April 20, 2026

PAYMENT PROCESSOR PROFILE

Cryptomus

Entity type:
Cryptocurrency payment processor and exchange

Year established:
2022

Volume:
USD 8.2 billion in total transactions as of March 2026

Founder:
Unknown

Base of operations:
Russia-linked; registered in Canada; primary operations likely in Eastern Europe

Sanctions details:
Not sanctioned; extensive on-chain exposure to sanctioned entities

Background

Cryptomus is a Russia-linked cryptocurrency payment processor and exchange incorporated in Canada under Xeltox Enterprises Ltd. Since its founding in 2022, the platform has enabled businesses to accept cryptocurrency payments while also offering personal wallet services, staking, an earn program, and peer-to-peer trading. Cryptomus has processed USD 7 billion in total transactions, with monthly on-chain volumes reaching approximately USD 153 million in January 2025.

Between 2022 and 2025, Cryptomus processed transactions associated with a broad range of illicit actors, including child sexual abuse material (CSAM) vendors, terrorist financing networks, human trafficking operations, and sanctions evasion networks. TRM identified over 75,000 transactions between Cryptomus and Iranian exchanges, including more than 50,000 with Nobitex alone, alongside extensive activity with sanctioned Russian exchange Garantex.

On October 22, 2025, FINTRAC issued a record penalty of nearly CAD 176 million against Cryptomus for multiple violations of anti-money laundering (AML) and terrorist financing legislation under Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

©TRM Labs 2026. All rights reserved.

Xeltox Enterprises Ltd. is currently appealing the fine, asserting a lack of knowledge or control over the relevant transactions.

FINTRAC enforcement and pivot to Heleket

In February 2025, Cryptomus introduced mandatory Know Your Customer (KYC) controls — likely prompted by prior engagement from FINTRAC. The change caused significant user disquiet and a corresponding drop in on-chain volume, from approximately USD 153 million in January 2025 to USD 86 million in March 2025.

TRM assesses with high confidence that Cryptomus — or its ultimate controllers — responded to this regulatory pressure by launching a parallel service, Heleket, designed to continue offering no-KYC payment processing to the same user base. Heleket launched between January and March 2025 and is incorporated as Handy Elect LLC in Georgia. The platform offers similar services to Cryptomus — including a personal hosted wallet solution and merchant payment processing that facilitates conversion and cash-out in USDT and other assets — but does not require KYC verification beyond a basic moderation requirement for its payment processing service. Although Heleket's AML policy claims to require identity documentation, TRM has observed that it is possible to transact on the platform without providing it.

The timing is instructive: Heleket's web traffic rose from zero visits in January 2025 to over 53,000 visits beginning in February 2025 — the same month Cryptomus introduced KYC controls — with the highest traffic originating from Nigeria, Russia, and India. Since its inception, Heleket has processed nearly USD 1 billion in transactions, maintaining approximately USD 200 million in monthly volume consistently. While it is not possible to quantify exactly how many Cryptomus users migrated to Heleket, the body of on- and off-chain evidence strongly suggests that many did.

The creation of Heleket appears designed to provide Cryptomus with sufficient separation to claim plausible deniability — while continuing to service a high-risk user base. If regulators determine the two entities are operationally linked, however, this could undermine Cryptomus' ongoing appeal of the FINTRAC penalty.

Evidence linking Cryptomus to Heleket

Heleket and Cryptomus share Garantex — the now-closed sanctioned Russian exchange — as a common liquidity provider. On January 16, 2025, Heleket's hot wallets received initial liquidity funding from Garantex, a sourcing pattern atypical for a regulated service registered in Canada. TRM observed large, rounded-value transactions between Cryptomus and Garantex

©TRM Labs 2026. All rights reserved.

consistent with a liquidity provider relationship, though a regulated virtual asset service provider (VASP) would be unlikely to use a sanctioned exchange in this role.

The volume trajectory of the two platforms is also telling. Heleket's on-chain activity rose sharply as Cryptomus' volumes declined following the February 2025 KYC implementation. In January and February 2025, Cryptomus accounted for the majority of combined illicit counterparty volumes between the two entities. By April and May 2025, Heleket accounted for over 80% of combined illicit flows — a reversal that aligns with the migration of high-risk users away from the KYC-enforcing platform. By late 2025, Heleket accounted for approximately 45% of combined illicit flows despite representing only about 30% of total combined volume, confirming a structurally higher illicit exposure ratio.

TRM has also observed numerous cybercrime actors — including CSAM vendors and cybercrime service providers — switching from Cryptomus to Heleket, with timing that corresponds directly with Cryptomus' introduction of KYC controls. There is crossover between illicit entities with counterparty exposure to both platforms, including smaller entities such as adult content and CSAM vendors that appear in both.

TRM analysts also identified numerous off-chain commonalities between the two platforms that, when paired with the on-chain indicators, support the assessment that they were created and are operated by the same organization.

Cryptomus and Heleket share the same privacy-focused domain registrar, identical branding and design elements, and unique phrasing on their public-facing websites that does not appear elsewhere in the industry. Both platforms charge matching 0.4% fees for payment processing and employ a practice called "project moderation" — requiring users to submit descriptions of their intended business activities for approval. This term is not commonly used by B2B payment processors; a comparable function at a regulated institution would typically be formalized as a Know Your Business (KYB) process. Both services also use the phrase "set discount to payment method," which does not appear to be used by any comparable entity.

Personnel overlap further supports the connection. The business development manager for Heleket is listed on Cryptomus' Telegram account. TRM also identified an individual located in Vilnius, Lithuania who claims employment with Cryptomus and is assessed with high confidence to be the same individual associated with Heleket's operations, based on physical similarities across profiles. In a thread on Cryptomus' Telegram channel, a Cryptomus administrator acknowledged a connection to Heleket, stating that the two entities had "entered into certain agreements" while simultaneously claiming they were distinct. Forum users noted similar observations, with one posting in March 2025 that they were able to log into Heleket using their existing Cryptomus credentials.

©TRM Labs 2026. All rights reserved.

Illicit activity and on-chain footprint

Between 2022 and 2025, TRM observed Cryptomus process hundreds of millions of USD in transactions associated with CSAM vendors, terrorist financing networks, human trafficking operations, and sanctions evasion. TRM identified over 75,000 transactions between Cryptomus and Iranian exchanges, with more than 50,000 involving Nobitex alone, alongside extensive flows through Garantex. Heleket has continued this pattern since its inception. Approximately 0.6% of Heleket's incoming volume in 2025 was identified as illicit — nearly five times greater than the average illicit inflow ratio observed across payment service providers in TRM data during the same period. Sanctions-related entities account for 60% of Heleket's illicit inflows, primarily driven by flows from Garantex. Additional exposure includes Russian darknet markets and cybercrime service providers that likely migrated from Cryptomus.

TRM analysis of Sinobi Group — a ransomware-as-a-service operation that emerged in June 2025 and is assessed as a potential rebrand of INC and Lynx ransomware — illustrates the platforms' role in ransomware cash-out. Following a ransom payment of approximately USD 122,246 made by a Canadian victim in December 2025, TRM traced proceeds to deposits at both Cryptomus and Heleket, among other services. The same investigation identified multiple addresses involved in laundering the funds accessing the network from non-VPN IP addresses geolocated to Russia and Iran, consistent with the geographic profile of actors known to transact through both platforms.

Law enforcement and regulatory response

FINTRAC issued a record penalty of nearly CAD 176 million against Xeltox Enterprises Ltd. for multiple violations of anti-money laundering and terrorist financing legislation — the largest penalty of its kind in Canada. Xeltox is currently appealing the decision.

©TRM Labs 2026. All rights reserved.