AO 91 (Rev. 11/11) Criminal Complaint (approved by AUSA Benjamin D. Traster) USAO CW No. 26-065

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America
v.

Ruslan Igorevich Tkachuk, a/k/a "AudiA6," "xai" and Alexander Vladimirovich Ledenev, a/k/a "Azazello"

Defendant(s)

Case No. 26-mj-1055

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 17, 2021 through June 2, 2026 in the county of Philadelphia in the Eastern District of Pennsylvania, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. Section 1956(h)	Conspiracy to Launder Monetary Instruments
18 U.S.C. Sections 1956(a)(3)(B) and 2	Sting Money Laundering and Aiding and Abetting

This criminal complaint is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

/s/ Elizabeth Aguilar Smith
Complainant's signature

Special Agent, United States Secret Service
Printed name and title

Sworn to before me and signed by telephone.

Date: June 2, 2026

/s/ Jose R. Arteaga, USMJ
Judge's signature

City and state: Philadelphia, Pennsylvania

Jose R. Arteaga, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Special Agent Elizabeth Aguilar Smith, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS) and have been so employed since April 2018. During my career, I have been trained to conduct criminal investigations involving or relating to the financial infrastructure of the United States including financial fraud and computer crimes. I have successfully completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC). While at FLETC, I completed blocks of instruction that enable me to identify potential sources of electronic evidence, including but not limited to computers, cell phones, and other digital storage media and to preserve and utilize such evidence. I received additional training in the Special Agent Training Course at the USSS James J. Rowley Training Center in conducting investigations into a variety of criminal violations to include fraud schemes and computer crimes. Furthermore, I have attended more than 120 hours of USSS training pertaining to computer investigations involving cyber and electronic crimes. Pursuant to my duties as a Special Agent, I have participated in and directed numerous investigations involving financial fraud and computer crimes. Based on my training and experience, I am familiar with the tactics, methods, and techniques of committing various types of fraud in violation of federal law.

2. This affidavit is submitted in support of a criminal complaint and arrest warrant charging the defendants, Ukrainian National Ruslan Igorevich TKACHUK "TKACHUK" and Russian National Alexander Vladimirovich LEDENEV "LEDENEV," both of whom reside in Batumi, Republic of Georgia, with the following offenses: one count of Conspiracy to Launder

Monetary Instruments, in violation of 18 U.S.C. § 1956(h); and one count of Sting Money Laundering and aiding and abetting the same, in violation of 18 U.S.C. §§ 1956(a)(3)(B) and 2.

3. The facts and information contained in this affidavit are based upon my training and experience, participation in this and other investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other special agents and individuals involved in this investigation. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by my review of the records, documents, and other physical evidence obtained during the course of the investigation. This affidavit is only meant to contain information necessary to support probable cause for the requested criminal complaint and arrest warrant and is not intended to include each and every fact observed by me or known to the government. All dates, times and amounts are approximate.

DEFINITIONS[1]

4. **Virtual Currencies:** Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (*i.e.*, they can be digitally traded or transferred, and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. Cryptocurrencies, like Bitcoin (BTC) and Ether (ETH), rely on cryptography for security. Cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts. Some of the most common virtual currencies include BTC, ETH, TRON (TRX), and USDT.

[1] The information provided in this section is based on my training and experience.

5. **Stablecoins:** Stablecoins are a type of virtual currency whose value purports to be pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDT is a stablecoin purported to be pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

6. **Blockchain:** A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists of the Bitcoin blockchain, while Ether (or ETH) exists in its native state on the Ethereum network.

7. **Virtual Currency Exchange:** A virtual currency exchange (VCE), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. To the extent they are operating wholly or in substantial part in the United States, VCEs may qualify as money services businesses (MSBs) under the Bank Secrecy Act and, thus, VCEs may be legally required to conduct due diligence of their customers (*i.e.*, know your customer (KYC) checks to collect identifying information about customers and verify their identities) and have anti-money laundering programs in place to the extent they operate and service customers in the United States. *See* 31 U.S.C. § 5311 *et seq*. (Bank Secrecy Act).

8. **Virtual Currency Address:** A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

9. **Virtual Currency Wallet:** A virtual currency wallet (*e.g.*, a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

10. **Blockchain Analysis:** Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement uses reputable, free open-source blockchain explorers, as well as commercial tools and services that have proven reliable in numerous investigations.

11. **Virtual Currency AML:** Virtual Currency AML refers to the practice of applying anti-money laundering (AML) policies to cryptocurrency. Some of these practices include traditional KYC rules to ensure cryptocurrency customers or clients are who they purport to be and to scrutinize the source and purpose of incoming and outgoing funds. This includes conducting risk assessment via blockchain analysis of cryptocurrency transactions to determine if the funds come from illegitimate or otherwise high-risk sources. Through my training and experience, I know that VCE's may freeze or block funds from their clients that they believe directly or indirectly come from an illegitimate source or otherwise have a high-risk score.

12. **Cryptocurrency Mixing or Tumbling:** A virtual currency mixing service (*i.e.*, a "mixer" or "tumbler") is an entity or software protocol that allows users to commingle or mix different streams of potentially identifiable virtual currency. While these services often promote themselves as designed to enhance privacy and anonymity, they are often used to conceal proceeds from illegal transactions by accepting "dirty" cryptocurrency from users and returning "clean" cryptocurrency to a wallet address specified by the original user. Generally, the customer can send virtual currency to a specific wallet address that is controlled by the mixer. The mixer then commingles this virtual currency with funds received from other customers and sends it through a convoluted series of transactions, making it difficult to trace on the blockchain.

13. **Cybercrime Forum:** A cybercrime forum is a website where cybercriminals meet to solicit, advertise and discuss cybercrime. On these websites, cybercriminals often solicit or advertise various cybercrime services among each other. Cybercrime forums are operated by administrators who create and enforce rules among forum members. Forum rules govern commerce on the forum, which is in the interest of forum members to lower the risk of fraudulent transactions between members and increase profitability.

14. **Moniker**: A moniker is the chosen online name of a cybercriminal that is used on cybercrime forums. Cybercriminals often use the same moniker or nickname to identify themselves online across multiple platforms. Because cybercriminals often communicate over the internet without divulging their true identity, many use one or more monikers frequently to generate a "brand" or consistent identity in their online interactions. Frequently, a cybercriminal's moniker will be incorporated into account names for online communication services, such as instant messaging platforms or email addresses.

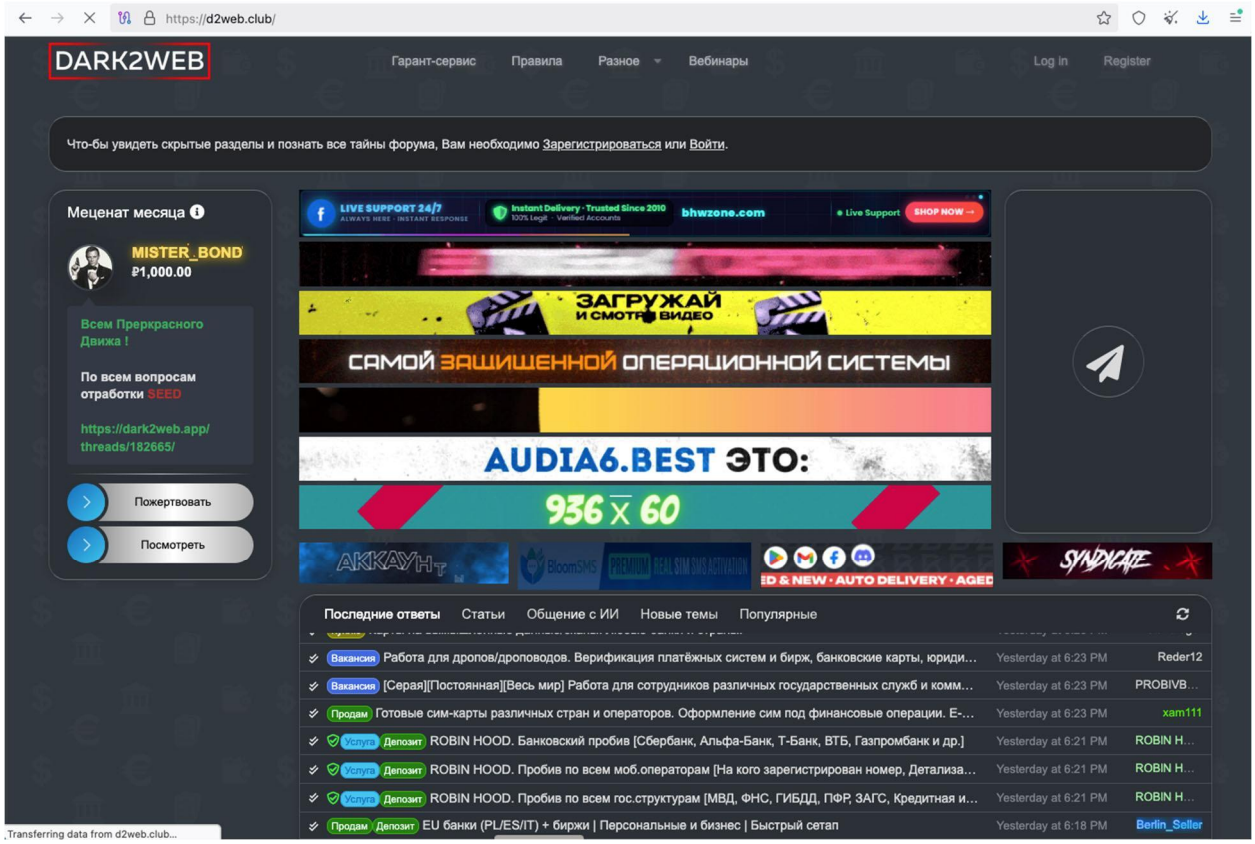
PROBABLE CAUSE

15. Since 2022, the USSS and Internal Revenue Service – Criminal Investigations (IRS-CI) have been investigating a criminal conspiracy that manages a cryptocurrency mixing service known as AudiA6.[2] The AudiA6 money laundering service purports to conceal the origins of funds sent to it by "mixing" cryptocurrency and returning cryptocurrency that is more difficult, if not impossible, to trace to a specific origin. As payment, the AudiA6 mixing service charges a commission based on the amount mixed and the risk the cryptocurrency may be traced to illicit sources. The AudiA6 mixing service advertises its service on cybercrime forums, including one called Dark2Web. As explained in detail below, the investigation has determined that TKACHUK and LEDENEV are senior members of the AudiA6 organization, who manage the cryptocurrency money laundering service and the Dark2Web cybercrime forum.

A. The Dark2Web Forum

16. On April 16, 2026, agents acting in an undercover capacity reviewed the Dark2Web forum which was accessible from the website address d2web.club. Below is a screenshot taken of the main Dark2Web landing page:

[2] As discussed throughout this Affidavit, the cryptocurrency mixing service under investigation is advertised under the brand name AudiA6. However, a known user of cybercrime forums uses the moniker "AudiA6" as an alias. I believe the individual who uses the moniker AudiA6 on cybercrime forums helped create and now manages the AudiA6 brand that offers a cryptocurrency mixing service on cybercrime forums.



Based on the agents' review of the Dark2Web forum, it has a similar construction to other darknet forums. It contains advertisements for criminal services and various threads where members can discuss criminal services or other topics. Forum members and management use monikers on the Dark2Web forum to hide their true identities, but through the registration process, administrators make sure monikers are not reused and therefore each unique moniker functions as a forum member's brand. Based on a review of the profiles of Dark2Web's forum management, the longest serving member of management joined the forum in 2015.

17. Having reviewed the Dark2Web forum in depth, I know that it, like many darknet marketplaces and forums, promotes illegal commerce on the forum by: vetting criminal service providers; arbitrating between and banning of members who do not uphold deals made with other members; and providing an escrow service or "Garant" for members conducting transactions with each other to ensure that vendors provide the services they purport to offer and

customers pay for those services. Dark2Web also has several other services that it uses to support its members' criminal activity such as an operating system its members can use that logs minimal information during its use to counter digital forensic investigation, as well as other anonymous internet services.

18. During my review of the Dark2Web forum, I observed a Russian language post, dated October 10, 2022, with the subject "Interview with the owner of the Dark2Web resource." The post includes an interview between a Dark2Web "journalist" and a person purporting to be the owner.[3] The owner states he does not want to provide his name or moniker in the interview. The owner claims he bought the Dark2Web forum in 2021, and that it was created in 2015 by an Uzbek and a second person, described as a technical specialist with the moniker "Azazello." The owner says the forum has a staff of eight people including an individual who goes by "AudiA6." The owner states he developed Dark2Web to be anonymous and secure and that it does not provide information to law enforcement.

B. AudiA6 Advertisement on the Dark2Web Forum

19. During the April 16, 2026 review of the Dark2Web forum, agents observed and took screenshots of an advertisement for AudiA6's money-laundering service. A screenshot of an excerpt of the advertisement is below:

[3] The translations of Russian language statements contained in the Affidavit were completed by Russian-speaking agents or analysts or by machine translation. Machine translation uses artificial intelligence software to automatically translate text or speech between language without human involvement. Where machine translation was used, agents or analysts verified the accuracy of the translations.

As portrayed in the above screenshot, Dark2Web member "AudiA6," who has the senior forum status of "moderator" and "arbiter,"[4] created an advertisement in Russian on April 17, 2021. The advertisement describes AudiA6's cryptocurrency exchange and mixing service. What follows is a machine translation of the full advertisement:

> I won't be like everyone else, blabbering on about how great my service is, like, the standard package: quality, efficiency, reliability, warranty, and so on and so forth...
> It's better to take a look than read advertising slogans.
> Below is a link to my profiles on various forums. You can visit each one and see what I'm like and whether you can trust me.
> https://audia6.best/about
>
> Deposits made:
> 1. XSS - 1 BTC
> 2. Exploit - 1 BTC
> 3. Rutor - 0.565496995 BTC
> 4. D2W - 2,000,000 rubles
> 5. Darkmoney - 200,000 rubles
> 6. Probiv - 50,000 rubles
> 7. Lolz - 150,750 rubles

[4] A forum "moderator" in senior forum administrator who reviews forum content and threads created by members to ensure they comply with forum rules and policy. A forum "arbiter" is senior forum administrator who is responsible for adjudicating disputes between members. Based on my training and experience, I believe a forum user who is both "moderator" and "arbitrator" suggests a significant role in the management of a cybercrime forum.

===AudiA6 Exchanger===
Exchange Directions:

Cash In - BTC
BTC - Transfer (Sber, Alfa, Tinkoff, Privat24, Monobank, Raiffeisen, etc.)
BTC - QR Tinkoff
BTC - QIWI
BTC - Yandex
BTC - Cash anywhere in the world
BTC - VISA/MASTERCARD
BTC - Payeer/ADVCASH/Perfect/PayPal/Skrill/Neteller
Convert any cryptocurrency to any cryptocurrency
Cash in any country - to any crypto
Cash in one country - cash in another

Currently, the exchange rate is around +3% on Binance.[5]
The rate varies daily, the market varies daily, and everything is very volatile. Sometimes I'll change the Binance rate by -1% in your favor; it all depends on the market at the time of exchange.
Minimum exchange or mix amount is $1,000.

ATTENTION!!! It's cheaper to exchange by contacting an operator via chat or Telegram at https://t.me/obmen_audia6 or by email at obmen@audia6.online and audia6-obmen@exploit.im. The rate is volatile, and unfortunately, it's technically impossible to exchange without losing the commission percentage I can give you in person! Sometimes it's 1%, sometimes 2%, sometimes 2.2%, sometimes 2.5%, but the maximum is 3%. The website always charges a 3% commission. You can exchange for less if you contact us directly through the contact section or chat.

WARNING!!!! Be sure to follow the direct link in Telegram, as there are many fakes! Also, be sure to verify your transactions via private messages, at least the first few. I will not be held responsible for transactions not confirmed via private messages!

===Cryptocurrency Mixer by AudiA6===
Most mixers are cheap scams. They trick you into thinking your transaction will be mixed with other transactions and split into parts, making it appear clean... In reality, mixing cryptocurrencies only complicates the investigation process for intelligence agencies, but it doesn't eliminate the risks.

Remember: a clean transaction at the output is a transaction with all the possible risks completely removed. There's only one way to cut off your tails—to take your dirty crypto and give you my clean one.

[5] Despite this statement, Binance as of June 1, 2026, advertises an exchange rate of 0.019% or less. *See* https://www.binance.us/fees. Similarly, the OKX exchange charges a 0.2% to 0.35% exchange fee. *See* https://www.okx.com/en-us/fees. As such, I believe an individual paying similarly high fees pays such fees to conceal the origins of the cryptocurrency sent to an illicit mixing service.

> That's why my mixer is better than all the others combined. I won't mix anything for you; I'll simply take your dirty crypto and give you the clean one. What I do with your dirty crypto is my personal responsibility.
>
> Rates... If you're reading this, you should know. Regardless of the rate you choose in the form on the website, the rate will still be the same: 5%. I added the rates for show.
>
> Cryptocurrencies we "wash" clean with Ariel: BTC, LTC, ETH, ETC, BCH, BSV, Tether (OMNI), XRP.
> The resulting AML risk score is no higher than 25%—the standard rate for exchanges. Sometimes it's as low as 18%, or even 0%. Most importantly, all transaction "tails" are completely severed.
> All requests are processed manually!
> CONTACTS:
> Telegram contact for inquiries: @obmen_audia6
> Direct link: https://t.me/obmen_audia6
> Jabber: obmen@audia6.online
> Jabber: audia6-obmen@exploit.im
> qTox:
> 1F2F83AA634455DE2FF21DE1CFBF3D5963E666FCFDDA18D3071D2B5F27012F7E7DEAB2186136
> Exchange Website: https://audia6.best/
> Mirror: https://all24.cc/
> Mirror: https://ronexchange.com/
> Mirror: https://nxt.am/
> Tor Website Version:
> http://audia6gazoidvnb77slrqdhwrwf6iqe5z5dxn5sg45cj5iek7inyv6qd.onion/
> Tor Website Version:
> http://audia6wwwfoegb4c4hwkvlttn5m4jzls6h3nnbqybvabei66gy6cm2id.onion/
> Mixer Website: https://audia6.vip/ (Under development; please use the contact details provided for faster service).
>
> ATTENTION! You MUST use the direct link to access our Telegram channel, as there are many impostors! Additionally, please ensure you verify all transactions—at least the initial ones—via Private Message (PM). I cannot be held responsible for any transactions conducted without explicit confirmation in our PM chat!
> Last edited: 27.01.2026

Based on the agents' review of the Dark2web forum, this advertisement was first posted in 2021 and last edited on January 27, 2026.

20. Based on my training and experience, in this advertisement, AudiA6 explicitly offers to conceal and disguise the source of any prospective customer's cryptocurrency that

would otherwise be traceable to criminal sources for a fee of up to five percent of the amount of funds being laundered. Specifically, in the advertisement:

a. AudiA6 describes the process of concealing the source of cryptocurrency as "washing" or washing clean with Ariel (a brand of detergent). To prevent a customer's cryptocurrency from being traced to criminal sources, AudiA6 offers to receive the "dirty" cryptocurrency and then send customers cryptocurrency from a separate and distinct source that is not traceable to criminal activity.

b. AudiA6 uses common money laundering phrases to describe the process, such as identifying cryptocurrency that can be traced to criminal activity as "dirty" and cryptocurrency whose criminal source has been concealed as being "clean."

c. AudiA6 references "cut[ting] off your tails," which effectively means the cryptocurrency provided to customers will no longer be traceable to the criminal source from which it originated.

d. The advertisement states that the clean cryptocurrency provided to customers will have an AML risk score of under 25%. Cryptocurrency exchanges, or the firms engaged to do it on their behalf, conduct AML risk scoring to determine the risk that cryptocurrency comes from an illegal source. AudiA6 purports to know that cryptocurrency exchanges have an internal AML policy to block transactions that have a risk score higher than 25%, and AudiA6 offers assurance that its money laundering service will send cryptocurrency to exchanges and eventually to customers with a risk score below 25%, meaning transactions will not be blocked or frozen by exchanges.

e. Based on my training and experience, I believe that the services offered by AudiA6 interfere with the risk management and business operations of cryptocurrency exchanges by manipulating the exchanges' AML policies and risk scoring. By manipulating the risk scores of cryptocurrency deposited in exchanges, AudiA6 enlists cryptocurrency exchanges as unwitting partners in AudiA6's money laundering operations.

21. The AudiA6 Dark2Web advertisement states:

Deposits made:
1. XSS - 1 BTC
2. Exploit - 1 BTC
3. Rutor - 0.565496995 BTC
4. D2W - 2,000,000 rubles
5. Darkmoney - 200,000 rubles
6. Probiv - 50,000 rubles
7. Lolz - 150,750 rubles

22. In my training and experience, I know XSS, Exploit, Rutor, Darkmoney, Probiv, and Lolz are major Russian-speaking cybercrime forums. These forums are notorious for offering cybercrime services to other cybercriminals and largely operate under the same rules as Dark2Web. The various "Deposits" quoted in this advertisement refer to a type of guarantee offered by the AudiA6 mixing service. The Deposits refer to payments made in escrow to the cybercrime forums, and the advertisement informs potential customers that they can recoup funds if the service does not follow through on a transaction. I believe the AudiA6 mixing service was noting its guarantee that it could provide cryptocurrency that was not tied to criminal activities but nonetheless originated as criminal proceeds.

23. Agents acting in an undercover capacity visited XSS, Exploit, Rutor, Darkmoney, Probiv, and Lolz, among others, and found advertisements for AudiA6's mixing service. The advertisements on these forums were created on close to the same day as the Dark2Web AudiA6

advertisement and used almost the exact same advertisement language. In other words, AudiA6 was offering its mixing service as a vendor on numerous cybercrime forums, in addition to the Dark2Web forum.[6]

24. Lastly, on the advertisement posted on the Dark2Web website, AudiA6 provides links to its own webpages and other ways to contact it to arrange to use its money laundering services, including Telegram, Jabber, and Tox. AudiA6 also provides numerous locations where an individual can use the darknet to access and use AudiA6's money laundering services.

C. Undercover Transactions Using AudiA6

25. Between December 2, 2022, and May 15, 2026, undercover agents conducted six undercover transactions using the AudiA6 mixing service while representing the funds as proceeds of criminal activity. For each transaction, undercover agents used the AudiA6 mixing service, requiring the infrastructure and concerted design implemented by the owners and managers of the AudiA6 mixing service.

26. On December 2, 2022, undercover agents located in Muskogee, Oklahoma, conducted two transactions using the AudiA6 mixing service. In one transaction, while communicating with the AudiA6 Telegram account, agents stated in Russian: "hello, do you have mix limits, can I mix $1,000 USD, is it possible to mix dirty money from ransomware, crypto scam etc." Based on my training and experience, I believe the undercover agents were informing the operator for the AudiA6 mixing service that the source of the cryptocurrency to be mixed represented proceeds of ransomware. AudiA6 responded in Russian: "hello, yes." Based on my training and experience, I believe the AudiA6 agreed to mix the cryptocurrency regardless of the criminal source of the funds. Agents subsequently sent $1,005 in cryptocurrency to

[6] In some cases, such as on the Exploit forum, the advertisement was made by a forum member with the moniker "xai," which is another moniker used by the cybercrime forum user known as AudiA6. *See* Part F, *infra*.

AudiA6 and received $968.37 in cryptocurrency back which resulted in AudiA6 keeping $36.63 or about a 3.6 % commission including bitcoin network fees.[7]

27. On January 26, 2024, undercover agents located in Washington, D.C., conducted a transaction with the AudiA6 mixing service. Agents contacted the AudiA6 Telegram account and stated in Russian that they would like to exchange "dirty" bitcoin. I believe agents informed the AudiA6 mixing service that the cryptocurrency to be mixed derived from criminal sources. Agents then transferred $2,003.89 in bitcoin to AudiA6, and the mixing service then returned $1,771 in bitcoin and kept a commission of $232.89 or 11.6% including network fees.

28. On March 11, 2026, undercover agents located in Washington, D.C., contacted AudiA6 via Tox and said in Russian: "I have 2.9 eth from scam… and stolen eth… is it ok?" (eth referring to the cryptocurrency Ethereum.) AudiA6 then responded in Russian, "yes, no problem." I believe the undercover agents informed the AudiA6 mixing service that the Ethereum cryptocurrency to be mixed represented proceeds of fraud. Agents subsequently transmitted $6,021.87 in Ethereum, and AudiA6 returned $5,661.90 in Bitcoin. AudiA6 kept $359.97, or 6% in network fees and commission.

29. On April 9, 2026, while located in Philadelphia, Pennsylvania, agents acting in an undercover capacity contacted the AudiA6 mixing service via the qTox ID listed in the AudiA6 advertisement and had the following conversation (in part):

…	
Undercover Agent	the direction is BTC --> USDT, ok?
Undercover Agent	the amount is 4.5k
…	
Undercover Agent	please remind me what is the commission structure
AudiA6 Exchange	Our commission:

[7] Based on my training and experience, I believe the commissions and fees paid for the undercover mixing transactions reveal the premium paid to the mixing service for its illicit services in concealing the origins of the cryptocurrency sent to it. Each undercover transaction included fees considerably higher than a cryptocurrency exchange would charge. See ¶¶ 26-28, 30, and 33.

	From $1000 - 5% + exchange fees Up to $1000 - $50 + exchange fees Up to $1000 and in the red zone - $100 + exchange fees Exchange fees: BTC - $60 ERC20 - $60 TRC - $5 The rest is $5 Crypto labeled with 50% as Stolen/Scam/Sanctions/Mixer/Dark market/ etc. refers to high-risk High-Risk Exchange - from 50% 10% + exchange fee
Undercover Agent	is BTC from scam ok? Stolen bitcoin...
AudiA6 Exchange	don't care
Undercover Agent	ha, great
…	
Undercover Agent	by the way, I wanted to ask you something
Undercover Agent	is d2w – your forum?
Undercover Agent	it's just I found [this] service through [that] platform
AudiA6 Exchange	yes
Undercover Agent	and what's the activity like over there?
AudiA6 Exchange	honestly, I don't know
AudiA6 Exchange	I'm just an operator
Undercover Agent	got it

30. As described in this conversation, undercover agents sent 0.06915651 Bitcoin, equal to $4,974 at the time of the transaction, to the AudiA6 mixing service. The AudiA6 mixing service then sent 4,662.295269 USDT, equal to $4,661.54 at the time of the transaction, back to the agents. The AudiA6 mixing service kept a commission of about $312.46 from the transaction, including network fees, or 6.2%. In the chat, agents told the AudiA6 Exchange operator that the funds came from a scam and were stolen funds, and the operator said they did not care. The operator confirmed that the Dark2Web forum was theirs. The operator also acknowledged they were just an operator for the service, implying that they were not the managers of the organization. Although the AudiA6 operator identified themselves as an operator rather than management, forum advertisements for the AudiA6 mixing service promote laundering "dirty" cryptocurrency, *i.e.*, criminal proceeds, as a service feature. Therefore, when

the operator stated that they did not care about the funds originating from fraudulent activity and proceeded to launder them, the AudiA6 operator was acting in accordance with AudiA6's organizational policy.

Sting Money Laundering Transaction with AudiA6, in violation of 18 U.S.C. § 1956(a)(3)(B)

31. On May 15, 2026, undercover agents located in Philadelphia, Pennsylvania, contacted the AudiA6 service via the qTox ID listed in the AudiA6 advertisement and had the following conversation which is a machine translation from Russian to English:

…	
Undercover Agent	straight to business
Undercover Agent	just got profit from selling coconut[8] on blacksprut[9]
Undercover Agent	is it ok or are the risks too high?
AudiA6 Exchange	everything like that needs to go through a mixer
Undercover Agent	now
Undercover Agent	ok, what percentage?
Undercover Agent	is BTC to BTC possible?
AudiA6 Exchange	5% or 10%, depends on your AML
Undercover Agent	got it
Undercover Agent	no problem... I have 0.063 BTC
…	
Undercover Agent	here's partner's wallet:
…	
Undercover Agent	great... send ETH directly to the partner:
…	
Undercover Agent	damn, I mean tether
Undercover Agent	sorry, just tired
Undercover Agent	do you have several operators?
AudiA6 Exchange	yes, of course
AudiA6 Exchange	will issue soon
AudiA6 Exchange	I'll write
Undercover Agent	ok, thanks
…	
Undercover Agent	great, partner received

[8] The Undercover Agent used the Russian word "kokos" which in my training and experience is a common euphemism for cocaine.
[9] Blacksprut is a well know Russian-speaking internet drug market.

32. In this transaction, the UC told the AudiA6 Exchange operator that the UC wanted to mix cryptocurrency described as proceeds from selling cocaine on a Russian speaking online drug market called "Blacksprut." The AudiA6 Exchange operator responded, "everything like that needs to go through a mixer." Based on my training and experience, I believe the AudiA6 Exchange operator acknowledged the origins of the criminal proceeds and recommended that such proceeds needed a mixer to mask the origins of the cryptocurrency.

33. The UC then sent 0.06311094 BTC, the equivalent of $5,148 at the time of the transaction, to the AudiA6 mixing service. The AudiA6 mixing service then returned 4,733.72748 USDT, the equivalent of $4,731.41 at the time of the transaction, back to a UC-provided address. During the transaction, the UC requested multiple times that the AudiA6 mixing service return the money to a "partner's" cryptocurrency address. Based on my training and experience, I believe the UC was revealing to the AudiA6 mixing service that the UC worked with other individuals to distribute narcotics. The AudiA6 mixing service took a commission of $416.59 or 8%, including network fees.

34. In each of these transactions, the undercover agent requesting the mixing transactions made clear that the money was coming from illicit sources: in particular, on May 15, 2026, the undercover agent described the proceeds as originating from the distribution of cocaine on a Russian-speaking internet drug market. The undercover agent also described working with a partner to distribute the narcotics, in violation of 21 U.S.C. §§ 841 and 846.

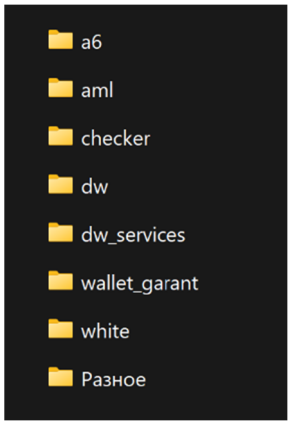
D. AudiA6 and Dark2Web Internet Infrastructure and Forensics

35. Based on open-source information, agents have observed that since at least 2022, AudiA6 and Dark2Web have used Cloudflare, Inc. ("Cloudflare"), a San Francisco, California based internet service provider to protect its websites from distributed denial-of-service (DDOS)

attacks. In September 2022, agents obtained records from Cloudflare identifying that Cloudflare was directing traffic for the AudiA6 website to a server owned and operated by 1984 ehf, an Iceland-based corporation. Pursuant to a U.S. mutual legal assistance request, Iceland provided a copy of the server to the USSS in December 2023. The 1984 ehf server included the webserver used to operate AudiA6 websites listed in the AudiA6 advertisements, as well as a Jabber communication application, a temporary email application, and a Customer Relationship Management (CRM) application. The server was also used to operate three Dark2Web services. Based on my training and experience, as well as my review of the 1984 ehf server, I believe this server was used to manage and control parts of both the AudiA6 mixing service and Dark2Web forum.

36. Review of the 1984 ehf server revealed it was using an application called Vesta Control Panel to manage and back up the server. Vesta Control Panel generated backups for the 1984 ehf server that were then sent to a Storage Box[10] with an address of "u328135.your-storagebox.de" controlled by a German company called Hetzner. Pursuant to a mutual legal assistance request transmitted in July 2024, Germany provided the USSS with Hetzner records for the "u328135.your-storagebox.de" Storage Box. The subscriber records show that this Storage Box was rented to Alexandr LEDENEV of Batumi, Republic of Georgia, with email address azzazelllo@mail.ru. The records also included a copy of this Storage Box, which shows it was used to store various AudiA6 and Dark2Web service backups. Specifically, the Storage Box had the following folder structure:

[10] Hetzner provides a Storage Box product that is a remote storage server that can be used to store backups or other large file archives, a description is provided by Hetzner at https://docs.hetzner.com/storage/storage-box.



37. A review of the information within these folders shows they contain Vesta Control Panel and other backups from various data centers around the world. The folder labeled, "a6," contains AudiA6 related websites and applications backups. The "dw" folder contains backups of the Dark2Web forum server including its database. The "dw_services" folder contains backups of applications on the Dark2Web forum that aid forum members in the commission of cybercrime. The "wallet_garant" folder contains backups of the Dark2web Garant or escrow service. The "white" folder contains backups of apparently non-criminal websites, including for a Georgian car rental service.[11] The car rental website backup contained email correspondence for the car rental service, including an email from Ruslan TKACHUK in which he provided a Georgian temporary residence card with his name and photograph.

38. The "a6" folder includes AudiA6 mixing and exchange website backups and backups for applications used to support the AudiA6 mixing and exchange services. A review of the exchange and mixing website backups shows that while the websites were operational, they were little used and had limited functionality. This is consistent with the UC agents' experience, in which they were guided to contact the AudiA6 service through private chats via Telegram,

[11] Based on my training and experience, I believe that "white" is frequently used by cybercriminals to describe legitimate, non-criminal, activities.

Jabber, or Tox to conduct transactions, instead of using the website. Based on my training and experience, I believe illicit cryptocurrency mixing and money laundering services prefer to use messaging services to further shield their identities and communications from law enforcement activities.

39. Other backups in the "a6" folder contained AudiA6 operational notes and records. One backup ("CRM") includes a database with a table listing 25 employee accounts (using monikers to identify them), and 13 tables listing 6,000 cryptocurrency exchange account logins and other account information. There is also a folder containing scans of passports and personal "selfie" photos of the people whose names are listed in the tables.[12] Based on my training and experience, these 6,000 accounts appear to be fraudulent cryptocurrency accounts created to move illicit funds through cryptocurrency exchanges without detection.

40. The CRM database also includes tables containing itemized listings of Dark2Web forum expenses, such as server rentals, and an itemized list of the forum's income, such as paid advertisements on the Dark2Web forum. Based on my training and experience, since Dark2Web administrative files are comingled with AudiA6 administrative files, both services are likely operated by the same group.

41. A second backup within the "a6" folder contains databases derived from an email application ("TMail"), including records of 4,000 email accounts and over 500,000 email messages, which appear to assist in the creation of fraudulent cryptocurrency accounts and to correspond with the cryptocurrency exchanges regarding the accounts. The email records include automatically generated transaction emails from cryptocurrency exchanges that were sent when a transaction was conducted, as well as emails with warnings from cryptocurrency exchanges

[12] Based on my training and experience, I believe these passport scans and selfie photos are provided to cryptocurrency exchanges who request know-your-customer data to open exchange accounts.

when fraudulent activity was detected, prompting internal investigations. For instance, on several occasions, an exchange froze funds received by an AudiA6 exchange account listed in the CRM database. When the fraudulent account operators inquired about the freeze, the exchange requested information about the source of the funds and the relationship with the sender. In response, the fraudulent account operators claimed to be application developers, explained that the transactions were payments for work completed, and provided fabricated documents that supported the story. Based on my training and experience, these fraudulent claims and documents were proffered to conceal the illegitimate sources of the funds and convince the exchanges to unfreeze the funds.

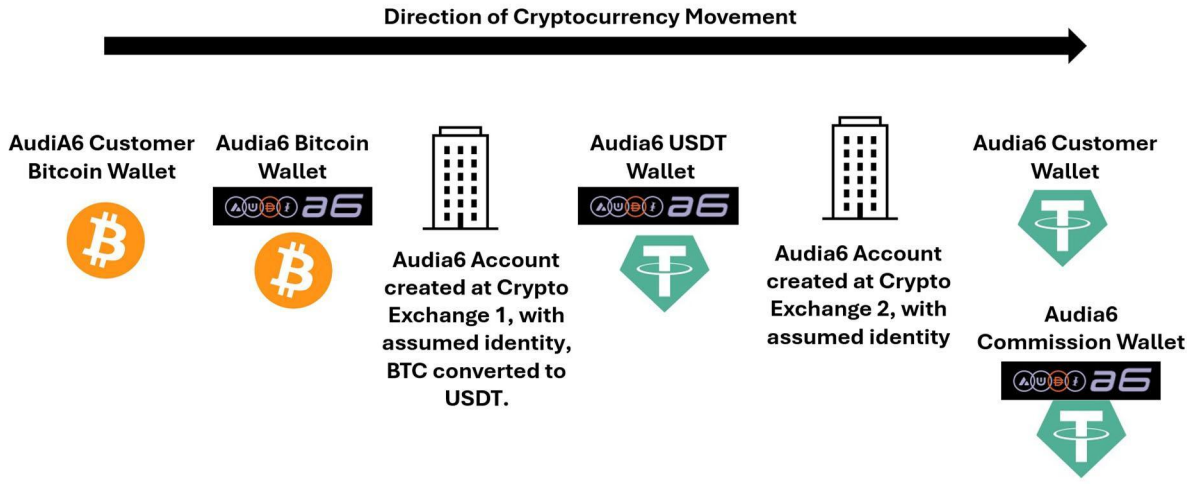
42. The same backup of the Tmail application contains a table within the database called "log_amls" which has 2,900 risk scores of cryptocurrency addresses and transactions from February to April 2025. Within these results, 1,438 (about half) show risk scores higher than 25%, the threshold AudiA6 identified in its advertisement as the level that exchanges used to block transactions. The log_amls table also shows sub-scores of risk, such as connections to ransomware, stolen funds, terrorist financing, dark markets and much more. Some of the sub-scores identify cryptocurrency addresses as having a 100 percent association with stolen funds or other risk categories. Thus, the AudiA6 operators were aware that many of the cryptocurrency transactions they received had high risk of being associated with criminal activity.

E. Cryptocurrency Tracing Analysis

43. Law enforcement conducted blockchain analysis and reviewed cryptocurrency exchange records connected to accounts from the AudiA6 CRM database and undercover transactions. While the AudiA6 mixing service offers to receive and exchange a variety of different cryptocurrencies, the records indicate it most commonly received BTC from its

customers.[13] Those funds were then transferred to a cryptocurrency exchange, converted to USDT, sent to another wallet controlled by AudiA6, and moved to a different cryptocurrency exchange.

44. At this point, AudiA6 typically sent USDT to the customer's designated recipient address, less a commission which was sent to another AudiA6 address. The customer could also elect to receive the funds in a different cryptocurrency, in which case they would be exchanged for the other cryptocurrency and sent to the customer. The total transaction time was typically an hour. Contrary to AudiA6's forum advertisement, which claimed that transactions are often untraceable due to the use of separate pools of funds, AudiA6 was not actually sending and receiving from distinct, unconnected sources. Instead, transactions could be directly traced through exchange records. Below is a visual aid of the AudiA6 money laundering process:



45. Through blockchain analysis, law enforcement has determined that over 10,333 BTC (valued at $389,747,417 at the time of the transactions) was deposited to AudiA6 Bitcoin

[13] In my training and experience, most ransomware and other criminal commodities are paid for using bitcoin due to its historical ease of use and name recognition.

wallets since the service was launched in 2021. Using blockchain analysis tools and financial records obtained during the investigation, IRS-CI cyber analysts reviewed the sources of funds for the deposits to these AudiA6 wallets. Out of the total 10,333 bitcoins deposited, 393.39 BTC (valued at $19,234,331 at the time of the transactions) were received *directly* from known darknet markets, ransomware organizations, cybercrime Garant services, and other illicit sources.[14] See table below:

Source Category	Total TXs	Total BTC	Total USD/BTC
darknet market	34	10.53	$ 492,328
illicit actor-org	20	72.95	$ 2,410,890
ransomware	22	180.12	$ 8,028,664
stolen funds	5	129.79	$ 8,302,448
Total	**81**	**393.3940208**	**$ 19,234,330.78**

46. Expanding the above analysis to include the receipts where there exists one intermediary "hop" between the sender and the receiver of the BTC, presumably designed to mask the origins of the proceeds before the AudiA6 service "mixed" the cryptocurrency, law enforcement determined that AudiA6 wallets received 731.59 BTC ($32,653,519 at the time of the transactions) from known darknet markets, ransomware organizations, cybercrime Garant services, and other illicit sources. See table below:

Source Category	Total TXs	Total BTC	Total USD/BTC
darknet market	100	16.96	$ 657,207
illicit actor-org	39	157.88	$ 4,764,631
ransomware	53	366.49	$ 15,197,561
stolen funds	15	190.26	$ 12,034,121
Total	**207**	**731.599149**	**$ 32,653,519.37**

[14] Based on my training and experience, I know that agents frequently use reliable and commercial blockchain tracing programs to identify the origins of cryptocurrency, including from criminal sources.

47. Further analysis of cryptocurrency exchange records identified at least 10 USDT addresses that were used to receive commission payments for the AudiA6 mixing service. A review of transaction history for these 10 USDT addresses shows the AudiA6 mixing service received a total of 10,530,468.337167 USDT, the equivalent of $10,530,320.98. In other words, AudiA6 profited from its self-described money laundering service in the amount of $10,530,320.98.

F. TKACHUK Identity Information

46. USSS agents observed AudiA6 advertisements on several other cybercrime forums whose advertisements were nearly identical to the Dark2Web AudiA6 advertisement. Through a separate investigation, agents obtained a copy of a cybercrime forum referred to herein as Forum A.[15] A review of the Forum A copy revealed that a user account "AudiA6" was created on April 11, 2016. In 2019, the AudiA6 Forum A user account asked that another user communicate with AudiA6 using the following email address: off-business@yandex.ru. The account also sent several messages to other members listing the Ukrainian phone number +380671000368 and asking them to send funds to a payment account associated with that phone number. I know that +380 is the country code for Ukraine.

47. The copy of Forum A also contained an account that used the moniker "xai," which is a moniker used on other forums to advertise the AudiA6 service. Beginning in 2016, the "xai" forum profile was registered with the email address r0671000368@gmail.com. The numbers in this email address largely correspond to the telephone number provided by the AudiA6 user account for Forum A. Pursuant to a search warrant, Google provided content for the email address r0671000368@gmail.com. The Google account used the same Ukrainian phone

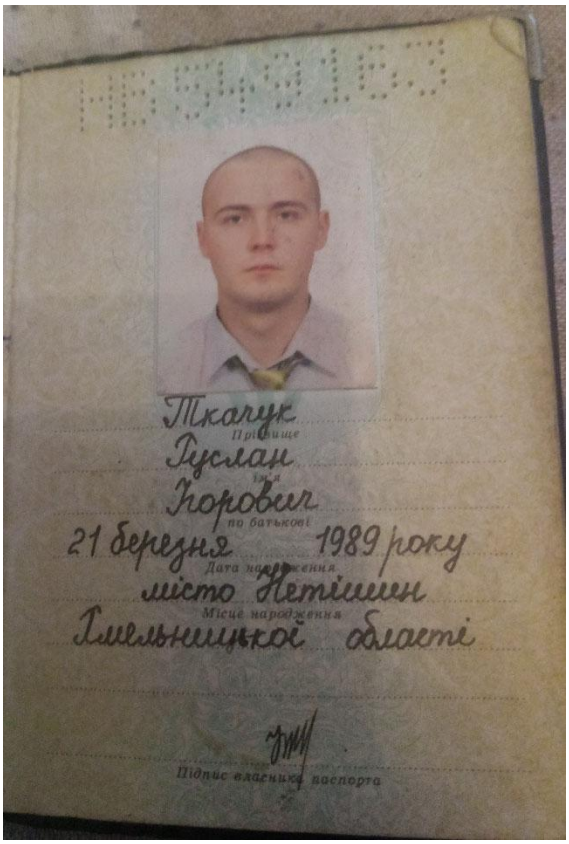
[15] The true name of Forum A is being withheld to protect law enforcement sources from disclosure when this affidavit is eventually unsealed.

number +380671000368 for account access as the AudiA6 Forum A user account.[16] Based on this information, I believe that since both the Forum A accounts for AudiA6 and xai are connected to the same Ukrainian phone number, it is likely they are controlled by the same person. Based on my training and experience, I know that services that require phone numbers often periodically send codes or other validation messages to the phone number to ensure it is still under the control of the account holder. Using the one phone number in a single user's control simplifies the authentication process. In addition, I know from reviewing multiple forums where users AudiA6 and xai have posted, both use the same user icon.

48. A review of the content from the Google account showed numerous messages addressed to Ruslan TKACHUK. For example, on August 20, 2020, the account received a Russian-language message from an online furniture store in Ukraine, which included an order confirmation for customer Ruslan Tkachuk, with a billing and shipping address in Kyiv, Ukraine. Separately, on August 21, 2020, the account received a Russian and Ukrainian-language message from a Ukrainian auto insurance company, which included a PDF attachment containing an insurance policy for customer Ruslan Igorevich Tkachuk, with an address in Netishyn, Ukraine. Finally, the Google Drive[17] for r0671000368@gmail.com contained the following Ukrainian identification document issued to TKACHUK:

[16] The account was registered in the name of Леонид Зеленков (transliterated as Leonid Zelenkov); however, in my training and experience, I know that cybercriminals often use fake names when registering for internet resources including email accounts.

[17] Google Drive is a service provided by Google that allows customers to store electronic files in the cloud and share those files with others who have been given access. See: https://workspace.google.com/products/drive/



49. The Google Drive for the account also contained two Excel files, Ауди_вбивы.xls and Товары.xls, which reference AudiA6 and are criminal in nature. The first file, Ауди_вбивы.xls, has a filename that references the moniker "Audi," and contains stolen victim credit card data and annotates payment for the "audia6" Jabber server. The second file, Товары.xls (which translates to "goods" or "merchandise"), contains gift card data as well as numerous references to the email address off-business@yandex.ru, the same email provided by Forum A user AudiA6.

50. Based on the foregoing evidence and my knowledge and experience, I believe that the r0671000368@gmail.com account is controlled by Ruslan TKACHUK. Further, the facts that 1) the r0671000368@gmail.com account contains files that reference AudiA6 and identification documents belonging to TKACHUK; and 2) servers for an apparently legitimate car rental

business owned by TKACHUK[18] were backed up to the same LEDENEV Hetzner-rented Storage Box where AudiA6 and Dark2Web servers were backed up, I believe TKACHUK uses the aliases "AudiA6" and "xai" and is a leader and manager of the AudiA6 mixing service.

G. LEDENEV Identity Information

51. Pursuant to a court order, Google identified programist1999@gmail.com as a recovery Google account linked to the email address azzazelllo@mail.ru, the email address used to rent the Storage Box server from Hetzner described above. Pursuant to a search warrant, Google provided content for programist1999@gmail.com account. According to Google records, the account was created in the name of "Alexeu T" on May 22, 2013.

52. Review of the programist1999@gmail.com account revealed that this account sent and received test emails to both the AudiA6 and Dark2Web servers. The programist1999@gmail.com received several emails from Google Search Console containing monthly search metrics for the domain dark2web.org, suggesting involvement in the operation of the forum. It also received emails addressing the account holder as Alexander and Alexander Ledenev (among other names) with an address in Batumi, Republic of Georgia. For example, on October 3, 2023, the account received a Russian-language message from a major European online travel agency confirming a hotel booking in Tbilisi, Georgia, with the guest's name listed as Alexander Ledenev. Furthermore, the programist1999@gmail.com account sent a total of 30 emails using the display name "Alex Led," further linking the account to the identity of Alexander Ledenev. Although the subscriber information lists a different name, the account receives multiple emails addressing "Alexander LEDENEV" or variations of the name.

[18] The servers for the car rental website were rented from Hetzner to TKACHUK. The car rental website was then backed up to the Storage Box rented by LEDENEV from Hetzner and contained within the "white" folder, as described above in ¶37.

Additionally, some of the messages sent to the programist1999@gmail.com account are from services that require identity documents for verification, such as those related to international travel. Based on review of the account contents, as well as my training and experience, there is probable cause to believe that LEDENEV controls the programist1999@gmail.com account. There is also probable cause to believe LEDENEV uses the moniker "Azzazello" and is involved in the operation of the AudiA6 mixing service and the Dark2Web forum. The programist1999@gmail.com account exchanged emails with both the AudiA6 and Dark2Web servers, and LEDENEV's name and the email azzazelllo@mail.ru were used to rent the Hetzner server that backs up the AudiA6 and Dark2Web servers. Moreover, the Dark2Web server contains an Azzazello user account that was registered with the email azzazelllo@mail.ru, and the "owner" of Dark2Web described Azzazello as the "technical creator" of the Dark2Web forum.

53. The Storage Box LEDENEV rents from Hetzner backs up information, in part, contained on other Hetzner servers rented in the name of Ruslan Tkachuk. As discussed *supra*, in ¶¶46-50, I believe that TKACHUK uses the moniker AudiA6 and manages the AudiA6 cryptocurrency mixing service. The Storage Box rented by LEDENEV contains information used by the AudiA6 cryptocurrency mixing service, including tables that contain profiles and email addresses used to open cryptocurrency exchange accounts and risk profiles for cryptocurrency addresses. The purpose of these tables is to store and aggregate data used for the operation and management of the AudiA6 mixing service. The use of the Storage Box to backup information could not be shared without the tacit coordination of the owners of the servers: LEDENEV and TKACHUK. Based on my training and experience, I believe the joint use of the Storage Box and the sharing of information contained within the Storage Box means that LEDENEV and

TKACHUK work together to operate the infrastructure of the AudiA6 mixing service and Dark2Web cybercrime forum.

54. In addition, review of emails contained in the LEDENEV-owned programist1999@gmail.com account reveals seven "test" emails received from the audia6.best and audia6.top domains and twenty-two "test" emails sent to the same domains. These emails contain little or no content but test the functionality of the AudiA6 cryptocurrency mixing websites. Based on my training and experience, I believe this email content shows that LEDENEV takes an active role in the management and operation of the AudiA6 websites and by consequence the cryptocurrency mixing service.

CONCLUSION

55. For all the reasons set forth above, I believe there is probable cause to believe that Ukrainian national Ruslan TKACHUK and Russian national Alexander LEDENEV work together to operate the AudiA6 mixing service, which launders criminal proceeds. There is also probable cause to believe that TKACHUK and LEDENEV work together to advertise the AudiA6 mixing service on the Dark2web forum, as well as other criminal cyber forums.

56. Using the AudiA6 mixing service and the Dark2Web cybercrime forum, undercover agents conducted six undercover money laundering transactions, including two within this district. During each transaction, undercover agents transparently informed AudiA6 service that the cryptocurrency transactions were meant to launder proceeds of crime, including proceeds of drug distribution in violation of 21 U.S.C. § 841, all in violation of 18 U.S.C. § 1956(h) and 18 U.S.C. §§ 1956(a)(3)(B) and 2.

57. In addition to the transactions conducted by undercover agents, IRS-CI agents have traced millions of dollars stemming from illicit sources as having passed through the AudiA6 money laundering service.

Respectfully submitted,

/s/ Elizabeth Aguilar Smith
ELIZABETH AGUILAR SMITH
Special Agent
United States Secret Service

Sworn to me by telephone on this 2nd day of June 2026

/s/ Jose R. Arteaga, USMJ
HONORABLE JOSE R. ARTEAGA
United States Magistrate Judge