and data from financial market monitoring materials, it exhibits numerous signs of a classic financial pyramid scheme.

The [Bank of Russia \(Central Bank of the Russian Federation\)](#) has included **Aurum Foundation** in the list of projects showing signs of illegal activity or financial pyramids.

On user review websites (for example: [irecommend.ru](#)), dozens of stories have been posted describing how investments in the scam project **Aurum Foundation** were not returned.

There is also an investigative video report about the scam project **Aurum Foundation**, which lists the project’s details and features comments from people who claim to have become victims.

On review platforms and forums, participants in the project report that after starting work with the **Aurum Foundation** platform, they were encouraged to invest funds under promises of high returns. However, as soon as the amount reached a certain threshold, withdrawals were blocked or they were required to “reinvest” into the next level. Many complained that their personal accounts became “frozen.”

The website [irecommend.ru](#) contains numerous negative reviews.

In addition, on thematic forums and anti-fraud websites (for example, [stop-projects.ru](#)), complaints have been registered, with victims uniting and reporting similar fraudulent patterns.

Despite the exposures, blocks, and inclusion in the financial pyramid lists, **Aurum Foundation** continues to operate actively. The project connected with the Knyazev family remains the showcase of their “new business”

and continues to attract investors from **Russia, CIS countries, Germany, the UAE, and Indonesia**. The geography of activity is confirmed by webinar recordings, Telegram group chats, and publications on English-language social media.

Even at first glance, it becomes obvious that the speakers of the numerous **Aurum Foundation** webinars (shown in official promotional materials) — several women and men who introduce themselves as “international experts in finance and self-development” — act as front figures. Their names are absent from the public sphere, and their **LinkedIn** profiles do not contain any mention of cooperation with **Aurum Foundation**.

At the same time, the project **Botosaur** — promoted as an AI platform for automatic investing — demonstrates the same pattern: aggressive advertising, a leadership network, promises of passive income, and a complete lack of legal transparency.

Alexander Knyazev — on international wanted list

The warrant for the search of **Alexander Knyazev**, a copy of which is available to the editorial office, is dated **July 2025**. The document states that Knyazev is suspected of committing crimes under articles related to large-scale fraud and the legalization of criminal proceeds. The investigation is also examining his possible participation in the creation of an organized group that operated under the cover of investment and educational projects.

At the same time, law enforcement agencies have sent requests to determine **Knyazev’s location abroad** — including to **Spain, Germany, and the UAE**, where his business contacts had previously been recorded. The issue of **Alexander Knyazev’s extradition to Russia** is already being discussed within the framework of the international search.

The story of the Knyazev family is a classic example of how a family group can build a network of interconnected pyramid schemes, disguising them as educational or innovative startups.

If you have suffered from the actions of **Alexander Knyazev** and the **MintXMarkets** project, or if you know his whereabouts, please contact the [website](#) administration or write to tonypopova4@gmail.com

Press release distributed by Wire Association on behalf of Europa, on Dec 7, 2025. For more information subscribe and [follow](#) us.

Media Assets

Images



Files

1. [alexander-knyazhev-gulnara-knyazheva-international-scam](#)
image/jpeg
<https://wire-association.s3.eu-west-2.amazonaws.com/production/325/alexander-knyazhev-gulnara-knyazheva-international-scam.jpeg>
 2. [fraudsters-alexander-knyazhev-gulnara-knyazheva-pyramid-scheme](#)
image/jpeg
<https://wire-association.s3.eu-west-2.amazonaws.com/production/326/fraudsters-alexander-knyazhev-gulnara-knyazheva-pyramid-scheme.jpeg>
-

Europa

Newsroom: <https://wireassociation.eu/newsroom/europa>

Website: <https://europa.eu/>

Primary Email: press@europa.eu

Social Media

Twitter - https://twitter.com/EU_commission

Facebook - <https://www.facebook.com/EuropeanCommission>

Instagram - <https://www.instagram.com/europeancommission/>

Linkedin - <https://www.linkedin.com/company/european-commission>
