Issue No. 23
04.08.2026

DISMANTLING A MAJOR CRYPTO-ASSET LAUNDERING NETWORK: KEY TAKEAWAYS FROM THE AUDIA6 OPERATION

AudiA6, a crypto-asset laundering service suspected of processing more than EUR 336 million in criminal proceeds, was dismantled as a result of a coordinated international investigation. The service was allegedly used by ransomware groups and other cybercrime networks to conceal the origin, ownership and movement of illicit crypto assets.

The dismantling of AudiA6 represented more than the disruption of an individual laundering service. It also targeted a broader digital and financial infrastructure allegedly used to transfer, conceal and reintegrate hundreds of millions of euros in criminal proceeds. The case provides a significant example of how financial investigations, cybercrime enforcement, digital evidence analysis, cross-border judicial co-operation and asset-securing measures can be combined in complex virtual asset-related investigations.

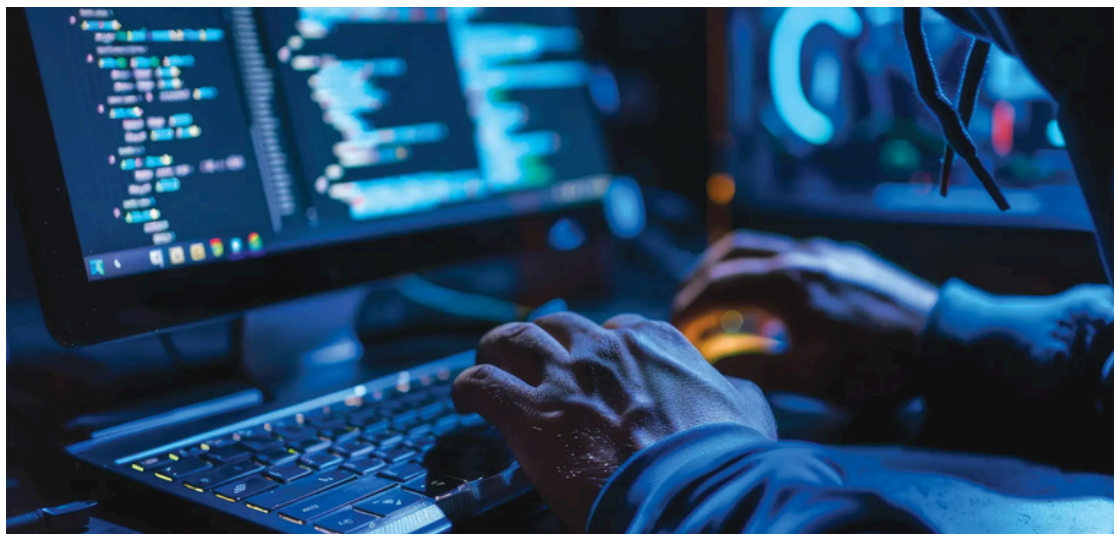
I. AudiA6's Alleged Laundering Model

AudiA6 allegedly operated as an intermediary between persons seeking to conceal criminally derived crypto assets and accounts established within the legitimate crypto-asset ecosystem. Prospective users were reportedly directed to AudiA6 through Dark2Web, a cybercrime forum allegedly operated by the same organisation, as well as through private messaging platforms.

Once a user engaged the service, crypto assets were transferred from the user's private wallet to wallets controlled by AudiA6. The funds were then divided into numerous smaller transactions and routed through multiple intermediary or mule accounts. These accounts were reportedly opened using stolen or commercially acquired identities.

Following this layering process, the funds were reassembled and returned to the user's wallet as purportedly "cleaned" crypto assets. AudiA6 allegedly charged a commission ranging from 3% to 10% for the service.

The structure was designed to increase the complexity of the transaction trail, create distance between the proceeds and their criminal source, and make the identification of the ultimate user more difficult. The case illustrates how laundering services may combine blockchain-based transfers with identity misuse, mule accounts and legitimate crypto-asset platforms in order to obscure beneficial ownership and the origin of funds.



II. Expansion of the Investigation

The U.S. Secret Service and IRS Criminal Investigation had reportedly been investigating AudiA6 since 2022. Between 2022 and 2026, investigators conducted undercover transactions during which AudiA6 allegedly accepted crypto assets presented as being linked to ransomware, fraud or theft and converted them in return for a commission.

A significant development occurred on 15 September 2025, when authorities arrested a Ukrainian national suspected of involvement in AudiA6-related money laundering activities. The examination of electronic devices seized during the arrest assisted investigators in identifying further individuals, communications and operational links within the network.

This stage of the case demonstrates the importance of combining undercover investigative techniques with the prompt examination of electronic devices and communications data. In complex cyber-enabled financial crime investigations, digital evidence obtained from a single suspect may provide the basis for identifying additional participants, infrastructure and financial connections.

III. Coordinated Enforcement Measures and the Securing of Assets

Following the investigation conducted by the Polish Central Cybercrime Bureau, arrests in Georgia were carried out on the basis of a Red Diffusion issued by the Łódź Regional Prosecutor's Office.

A criminal complaint dated June 2, 2026 identified Igorevich Tkachuk and Alexander Vladimirovich Ledenev as alleged senior members of AudiA6 and operators of Dark2Web. On June 10, 2026, both suspects were arrested in Georgia, while the infrastructure associated with AudiA6 and Dark2Web was targeted as part of the same operation.

The enforcement measures resulted in:

- the shutdown of 25 domain names;
- the seizure of more than 30 servers;
- the securing of more than 80 vehicles and several real estate assets in Georgia;
- the freezing of EUR 692,000 in crypto assets; and
- the seizure of more than EUR 86,000 in additional crypto assets.

The simultaneous targeting of suspects, digital infrastructure and assets was a central feature of the operation. Such an approach reduces the risk that members of the network may relocate servers, destroy evidence, transfer funds to alternative wallets or continue operating through replacement domains and accounts.

The case therefore underlines the need for enforcement measures to be planned and executed in a coordinated manner. In virtual asset-related investigations, the effectiveness of arrests may be substantially reduced unless they are accompanied by the immediate securing of relevant devices, servers, domains, accounts and assets.

IV. KYC Records, Digital Infrastructure and Investigative Indicators

Investigators identified more than 6,000 know-your-customer records linked to accounts allegedly used in connection with the AudiA6 network. Many of these accounts were reportedly associated with Russian-speaking intermediaries recruited to transfer criminal proceeds through legitimate crypto-asset exchanges.

The accounts were established using commercial email providers and email addresses connected to domains controlled by the organisation. The relevant domain names were subsequently disclosed to assist crypto-asset service providers in identifying and blocking accounts potentially linked to the laundering service.

These findings demonstrate that crypto-asset laundering investigations should not be limited to blockchain data. Although blockchain analysis may reveal the movement of funds, it does not necessarily identify the persons controlling the relevant wallets or accounts.

KYC records, exchange account information, email addresses, domain registrations, device identifiers and communications data can provide the off-chain evidence required to connect blockchain transactions to specific individuals and organisations. When assessed together, these data sources may reveal the operational structure of the laundering network, the identities of intermediaries and the points at which illicit funds entered or passed through regulated platforms.

V. International Co-operation Behind the AudiA6 Operation

The AudiA6 case involved parallel investigations led by the U.S. Secret Service and IRS Criminal Investigation on one side and the Polish Police on the other. Europol, Eurojust and other international law enforcement partners provided support throughout the operation. Eurojust coordinated judicial measures involving France, Poland, Georgia and Iceland. Liaison prosecutors from the United States, Georgia and Iceland also contributed to the process. Authorities from the United States, France, Poland, Georgia, Germany, Iceland, Japan, Switzerland, the United Kingdom, Canada and Australia participated in the operation or in related investigations.

The breadth of this co-operation reflects the cross-border nature of crypto-asset laundering. The suspects, digital infrastructure, service providers, accounts and assets involved in such cases are frequently located in different jurisdictions. Accordingly, no single national authority may have access to all the evidence or enforcement powers required to dismantle the network effectively.

The AudiA6 operation illustrates the practical importance of parallel investigations, rapid information exchange, co-ordinated judicial measures and active communication between competent authorities. These mechanisms enable investigators to identify assets and suspects across borders, align enforcement actions and reduce the risk that evidence or criminal proceeds will be moved before formal measures can be implemented.

VI. Key Takeaways for Crypto-Asset Investigations

The AudiA6 case demonstrates that blockchain tracing, although essential, is not sufficient on its own in complex crypto-asset laundering investigations. An effective investigative strategy requires blockchain analysis to be combined with i) undercover investigative activity, ii) KYC and exchange account records, iii) electronic device examinations, iv) domain and server data, v) email and communications records, vi) financial intelligence; and vii) conventional asset tracing techniques.

The case also highlights the importance of targeting the laundering structure as a whole. Arresting individual suspects without simultaneously securing related servers, domains, wallets, accounts and assets may allow other members of the network to continue operating, destroy evidence or move proceeds beyond the reach of the authorities. Equally, the public disclosure of relevant technical indicators, such as domain names and account-related information, can assist crypto-asset service providers in identifying connected activity and applying appropriate risk-based controls.

Ultimately, the AudiA6 operation demonstrates that parallel investigations, rapid information-sharing, coordinated judicial measures and cross-border asset tracing can significantly improve the ability of competent authorities to identify suspects, disrupt digital infrastructure and freeze or seize criminal proceeds.